RM Revisjon Midt-Norge

Informasjonssikkerhet og personvern

Overhalla kommune

Forvaltningsrevisjon

2026

FR1364

FORORD

Revisjon Midt-Norge SA gjennomfører denne forvaltningsrevisjonen på oppdrag fra Overhalla kommunes kontrollutvalg i perioden november 2025 til mai 2026.

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

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

Trondheim, 11.05.2026

Anna Ølnes

Oppdragsansvarlig revisor

Hanne Marit Ulseth Bjerkan

Prosjektmedarbeider

SAMMENDRAG

I denne forvaltningsrevisjonen er følgende problemstillinger undersøkt:

- Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
- Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (vertskommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Forvaltningsrevisjonen er gjennomført på bakgrunn av kontrollutvalgets bestilling i sak 16/25

Konklusjon

Revisors overordna konklusjon på den første problemstillingen er at Overhalla kommune har etablert sentrale elementer i et styringssystem for informasjonssikkerhet og personvern. Kommunens styrende dokumenter inneholder delvis sikkerhetsmål, sikkerhetsstrategi og beskrivelse av sikkerhetsorganisasjon, men revisor stiller spørsmål ved om dette har vært så forankret i organisasjonen. Ledelsessystemet (styrende dokumenter) for informasjonssikkerhet og personvern er gjenstand for revidering årlig, men inntrykket er at dette er enkel revidering som i hovedsak utføres IT-leder.

Kommunens system for internkontroll inneholder en stor del av de styrende dokumentene, prosedyrer og rutiner for informasjonssikkerhet og personvern. Noen dokumenter finnes også i systemet Elements (sak- og arkivsystem) og systemet for virksomhetsstyring, Framsikt. Revisor vil trekke fram at det i den nylig vedtatte, helhetlige ROS-analysen er tatt inn flere elementer som gjelder informasjonssikkerhet og personvern.

Overhalla kommune har personvernombud i egen organisasjon. Kombinasjonen mellom denne funksjonen og stillingen som HR-leder, kan utfordre uavhengigheten som funksjonen som personvernombud skal ha til kommunens ledelse. Funksjonen som personvernombud kommer dessuten i tillegg til full stilling som HR-leder, noe som kan medføre risiko for at det ikke er tilstrekkelig ressurser for å utføre funksjonen. Revisor vil likevel trekke fram at personvernombudet er oppmerksomt på dette, og informasjonsgrunnlaget i forvaltningsrevisjonen viser at hun bidrar med viktig støtte i personvernspørsmål for ledere i organisasjonen.

Det er etablert et system for behandlingsprotokoller, men det er noen mangler i noen av behandlingene for obligatoriske opplysninger. Kommunen har ikke et system for databehandleravtaler, men databehandleravtaler blir i stor grad praktisert. Controller har en rolle her. Kommunen har praksis for å gjennomføre DPIA, men det er i mindre grad etablert et system for dette.

Revisor konkluderer med at det skjer opplærings- og informasjonstiltak knyttet til informasjonssikkerhet og personvern, men det er i liten grad satt i system. Kommunen har et arbeid på gang, med utforming av policy for bruk av kunstig intelligens (KI). Dokumentasjonen viser at det er etablert beskrivelser av bruk av KI i kommunen, som synliggjør nødvendigheten av varsomhet når det gjelder personvern og annen taushetsbelagt informasjon. Det er likevel viktig å ha oppmerksomhet på forsvarlig bruk av KI, for eksempel gjennom opplæringstiltak.

På den andre problemstillingen konkluderer revisor med at Overhalla kommune ikke har etablert tilfredsstillende avtaler med Namsos kommune som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern. Utviklingen skjer raskt innenfor dette området, og nye sikkerhetsutfordringer oppstår kontinuerlig. Det er viktig at Overhalla har et avtaleverk med vertskommunen som er tydelig på ansvar og oppgaver. Oppfølgingen av vertskommune på informasjonssikkerhet og personvern er i hovedsak gjennom tilknytningen og kontakten IT-leder har med IT-tjenesten. Fraværet av systematikk og at oppfølgingen i hovedsak hviler på enkeltpersoner, gjør kommunen sårbar.

Anbefalinger

Revisor anbefaler kommunedirektøren i Overhalla kommune å iverksette en gjennomgang av styringssystemet for informasjonssikkerhet og personvern i kommunen som omfatter

- gjennomgang og revidering av styrende dokumenter, som involverer organisasjonen,
- vurdering av personvernfunksjonen med tanke på uavhengighet og ressurstilgang,
- vurdering av behov for rutiner og prosedyrer knyttet til behandlingsprotokoller, databehandleravtaler og vurdering av personvernkonsekvenser,
- utarbeiding av systematisk opplæring i informasjonssikkerhet og personvern, som også omfatter bruk av KI.

Revisor anbefaler videre, kommunedirektøren i Overhalla kommune om å ta initiativ til gjennomgang og revidering av alle avtaler som gjelder tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet og personvern.

Konklusjon og anbefalinger bygger beskrivelse av samla datagrunnlag og vurderinger knyttet til de to problemstillingene. Dette er gjort opp mot revisjonskriterier som er utledet fra regelverk og veiledere for informasjonssikkerhet og personvern. Datagrunnlaget er framskaffet ved gjennomgang av styrende systemer, dokumenter og avtaler, i tillegg til intervju med ledere og nøkkelpersoner i Overhalla kommune og ledere i IT-tjenesten i Namsos kommune.

Et utkast til rapport har vært til uttalelse hos kommunedirektøren i Overhalla kommune. Uttalelsen er lagt ved rapporten (vedlegg 2).

INNHOLDSFORTEGNELSE

Figurer

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Overhalla kommune bestilte en forvaltningsrevisjon med tema informasjonssikkerhet og digitalisering den 22.05.2025 (sak 16/25). Revisor la fram en prosjektplan i kontrollutvalgets møte den 11.12.2025 (sak 43/25). I prosjektplanen foreslo revisor å avgrense forvaltningsrevisjonen til informasjonssikkerhet og personvern, og holde digitalisering i form av utviklingsarbeid utenfor. Kontrollutvalget vedtok prosjektplanen med disse avgrensningene.

1.2 Problemstillinger

Følgende problemstillinger belyses i forvaltningsrevisjonen:

1) Har Overhalla kommune etablert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller kravene i regelverket (systematisk rammeverk)?
2) Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (vertskommunen), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

1.3 Om informasjonssikkerhet og personvern

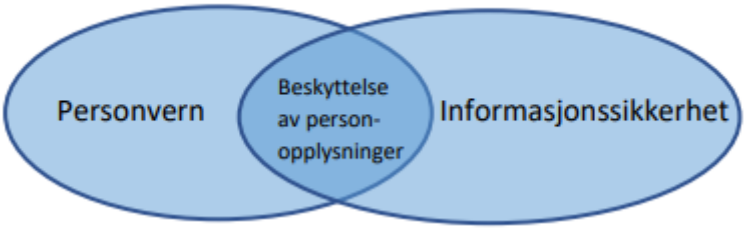
Informasjonssikkerhet handler om å verne alle typer informasjon. Eksempler på informasjonsverdier er data, fysisk IT-utstyr og infrastruktur, systemer, konfigureringer, programvare, applikasjoner og til og med menneskelige ressurser (Jøsang 2025)[1]. Ulike typer informasjon vil ha forskjellig beskyttelsesbehov. Videre skriver Jøsang at det ikke er noen tydelig avgrensning av hva som kan være informasjonsverdi. Derimot er det en klar definisjon på hvordan informasjonsverdier kan skades, nemlig gjennom brudd på konfidensialitet, integritet og/eller tilgjengelighet (se forklaring nedenfor).

KS har utarbeidet en veileder i informasjonssikkerhet og personvern, Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet.[2] I veilederen forklares personvern og

[1] A. Jøsang, *Cybersikkerhet - teknologier og styring*, 3. utg. (2025).

[2] KS og KPMG, *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet* (2022), https://www.ks.no/contentassets/c019638eeb1e4972bac838e34c75dc47/-19-03185-6-Kommunedirektorens-verktoykasse-for-personvern-og-informasjonssikkerhet-1418678-2-1.pdf.

informasjonssikkerhet som to fagområder som har mye til felles, men også noen forskjeller. Fagområdene overlapper hverandre når det gjelder beskyttelsen av personopplysninger. Det er viktig å være oppmerksom på at informasjonssikkerhet er mer enn personopplysningssikkerhet, på samme måte som at personvern er mer enn informasjonssikkerhet. Forholdet mellom fagområdene forklares ved bruk av figuren under:



Kilde: Veileder for personvern og informasjonssikkerhet, KS.

Figur 1. Forholdet mellom personvern og informasjonssikkerhet.

I veilederen beskrives informasjonssikkerhet som å verne all type informasjon, for eksempel opplysninger om kommunens innbyggere, ansatte, vannverk, økonomi eller kommunens servicetilbud. Ulik type informasjon vil ha forskjellig beskyttelsesbehov. Her trekker veilederen fram at beskyttelsesbehovet kan deles i:

Konfidensialitet, som er å beskytte informasjon mot uautorisert innsyn.
Integritet, som er riktig og komplett informasjon, og som er til å stole på.
Tilgjengelighet, som er at informasjonen er tilgjengelig når det er behov for den.

I veilederen trekkes fire grunnprinsipper fram for sikkerhetsstyring. Dette er de samme prinsippene som Norsk sikkerhetsmyndighet (NSM) legger til grunn. Disse beskriver hva kommunen bør gjøre for å opprettholde et akseptabelt sikkerhetsnivå. Grunnprinsippene er delt inn i fire kategorier:

Identifisere og kartlegge, som er kartlegging av eksterne og interne krav, identifisere verdiene, identifisere trusler, avdekke sårbarheter, utarbeide scenario, kartlegge avhengigheter og gjennomføre en konsekvensanalyse.
Beskytte og opprettholde, håndtere identifisert risiko, etablere sikkerhetsorganisasjon, etablere styringssystem og gjennomføre jevnlige øvelser.
Oppdage, jevnlig kontroll av sikkerhetstilstanden og gjennomføring av ledelsens gjennomgang.

Håndtere og gjenopprette, håndtere hendelser, evaluere og lære av hendelser.
De fire grunnprinsippene samsvarer godt med kravene i personvernforordningen artikkel 32.

I 2023 ble det vedtatt ny lov om digital sikkerhet (digitalsikkerhetsloven) som trådte i kraft fra og med 1. oktober 2025. Formålet med loven er at den skal bidra til å sikre grunnleggende krav til digital sikkerhet i virksomheter med særlig betydning for samfunnet ved å forebygge, avdekke og motvirke uønskede hendelser i nettverks- og informasjonssystemer som brukes for å levere samfunnsviktige tjenester og digitale tjenester. Loven skal også legge til rette for sikkerhet i IKT-produkter, IKT-tjenester og IKT-prosesser.[3] Loven gjelder for tilbydere av samfunnsviktige tjenester i sektorene energi, transport, helse, vannforsyning, bank, finansmarkedsinfrastruktur og digital infrastruktur. Den gjelder dessuten for tilbydere av digitale tjenester. Loven gjelder for tilbydere av samfunnsviktige tjenester, men til en viss grad kommuner. Den gjelder for kommuner med flere enn 50 000 innbyggere (helse- og omsorgstjenester) og kommuner som leverer minst 2000 m^3 vannressurser per døgn. Loven er ikke anvendt i denne forvaltningsrevisjonen.

I vedlegg 1 (utledning av revisjonskriterier) er regelverk og føringer for informasjonssikkerhet nærmere beskrevet.

1.4 Informasjonssikkerhet og personvern i Overhalla

Overhalla kommunes administrative organisering er kommunedirektør og strategisk ledergruppe på øverste ledernivå og tjenesteenheter på neste nivå, som er tjenester innen helse og omsorg, oppvekst osv.

Den strategiske ledergruppen består av kommunedirektøren, kommunalsjefene for oppvekst og helse og mestring, i tillegg til HR-leder og økonomisjef. I tillegg til strategisk ledergruppe og tjenesteenhetene, er det stabs- og støttefunksjoner innen IT, økonomi og servicesenter.

Overhalla har samarbeidet med Namsos kommune om IT-tjenester over lang tid. Først var det felles tjenester gjennom samkommunen Midtre Namdal samkommune. Fra og med 01.01.2020 ble samkommunen oppløst, og samarbeidet fortsatte som et vertskommunesamarbeid, med Namsos kommune som vertskommune og Overhalla kommune som en av samarbeidskommunene. Organisasjonen er nærmere beskrevet i kapittel 2.2.2 om beskrivelse av organisasjonen og informasjonssikkerhet og personvern.

[3] Lov om digital sikkerhet (Digitalsikkerhetsloven) (2023).

1.5 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001. Oppdragsansvarlig forvaltningsrevisor har vurdert egen uavhengighet overfor Overhalla kommune[4], og sørget for uavhengighet i revisjonsteamet.

Oppstartsbrev og oppstartsmøte

Etter at kontrollutvalget vedtok prosjektplanen, sendte revisor oppstartsbrev til kommunedirektøren og ba samtidig om et oppstartsmøte. Oppstartsmøtet fant sted 26.01.2026, og hadde som formål å redegjøre for bakgrunnen for prosjektet og problemstillingene, i tillegg til å forankre revisjonskriterier, anslå informasjonsbehov og tidsplan for gjennomføring av forvaltningsrevisjonen. I tillegg fikk vi oppnevnt kontaktperson, som har sørget for tilgang til kvalitetssystemet og koordinert intervjuavtaler. Kommunedirektøren deltok sammen med HR-leder, som også er personvernombud, og IT-leder. IT-leder har vært vår kontaktperson i denne forvaltningsrevisjonen.

System- og dokumentgjennomgang

Arbeidet med datainnsamling startet med lesetilgang til kvalitetssystemet Compilo. Her gjennomgikk vi mye av det som er styrende dokumenter for informasjonssikkerhet i kommunen, og vi gjennomgikk ROS-analyser og avviksstatistikk. I tillegg var samarbeidsavtalen (vertskommuneavtale) tilgjengelig i systemet, med leveranseavtale som vedlegg. Utover dette har vi etterspurt og fått tilsendt annen skriftlig dokumentasjon som belyser problemstillinger og revisjonskriterier.

Skriftlig dokumentasjon av styrende dokument, rutiner og prosedyrer, gir et konkret bilde på hva kommunen har av nødvendige dokumenter, rutiner for revidering av dokumenter, i tillegg til at det gir et godt grunnlag for å gå videre med spørsmål til de vi intervjuer.

Intervju

Vi har gjennomført intervju med seks ledere/ansatte i Overhalla kommune og to ansatte (gruppeintervju) i Namsos kommune. I Overhalla kommune intervjuet vi:

- Kommunedirektøren
- Kommunalsjef for oppvekst
- Kommunalsjef for helse og mestring

[4] jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

- HR-leder, både i kraft av å være HR-sjef og personvernombud
- IT-leder
- Økonomisjef
- Controller

I Namsos kommune intervjuet vi:

- IT-sjef og driftssjef (sammen)

Intervjuene er gjennomført ved fysisk besøk i kommunene, og individuelle intervjuer. Unntaket er kommunedirektøren, som ble intervjuet digitalt.

Intervjuene er basert på delvis strukturerte intervjuguider, med spørsmål som dels var felles for alle, og spørsmål som var tilpasset funksjonen til intervjuobjektene. Det ble skrevet referat for hvert intervju, som alle informantene har godkjent.

Intervju som metode er egnet til å få informasjon om ledere og ansatte har kjennskap til og praksis for informasjonssikkerhet og personvern, og deres opplevelse av om dette er tilfredsstillende i kommunen.

KI-verktøyet Copilot er brukt til korrekturgjennomgang og setningsforbedring.

Vurdering av metode

Alt i alt er det revisors vurdering at det totale dokumentasjonsgrunnlaget i rapporten gir et dekkende bilde av problemstillingene og revisjonskriteriene.

Det vil gjerne være dokumentasjon som kunne vært etterspurt, og flere intervjuer som kunne vært gjennomført. Vi har ikke intervjuet enhetsledere og ansatte i tjenestene. Det kunne gitt utdypende informasjon om kunnskap, bevissthet og praksis knyttet til informasjonssikkerhet og personvern. Målt opp mot tids- og ressursbruk er informasjonsgrunnlaget tilfredsstillende.

1.6 Uttalelse om rapport

Et utkast til rapport ble sendt til uttalelse hos kommunedirektøren. Det er gjort korrigeringer faktagrunnlaget på bakgrunn av innspillene fra kommunedirektøren, men det har ikke gjort det nødvendig med endringer i vurderinger og konklusjon. Etter at rapporten ble sendt til uttalelse fikk vi tilsendt en nyere versjon av databehandleravtale mellom Overhalla kommune og Namsos kommune. Kapittel 3.5.1 (funn) og 3.5.2 (vurderinger) er endret på bakgrunn av det. Konklusjon og anbefalinger er ikke endret.

2 STYRINGSSYSTEM

I dette kapittelet legger vi fram utleda kriterier, funn og revisors vurderinger på første problemstilling.

2.1 Problemstilling

Problemstillingen som belyses er:

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

2.2 Ledelsessystem for informasjonssikkerhet

I dette delkapitlet ser vi på om det er utarbeidet ledelsessystem for informasjonssikkerhet. Med ledelsessystem for informasjonssikkerhet legger vi Audun Jøsangs forklaring til grunn:

> Ledelsessystem for informasjonssikkerhet er en samling av dokumenterte samvirkende prosesser og aktiviteter for informasjonssikkerhet som organisasjonen har definert basert på anerkjente standarder, rammeverk og retningslinjer, samt egendefinerte policyer og prosedyrer. Det kalles system fordi det representerer en systematisk tilnærming til informasjonssikkerhet.[5]

2.2.1 Revisjonskriterier

- Kommunen skal ha et ledelsessystem for informasjonssikkerhet som angir
  - mål for informasjonssikkerhet og personvern (sikkerhetsmål)
  - strategi for hvordan sikkerhetsmålene skal nås (sikkerhetsstrategi)
  - roller og ansvar for informasjonssikkerhet og personvern (sikkerhetsorganisasjon)

2.2.2 Funn

Datatilsynet gjennomfører vinteren og våren 2026 et tilsyn i alle kommuner i Norge, om hvordan kommunene ivaretar sikkerhet rundt personopplysninger. Det er gjennomført en kartlegging i alle kommunene, hvor kommunene har blitt bedt om å svare på en rekke spørsmål i et spørreskjema. Revisor har fått tilsendt svarene på spørsmålene fra Overhalla kommune.

På spørsmål om kommunen har etablert et styringssystem for informasjonssikkerhet og personvern, har kommunen krysset av for «ja». Vi kommer tilbake til svar på flere spørsmål der det er aktuelt.

Revisor har fått tilgang til kommunens kvalitetssystem, Compilo,

I systemet finner revisor et dokument med tittelen Personvern og informasjonssikkerhet – sikkerhetsmål, sikkerhetsorganisasjon og sikkerhetsstrategi for Overhalla kommune. Dokumentet er opprettet november 2017, og sist revidert i februar 2026. Her framgår det et overordna formål i tre punkt. De tre punktene er:

- tilby innbyggerne i Overhalla et best mulig tjenestetilbud
- understøtte og sikre kommunens drift, allmenne tillit og omdømme
- tilfredsstille lovpålagte krav og andre myndighetskrav.

Kommunedirektøren forteller at kommunen er i gang med revidering av styrende dokument og operative dokument. Han sier at en del av dokumentene er noen år, og med bakgrunn i endring i verdensbildet, ser kommunen behov for å gjennomgå disse på nytt. Informasjonssikkerhet er et felt som endrer seg hele tiden. Med endring av verdensbilde, sikter kommunedirektøren til den politiske situasjonen og avhengigheten til de store, amerikanske teknologigigantene, som Microsoft, Google og sosiale medier, som Facebook.

I introduksjonen av **sikkerhetsmål** framgår det at kommunen skal ha et internkontrollsystem som sikrer konfidensialitet, integritet og tilgjengelighet. Det framgår fem punkt for å sikre dette:

1. at *uautoriserte ikke får adgang til* beskyttelsesverdig informasjon og sensitive personopplysninger
2. at tilgang til systemer og informasjon skal begrenses til *tjenstlig behov*.
3. at informasjonsbehandling er *korrekt* og at informasjon *ikke forandres* uten lovlig tilgang.
4. tilstrekkelig mulighet for å *oppdage, spore, forhindre og håndtere uønskede forsøk på uautorisert adgang*.
5. at medarbeidere har en *tilstrekkelig kompetanse* for å ivareta virksomhetens sikkerhetsbehov/krav.

Sikkerhetsmålene skal årlig vurderes som en del av ledelsens gjennomgang.

IT-leder forteller at strategien er et overordna dokument, og at det ikke er gjort store revideringer av dokumentene. Det var en gruppe som arbeidet med dokumentene da GDPR ble innført.[6] I kvalitetssystemet kommer det automatiserte meldinger om at det er tid for revidering. Da ser IT-leder over dokumentene. På spørsmål om det er styrende dokumenter som mangler, svarer IT-leder at det mangler styrende dokument om hvordan kommunen skal håndtere KI. Dette kan komme på sikt.

De andre informantene kjente til dokumentene, men hadde ikke deltatt i utarbeidelse eller revidering av dokumentene.

Kommunedirektøren viser til at også sikkerhetsmålene skal gjennomgås, i forbindelse med gjennomgangen som kommunen har med bakgrunn i verdenssituasjonen.

Dokumentet består videre av et kapittel som beskriver **sikkerhetsorganisasjon og sikkerhetsstrategi**. Her fremgår det følgende:

3.1. Ledelse og ansvar

1. Å nå sikkerhetsmålene skal oppnås ved kommunens ordinære ledelses- og styringssystem. Å ivareta kravene til personvern og informasjonssikkerhet skal være et ordinært lederansvar på ulike nivå jf. organisasjonskartet.
2. Kommunedirektøren er den behandlingsansvarlige jf. personvernloven.
3. Enhetslederes ansvar framgår av dokumentasjonen i kommunens internkontrollsystem for personvern, herunder Sikkerhetsinstruks for ledere.
4. Øvrige ansattes ansvar framgår av prosedyrer, rutiner mv. i internkontrollsystemet.

I sikkerhetsinstruksen for ledere, som det er henvist til ovenfor, er ansvaret for ledere med personalansvar beskrevet. Enhetsleder skal sørge for at eksisterende ansatte og nytilsatte gjør seg kjent med Sikkerhetsinstruks for ansatte. Enhetsledere skal sørge for at kommunale nøkler, nøkkelkort og IT-utstyr utleveres/innleveres etter behov, at det blir bestilt tilganger til relevante informasjonssystemer, og disse endres eller avsluttes. Videre skal enhetsledere

[5] A. Jøsang, *Cybersikkerhet - teknologier og styring*, 3. utg. (2025)

[6] Ikrafttredelse 20.07.2018

sørge for at ansatte gis nødvendig opplæring, at avvik som berører personvern og informasjonssikkerhet, bidra til at ansattes tilganger blir gjennomgått minimum 1 gang i året, at personvern og informasjonssikkerhet hvert år settes på dagsorden ved enheten og søke veiledning hos kommunens personvernombud ved behov for det.

IT-leder sier at det ikke er fastsatte roller i sikkerhetsorganisasjonen, men at det er fagpersoner som jobber med sikkerhet, og da datasikkerhet hvor arbeidet gjøres fra Namsos. Namsos kommune har et sikkerhetsutvalg, men Overhalla og andre samarbeidskommuner har vært ute av dette utvalget en periode. Det er meningen at de skal inn igjen i utvalget.

Kommunen har et administrativt delegeringsreglement, vedtatt 04.09.2025. Kapittel 2.7 handler om internkontroll og beredskap. Her går det fram at ledere på nivå 1-2[7] har ansvar for beredskap, internkontroll og informasjonssikkerhet for egen enhet.

Vi har spurt de vi intervjuet om ansvaret de har i organisasjonen generelt, og spesielt innenfor informasjonssikkerhet og personvern.

IT-leder har overordna IT-ansvar, som innebærer ansvar for driften av IT-systemer i samarbeid med Namsos kommune. Han har 80 % stilling i Overhalla og 20 % stilling i Namsos. Overhalla kommune kjøper 40 % stilling fra Namsos IKT, og IT-leder i Overhalla kommune er arbeidsleder til denne 40 % ressursen. IT-leder deltar ikke i ledergruppa, men hentes inn hvis det er eventuelle spørsmål som vedrører ledergruppa. IT-leder sitter i kriseledelsen.

HR-leder forteller at i den rollen handler det om å sikre informasjonen om de ansatte, helt fra rekruttering og til ansettelse. Videre handler det om å beskytte informasjonen slik at den ikke kommer på avveie, både fødselsnummer, fagforening, bankkonto og informasjon kommunen får gjennom rekrutteringsprosessen (intervju og søknad). HR-leder deltar i ledergruppen. HR-leder kjenner ikke til dokumentet som beskriver sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisasjon. Hun har tatt initiativ til at delegeringsreglementet blir revidert, for å tydeliggjøre ansvaret til hver enkelt leder. Hun mener at det er delegeringsreglementet som er fundamentet for alt ansvar i kommunen.

Kommunalsjef for helse og mestring har hatt den jobben siden september 2025. Hun har tidligere vært enhetsleder for helse i kommunen. Helse har mange systemer som berører både informasjonssikkerhet og personvern. Hun kjenner ikke detaljene som står i styringsdokumentet, men hun mener at innbyggerne skal være trygge på måten

[7] Revisor antar at det er nivå 1 er kommunalsjefer andre i kommunedirektørens ledergruppe, og nivå 2 er enhetsledere.

personopplysninger ivaretas. Som en del av ledergruppa har hun ansvaret for at enhetsledere sørger for at ansatte signerer sikkerhetsinstruks og får opplæring.

Kommunalsjef for oppvekst forteller at hun har det samme ansvaret som andre ledere, nemlig å sørge for at ledere og ansatte i hennes sektor kjenner til relevante regelverk, og at det øves. Informasjonssikkerhet blir tatt opp jevnlig i skoleledermøter, barnehagestyrermøter og på ledersamlinger i sektoren.

Teknisk sjef svarer direkte til kommunedirektøren, og i tillegg til funksjonen som teknisk sjef er hun beredskapskoordinator. Teknisk sjef er en enhetslederrolle. I mars 2026 har hun hatt funksjonen som beredskapskoordinator i ca. to år. Hun forteller at hun i den funksjonen har jobbet mye med helhetlig ROS. Det tilhører funksjonen som beredskapskoordinator å ha ansvar for å følge kontaktlisten i RAYVN, som er et nettbasert verktøy for krisehåndtering. Det er ikke beredskapskoordinatorens oppgave å føre logg. I kriseledelsen deltar hun som teknisk sjef. Som teknisk sjef tolker hun styringsdokumentene for informasjonssikkerhet inn i kommunens etiske retningslinjer.

Kommunedirektøren har opplevd at sikkerhetsorganisasjonen har stått seg godt, og kommer ikke på eksempler på at den ikke har vært tydelig og dekkende for kommunen. Han forteller at informasjonssikkerhet og personvern har vært tema i de to siste møtene i lederteamet. Han trekker også fram her at endringer i verdensbildet er medvirkende til at det har vært mye oppmerksomhet rundt informasjonssikkerhet og personvern på de siste møtene.

Det er ikke beskrevet i dokumentet hva som er kommunens **sikkerhetsstrategi.**

2.2.3 Revisors vurdering

- Kommunen skal ha et ledelsessystem for informasjonssikkerhet som angir
    - mål for informasjonssikkerhet og personvern (sikkerhetsmål)
    - strategi for hvordan sikkerhetsmålene skal nås (sikkerhetsstrategi)
    - roller og ansvar for informasjonssikkerhet og personvern (sikkerhetsorganisasjon)

Kommunen har dokumentert et ledelsessystem for informasjonssikkerhet og personvern, men revisor stiller spørsmål ved hvor oppdatert det er, om det holdes levende, og forankringen i organisasjonen.

Regelmessig revidering er satt i system, men det er få ansatte og ledere som er involvert i dette. Det har ikke vært regelmessig på sakskartet i lederteamet før den siste tiden.

Kommunens ledelsessystem inneholder sikkerhetsmål om å sikre konfidensialitet, integritet og tilgjengelighet. Revisor viser til vurderingen ovenfor, vurderer at sikkerhetsmålene er lite kjent i organisasjonen.

Etter revisors vurdering er sikkerhetsmålene konkrete for å sikre konfidensialitet, integritet og tilgjengelighet.

Kommunens ledelsessystem har delvis beskrevet hvordan sikkerhetsmålene skal nås (sikkerhetsstrategi).

Strategien beskriver organisering og ansvar for å nå sikkerhetsmålene. Utover dette går det ikke fram hvilken strategi kommunen har for å nå sikkerhetsmålene, for eksempel gjennom prioriterte tiltak, handlingsplaner eller målbare oppfølgingspunkter.

Kommunen har et ledelsessystem som delvis beskriver en sikkerhetsorganisasjon.

Sikkerhetsansvaret er innenfor kommunens ordinære ledelses- og styringssystem, men etter revisors vurdering mangler det beskrivelse av definerte sikkerhetsroller. Beskrivelse av sikkerhetsorganisasjonen er utvidet i en sikkerhetsinstruks for ledere og i kommunens administrative delegeringsreglement.

Noe av sikkerhetsarbeidet gjøres fra Namsos, som blant annet har et sikkerhetsutvalg. Overhalla (og andre samarbeidskommuner) deltar ikke i sikkerhetsutvalget. Overhalla har heller ikke et slikt utvalg internt i egen kommune.

2.3 Informasjonssikkerhet i systemet for internkontroll

2.3.1 Revisjonskriterier

eForvaltningsforskriften krever at det skal være etablert internkontroll på området for informasjonssikkerhet.

- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
    - Internkontrollsystemet skal inneholde regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern

- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må ha et avvikssystem og ansatte må melde avvik.

2.3.2 Funn

Overhalla kommune bruker Compilo som system for internkontroll. Revisor har gjennomgått systemet. Nedenfor beskrives det revisor har funnet i systemet.

Regelverk, prosedyrer og rutiner i systemet for internkontroll

Vi finner ulike mapper i Compilo, som har prosedyrer og rutiner for informasjonssikkerhet og personvern. Compilo er bygd opp med blant annet et dokumentbibliotek. I dokumentbiblioteket ligger ulike planer, regelverk, rutiner og prosedyrer. Opplistingen i dette dokumentet er ikke uttømmende. Innledningsvis i dokumentbiblioteket er det sju mapper, hvorav en mappe inneholder dokumenter som gjelder støtteprosesser, en mappe gjelder lover, forskrifter og rundskriv, og en mappe inneholder beredskap og krisehåndtering. Under lover, forskrifter og rundskriv er det lenker til tre lover; hvor bestemmelser om taushetsplikt og unntak for offentlighet i forvaltningsloven og offentlighetsloven er det som kan ha mest relevans for informasjonssikkerhet og personvern.

I mappen for beredskap og krisehåndtering, ligger det lenker til fem beredskapsplaner, hvorav Kommunal beredskapsplan og Beredskapsplan for langvarig strømbrudd er to av beredskapsplanene som tar opp informasjonssikkerhet. Videre ligger det to dokumenter om helhetlig ROS i mappen, et om helhetlig analyse og den andre er rapport fra helhetlig ROS-analyse.

I en mappe som heter «personvern, arkiv, informasjonsarbeid, kommunikasjon og saksbehandling» finner vi en undermappe for «personvern og informasjonssikkerhet». Her er det fem underliggende mapper. En mappe er «informasjonssikkerhet - styrende dokumenter» hvor vi blant annet finner dokumentet om sikkerhetsmål, sikkerhetsstrategi og sikkerhetsorganisasjon som ble beskrevet i kapittel 2.2. I tillegg er det et dokument om gjenoppretting av data og systemer, personvern ved IT- og papirbaserte løsninger, policy ved anskaffelse/forvaltning av programvare, policy for bruk og sikring av brukerutstyr og policy for passord og/autentiseringsinformasjon. En annen mappe inneholder prosedyre for risikovurdering og mal for risikovurdering. En tredje mappe under hovedmappen «personvern, arkiv,…osv.» heter personvernregelverk, som inneholder lenke til Datatilsynets oversikt over personvernregelverket.

I mappen for «beskrivelse av informasjonssystemet, sikkerhetstiltak og driftsrutiner, ligger det ulike prosedyrer for digital sikkerhet (konfigurasjon og sikkerhetsarkitektur, autorisasjon og tilgangsstyring osv.). For noen av rutinene vises det til vertskommunen. En annen mappe, hvor det er flere rutiner, kalles «rutiner for håndtering av personopplysninger. Her finner vi blant annet en rutine for bruk av kunstig intelligens (KI). Her er det også flere andre rutiner for håndtering av personopplysninger, bl.a. rutine for iverksettelse og opphør av behandling av personopplysninger. Flere av rutinene i denne mappen gjelder helsetjenestene. I en annen mappe finner vi sikkerhetsinstrukser, en som gjelder for ansatte og en som gjelder for ledere.

Det er også en rutine for avvikshåndtering i Compilo. I tillegg til beskrivelse av formål, definisjon av avvik og ansvar, er det et punkt om melding av avvik til Datatilsynet. Der går det fram at melding av avvik til Datatilsynet foretas av den behandlingsansvarlige, som er kommunedirektøren, eller av personvernombudet.

HR-leder forteller at ansvar for dokumenter i Compilo følger roller i systemet. Compilo gir, som vi beskrev tidligere, beskjed om når dokumenter skal revideres. HR-leder er også personvernombud, og i den rollen har hun ansvar for dokumenter knyttet til personvern og informasjonssikkerhet.

Kommunalsjef for helse og mestring sier at det gjøres mye arbeid med og innenfor internkontroll uten at det er dokumentert.

Kommunalsjef for oppvekst beskriver det som krevende å holde dokumentasjonen oppdatert. De har brukt skoleledermøtene til å justere prosedyrer og regelverk, for eksempel etter ny opplæringslov. Rektorene tar det deretter ned til egen skole.

ROS og beredskap

Som nevnt i kapittel 2.3.2 ligger det to dokumenter om helhetlig ROS i mappen for beredskap og ROS. Det ene er om helhetlig ROS-analyse, aggregert bilde, og det andre er rapport fra helhetlig ROS-analyse. Begge dokumentene er utgått, og det er vedtatt ny ROS-analyse i sak 2/2026, den 24.02.2026.

I avsnittet over, om regelverk, omtalte vi en prosedyre for risikovurdering. Prosedyren er generell, og gjelder alle former for risikovurderinger. Om personvern står det følgende:

> *Når det gjelder personvern skal risiko vurderes i forhold til a) konfidensialitet, b) integritet og c) tilgjengelig. For sensitive personopplysninger går ved kryssende hensyn, hensynet til konfidensialitet foran hensynet til tilgjengelighet og integritet.*

Videre finner vi mal for risikovurdering i samme mappe.

Teknisk sjef, som også er beredskapskoordinator, viser til at helhetlig ROS ble vedtatt i kommunestyret 24.02.2026. Hun forteller at det har vært jobbet mye med den. Kommunen har tatt utgangspunkt i fylkeskommunens ROS, og tilpasset den. Kommunen har tatt utgangspunkt i DSB sine skjemaer for å vurdere hendelsene. Oppsummering av disse hendelsene er gjennomgått i kriseledelsen.

Hun forteller at det i arbeidet med ROS er kommet forslag til nye tiltak, hvor det skal gjennomføres nye risikovurderinger etter at tiltakene er gjennomført. Hendelser rundt IKT og cybersikkerhet er noe av det som er risikovurdert og oppdatert.

Revisor har gjennomgått ROS-en. Om hendelse rundt IKT/cybersikkerhet står det:

> Denne hendelsen innebærer at kommunen er uten Internett, eller uten tilgang på sakssystemer. Dette vil påvirke kritiske samfunnsfunksjoner og -tjenester. Eksempelvis vil det ikke bli tilgang til pasientinformasjon hos legekontor, tilgang på overvåkningsutstyr på vann og avløp med mer. Krisehåndtering uten tilgang på Internett vil være problematisk.
>
> Kommunen blir fortløpende utsatt for risiko for slike hendelser. Kommunen må fortløpende vurdere nye tiltak for å imøtekomme de trusler som oppstår. Det er behov for å gjennomgå og revidere våre rutiner og planer for å imøtekomme nye trusler. Dette gjøres i samarbeid med de nabokommuner som vi har IKT-samarbeid med, samt øvrige kommuner i Trøndelag gjennom DigiTrøndelag-nettverket.

I skjemaet for aggregert risikobilde, er hacking oppgitt som mulig årsak til IKT/cyberangrep, og risikoen er framstilt med gult.[8] Tiltak som angis for å redusere risiko er: opplæring og bevisstgjøring, sikkerhetstiltak og beredskapsplan. Etter slike tiltak angis framstilles risikoen som grønn.

En annen hendelse som er tatt med er påvirkningsoperasjoner. Dette angis som høy risiko (rød), både før og etter tiltak. Et tiltak som kommunen har iverksatt som følge av dette, er utfasing av Facebook som kommunikasjonskanal med innbyggerne, og bruk av en annen plattform, Friskus.[9]

Beredskapsplanen ligger i verktøyet for virksomhetsstyring, Framsikt. Revisor har gjennomgått Overordna beredskapsplan, datert januar 2025, og sett om og hvordan den omtaler beredskap

[8] Skala grønn, gul, rød, der grønn representerer risiko og rød høy risiko.

[9] Norsk plattform for kommuner, primært rettet mot innbyggere og fritidsaktiviteter

for informasjonssikkerhet og personvern. Det henvises til overordna føringer i kommuneplanens samfunnsdel, hvor forebygging og håndtering av digital sårbarhet er et av delmålene. Av funksjonene som inngår i kriseledelsen er IT-leder en av funksjonene. Utover dette er ikke informasjonssikkerhet og personvern omtalt i beredskapsplanen, men det er henvist til beredskapsplan for strømbrudd.

IT-leder forteller at kommunen har gjennomført en diskusjonsøvelse i samarbeid med Namsos og Flatanger kommuner i regi av KiNS. Øvelsen handler om at kommunen er uten internett og programmer, men at de har strøm. Øvelsen varte i fire timer. Kommunene gjorde seg noen erfaringer, blant annet at et av tiltakene er å møtes fysisk. Kommunen har også gjennomført en enkel ROS knyttet til at Microsoft bortfaller. Revisor har fått tilsendt et dokument som oppsummerer et møte om microsoftavhengighet. Dokumentet oppsummerer hvilke sårbarheter det er rundt bortfall av Microsoft. Det var ansatte ved tre samarbeidskommuner, deriblant Overhalla som deltok i møtet. Fra Overhalla deltok IT-leder og controller.

Avvik

Informasjonssikkerhet og personvern er en egen avvikskategori i avvikssystemet i Compilo. Totalt ble det meldt 6 avvik i denne kategorien i 2024, 5 avvik i 2025 og 2 hittil i 2026 (begge i mars). Avvik innen informasjonssikkerhet og personvern er delt i underkategorier. Det er bare forhold som angår personvern som inngår i de underliggende kategoriene. Den kategorien det er meldt flest avvik i, er personopplysninger på avveie. Andre kategorier er svikt i systematisk internkontroll for personvern, brudd på registrertes rettigheter og tilgang til system.

Generelt, forteller HR-leder, at avvikskulturen i kommunen er i positiv utvikling, og det gjelder særlig avvik innen HMS.[10] Hun legger til at ansatte ikke er like flinke til å melde avvik som gjelder informasjonssikkerhet og personvern. Hun stiller spørsmål om ansatte tenker over eventuelle konsekvenser av det som gjøres ved bruk av epost og Teams? Av de fem avvikene som ble meldt i 2025, er tre-fire alvorlige avvik, ifølge HR-sjefen. Ett av avvikene ble meldt til Datatilsynet. Som personvernombud får HR-leder varsel om avvik som gjelder personvern. Det er leder som har ansvar for å behandle avvikene, men personvernombudet vurderer sammen med leder om avviket skal meldes videre (til Datatilsynet).

[10] Helse, miljø og sikkerhet

IT-lederen er også hovedverneombud. Han er involvert i avvikssystemet både som IT-leder og verneombud. Han er enig med HR-leder i at det er meldt få avvik innen informasjonssikkerhet og personvern. Han tror at grunnen til det er at ansatte ikke tenker over at det er avvik.

Kommunalsjef for oppvekstsjefen mottar av og til avvik, og understreker viktigheten av at ansatte må ta seg god tid når de behandler personopplysninger. Det har blitt meldt avvik til Datatilsynet, men det fikk ikke konsekvenser for kommunen. I etterkant av avviket, ble rutinene gjennomgått. Det er i hovedsak rektorene eller barnehagestyrerne som håndterer og lukker avvikene. Rektor eller barnehageleder tar kontakt med kommunalsjefen ved uklarhet. I forbindelse med rapporteringen til Datatilsynet, bistod HR-sjef/personvernombudet.

Kommunedirektøren forteller også at det meldes få avvik innenfor informasjonssikkerhet og personvern. Også han stiller spørsmål om det underrapporteres.

De øvrige som ble intervjuet kjente ikke til at det har vært meldt avvik innenfor aktuelt ansvarsområde.

2.3.3 Revisors vurdering

Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.

- Internkontrollsystemet bør inneholde regelverk, prosedyrer og rutiner for informasjonssikkerhet og personvern
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må ha et avvikssystem og ansatte må melde avvik.

Kommunens internkontrollsystem, Compilo, inneholder regelverk, prosedyrer og rutiner for informasjonssikkerhet, men det kan være mangelfullt.

Ettersom Compilo inneholder automatisk varsling om oppdatering/revidering av dokumentene, er dette i hovedsak satt i system. Det går fram når dokumentet sist ble revidert, og neste revidering. Revisor har, basert på intervjuinformasjon, inntrykk av at Compilo brukes aktivt, men at det er krevende å holde oppdatert.

Kommunen har nylig vedtatt helhetlig ROS-analyse, hvor flere elementer som vedrører informasjonssikkerhet og personvern er tatt inn. Kommunen gjennomfører delvis risikovurderinger, inklusive DPIA-er.

Risikoer knyttet til informasjonssikkerhet og personvern er omtalt i et kapittel om IKT/cyberangrep, i tillegg til påvirkningsoperasjoner. Revisor vil trekke fram som positivt, øvelsen som Overhalla og deltakerkommunene i IKT-samarbeidet har gjort sammen med KiNS.

Kommunen har informasjonssikkerhet og personvern som egen avvikskategori i Compilo. Det meldes få avvik innen denne avvikskategorien.

Revisor registrerer at informantene tror at avvik innen informasjonssikkerhet og personvern er underrapportert.

2.4 Personvern

I dette kapitlet presenteres revisjonskriterier, funn og revisors vurderinger om det som spesielt gjelder personvern.

2.4.1 Revisjonskriterier

- Kommunen skal ha personvernombud som skal støtte den behandlingsansvarlige i å oppfylle pliktene i virksomheten etter personvernregelverket:
    - Ha tilstrekkelige ressurser til å utføre oppgavene
    - Involveres regelmessig, ved relevante beslutninger og hendelser
    - Risikobasert tilnærming
    - Uavhengig rolle
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.

2.4.2 Funn

I dette kapittelet presenteres data fra styrende dokumenter og intervju om det som gjelder personvern.

Personvernombud

Det er etablert rutine for personvernombud[11] (Compilo). Rutinen inneholder 11 punkt om den behandlingsansvarliges/kommunedirektørens oppgaver og 14 punkt om personvernombudets oppgaver. Den behandlingsansvarlige, som er kommunedirektøren, skal utpeke personvernombud, sørge for opplæring, informere ansatte om personvernombud (navn, telefonnummer, epost, kontaktskjema), og ellers legge til rette for at personvernombudet får gjennomført oppgaven sin. Kommunedirektøren skal sørge for å sikre ombudets uavhengighet, og sørge for at det ikke oppstår interessekonflikter mellom rollen som ombud og ombudets øvrige oppgaver i organisasjonen.

Personvernombudets oppgave, slik den er definert i rutinen, er å påse at virksomheten har et system for internkontroll, veilede i, kontrollere overholdelse av og påpeke eventuelle brudd på personvernregelverket, og ellers bistå alle som henvender seg til ombudet om personvern.

Kommunens HR-leder har også funksjonen som personvernombud. Stillingen er 100 prosent som HR-leder, og det er ikke definert en stillingsressurs som personvernombud. Personvernombudet forteller at rammen for personvernombud må hun avgjøre selv. Hun er kjent med hva som bør gjøres og prioriteres, og det blir gjort en del ombudsrelaterte oppgaver i det daglige, men det er ikke satt i system.

Kommunedirektøren bekrefter at rollen som personvernombud ikke er definert som en stillingsandel. Han viser til at personvernombud ikke er en fortløpende driftstjeneste, men knyttet til endringer med informasjonssystemene og ivaretakelse av avvik og hendelser som gjelder personvern. Videre trekker han fram at rollen som HR-leder er en selvgående rolle og har stor mulighet til å definere egen hverdag. Hun kan derfor tilpasse ressursen etter behovene. Det er vanskelig å lage en idealsituasjon innenfor personvern.

Personvernombudet har ikke opplevd situasjoner der kombinasjonen av rollen som HR-leder og rollen som personvernombud har vært vanskelig. De to rollene blir hensyntatt i ledermøter. Hun viser likevel til at Datatilsynet er tydelig på at HR-leder ikke skal være personvernombud, og dette er noe kommunen har drøftet. Hun er tydelig på hvilke roller hun har i møter.

Personvernombudet trekker fram at Datatilsynet er tydelig på at HR-leder ikke bør være personvernombud.[12] Hun har ikke opplevd situasjoner hvor rollekombinasjonen har vært

vanskelig. De to rollene blir hensyntatt i ledermøter, og hun sier at hun er tydelig på hvilken rolle hun har i møter.

Kommunedirektøren sier at det er ambisiøse krav til personvernombud fra nasjonalt nivå, som skal tilpasses til lokalt nivå. En må ha ansatte som har grunnlag til å fungere som personvernombud. Han opplever at HR-sjefen har de egenskapene som gjør at hun kan ivareta disse oppgavene. Kommunedirektøren er komfortabel med løsningen. Kommunedirektøren mener at det er motstridende målsetninger. Ved større uavhengighet, er det i praksis vanskelig ha en ansatt som sitter tett på og som kan bli involvert og informert tilstrekkelig for å stille de riktige spørsmålene. Derfor er dette med uavhengighet en avveining. Han er komfortabel med løsningen og syns det er en god balansegang. Dersom de hadde satt bort rollen, ville personvernombudet kommet lenger unna, og følgelig mindre involvert. Kommunedirektøren har ikke tro på at det hadde vært en bedre løsning for kommunen.

Tidligere, i kapittel 2.4, viste vi til at HR-leders (personvernombudet) fokus på risiko i hovedsak var rettet mot HMS-vurderinger rettet mot vold og trusler, og at hun var usikker på risikovurderinger knyttet til informasjonssikkerhet.

Protokoll for behandling av personvern

Kommunen (behandlingsansvarlig eller den behandlingsansvarliges representant) skal føre protokoll over hvilke personopplysninger de behandler. Protokollen skal inneholde minimumskravene til opplysninger.

I mappen for informasjonssikkerhet i Compilo er det et dokument som har lenke til oversikt over behandlinger av personopplysninger. I tillegg inneholder dokumentet rutine for å oppdatere oversikten. Ifølge rutinen består oversikten av en fellesdel som gjelder behandlinger som bare foregår i administrasjonen eller behandlinger som er felles på tvers av sektorene. Videre står det at den inneholder oversikt per tjenesteområde. Oversikten skal oppdateres fortløpende og kontrolleres periodevis, ifølge rutinen. Ansvarlige for oppdatering er kommunalsjefene, teknisk sjef og enhetsleder for kultur og samfunn, i tillegg til kommunedirektøren.

Revisor har fått tilsendt behandlingsprotokoll. HR-leder/personvernombud forteller at kommunen har prøvd å finne gode system for behandlingsprotokoll, men at de har endt opp med et excellark.

Regnearket består, i tillegg til en oversikt for Overhalla kommune, en arkfane for veiledning, en arkfane for artikkel 30 protokoll[12], en fane for protokollforside og en arkfane for utgått avtaler. I veilederen framgår det at oransje kolonner skal inngå i protokollen over behandlingsaktiviteter etter personvernforordningens artikkel 30. Videre framgår det at de grønne kolonnene ikke er obligatoriske, men at det kan være hensiktsmessig å fylle de ut.

I oversikten for Overhalla kommune er det i alt oppført 87 informasjonssystem/fagsystem. Vi beskriver status for den informasjonen som er obligatorisk. For alle systemene er det fylt ut formål med behandlingen, det samme er det for kategorier av registrerte. Når det gjelder kolonnen for kategorier av personopplysninger, er det fire systemer som det ikke er fylt ut for. Når det gjelder kolonnen for kategorier av mottakere som personopplysningene vil bli eller er utlevert til, er det ikke fylt ut for noen av de 87 systemene. Når det gjelder kolonnen for planlagte frister for sletting av forskjellige kategorier personopplysninger, er det fylt ut for 11 av de 87 systemene.

Den siste obligatoriske informasjonen er navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet. Denne informasjonen er fylt på arkfanen kalt protokollforside.

HR-leder/personvernombud sier at protokollen ikke nødvendigvis er fullstendig. Det er IT-leder som sender ut excelarket og ber ansatte om å revidere.[13]

I Compilo finner revisor også rutine for databehandleravtaler og tjenestenivåavtale (SLA). Det framgår at databehandleravtale skal inngås ved engasjering av databehandler så framt ikke kravet om databehandleravtale er unntatt ved lov. Det framgår videre at tjenestenivåavtale skal inngås ved anskaffelse/ kontrahering av tjenesteleveranser.

HR-leder/personvernombudet kjenner ikke til rutiner rundt databehandleravtaler, men viser til at controller bistår med å holde oversikt over databehandleravtaler. IT-leder forteller at det har blitt enighet om at databehandleravtaler skal legges i sak- og arkivsystemet (Elements). Det

[11] [11] Rutine for personvernombud med ansvars- og oppgavefordeling

[12] 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]. Kapittel IV: Behandlingsansvarlig og databehandler

[13] Revisor har ikke utdypende informasjon om det er ansatte som er ledere eller det er andre ansatte.

er krevende å følge opp alle avtalene, og IT-leder viser også til controller, og at han bistår her. Det er ofte systemeier, kommunalsjef, som signerer avtalene.

Controller bekrefter at han har en rolle knyttet til databehandleravtale. Han sørger for å se gjennom databehandleravtalen sammen med leverandøren i forbindelse med anbudet. Controller forteller at det i gjennomgangen av databehandleravtalene, er billagene som er interessante og som krever utfylling ved inngåelse av kontrakter etter SSA avtalestandarden[14] Det er ikke alltid nødvendig å koble på IT. Anskaffelsesprosessen kan også være kjørt av andre aktører, som andre kommuner og fylkeskommunen. Det er fagledelsen som signerer på sine avtaler. Controller forteller at kommunen i stor grad støtter seg på malene fra DFØ og Datatilsynet som dekker det de vesentlige momentene som må avklares mellom databehandler og behandlingsansvarlig. Kommunen benytter som hovedregel disse malene i alle anskaffelser der de selv gjennomfører prosessen. Det hender at leverandører legger fram egne databehandleravtaler. Disse blir da gjennomgått og sammenlignet med DFØs og Datatilsynets maler for å sikre at risikofordelingen mellom partene er rimelig og ikke skjevfordelt og at behandlingsansvarliges ansvar er ivaretatt.

Revisor har ikke etterspurt konkrete eksempler på databehandleravtaler, men ser at det ligger flere databehandleravtaler i Compilo.

Vurdering av personvernkonsekvenser (DPIA)

Revisor ser at det er tre DPIA-er i Compilo:

- Confrere – videokonsultasjon
- Dignio Prevent – elektronisk medisineringsstøtte
- Digitalt tilsyn (rapport)

Alle tre DPIA-ene er fylt ut etter en mal, men noe ulike maler. Det er ikke mal for dette i Compilo.

HR-leder involveres i DPIA-er som personvernombud. Personvernombudet har tatt opp spørsmålet om hvor DPIA-ene best kan lagres. Hun mener at DPIA-ene bør være i sak- og arkivsystemet, for å vise at kommunen har gjennomført disse vurderingene. Kommunen har ingen rutine på hvordan oppbevare DPIA-er.

[14] Statens standardavtaler

Personvernombudet viser til eksempler der hun har bistått med risikovurderinger knyttet til nye system. Matombringing og bruk av KI innen helse, er eksempler hun trekker fram, hvor hun har bidratt i DPIA-vurderinger for å sikre personvernet.

IT-leder bekrefter at kommunen har forbedringspotensial når det gjelder rutiner for DPIA. Han mener at kommunen har mer å gå på knyttet til dette i samarbeidet med Namsos kommune. Han har ikke gjennomført DPIA-er.

Kommunalsjef for helse og omsorg sier at det er gjennomgang av hvilke opplysninger som lagres og hvem berøres ved nye system. Det er maler som brukes i disse vurderingene. Malen og gjennomgangen viser om det må utarbeides en fullverdig DPIA. Her benytter de seg også av andre kommuner, og hva de har tenkt i sin DPIA. I forbindelse med disse vurderingene blir personvernombudet involvert. De beskriver punktene i malen, blant annet lagring og sletting av data. Vurderingene som gjøres, er noe de er bevisste på i starten når de jobber med dette, men utfordringer er å ha bevissthet på det etter oppstart. Samtidig er det sjeldent store endringer, sier kommunalsjefen, slik at det som er gjeldende er ofte relevant. Det er hennes ansvar å følge opp dette, men hun er sjelden nede i detaljene. Det er enhetsledernes oppgave.

Kommunalsjef for oppvekst sier at hun gjør dette sammen med IT-leder. Hun sier at det skal ha en hensikt for mange hvis apper skal tas i bruk. Det er oppvekstsjefen som beslutter programvare og apper.

Kommunedirektøren trekke fram at dette skal gjennomføres der det særlig er behov for det. Han er komfortabel for helse, hvor det er gjort gode vurderinger. Når det er systemer som anskaffes med andre kommuner, kan kommunen bruke deres grunnlag for vurderinger. Samtidig stiller han spørsmål om nivået på DPIA-ene og om dette er godt nok.

2.4.3 Revisors vurdering

- Kommunen skal ha personvernombud som skal støtte den behandlingsansvarlige i å oppfylle pliktene i virksomheten etter personvernregelverket:
    - Ha tilstrekkelige ressurser til å utføre oppgavene
    - Involveres regelmessig, ved relevante beslutninger og hendelser
    - Risikobasert tilnærming
    - Uavhengig rolle
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Kommunen skal ha system for at det blir inngått databehandleravtaler
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.

Kommunen har personvernombud som langt på veg støtter den behandlingsansvarlige i å oppfylle pliktene i kommunen etter personvernregelverket.

Personvernombudet har ikke definerte ressurser til å utføre funksjonen.
Personvernombudets tilnærming til rollen, er ikke nødvendigvis risikobasert.
Personvernombudet er også HR-leder, to funksjoner som Datatilsynet anbefaler at ikke kombineres på grunn av personvernombudets uavhengighet.

Kommunen har et system for (regneark) for behandlingsprotokoller som delvis er fulgt opp.

Regnearket som er systemet for behandlingsprotokoller, mangler obligatorisk informasjon på mange av kategoriene.

Kommunen har langt på veg praksis for å inngå databehandleravtaler, men det er uklart om kommunen har et system for dette

Revisor har sett at det er maler for databehandleravtaler i Compilo, men intervjuinformasjonen tyder på at det er lite kjennskap til malene. Kommunen støtter seg på DFØ i dette arbeidet.

Kommunen har langt på veg praksis for å gjennomføre DPIA-er, men kommunen har i varierende grad system for dette.

Etter revisors vurdering er det i stor grad praksis i organisasjonen med å gjennomføre DPIA-er, men med unntak av helse, er det i varierende grad skriftlige rutiner og maler for dette.

2.5 Opplæring i informasjonssikkerhet og personvern

I dette kapitlet presenteres opplæring av ledere og ansatte i informasjonssikkerhet og personvern, inklusive KI.

2.5.1 Revisjonskriterier

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i policy og informasjon om informasjonssikkerhet.
- Kommunen bør ha policy for bruk av kunstig intelligens (KI).

2.5.2 Funn

I dette kapitlet presenterer vi informasjon og vurderinger av opplæringen i informasjonssikkerhet og personvern i kommunen.

Opplærings- og informasjonstiltak i informasjonssikkerhet og personvern

I dokumentet «Sikkerhetsinstruks for ledere» framgår det en rekke punkter som enhetsleder skal sørge for. Enhetsleder skal sørge for at «eksisterende ansatte og nyansatte ved tiltredelse (så tidlig som mulig) gjør seg kjent med «Sikkerhetsinstruks for ansatte». Videre framgår det i et av punktene at enhetsleder skal sørge for at det gis nødvendig opplæring i informasjonssystemer. Personvern og informasjonssikkerhet skal hvert år settes på dagsorden ved enheten, for bevisstgjøring av egne ansatte. Enhetsledere skal søke veiledning hos kommunens personvernombud ved behov.

Det er også en sikkerhetsinstruks for ansatte. Denne inneholder instruks for taushetsplikt, innsyn i sensitiv informasjon, bruk av privat epostadresse til jobbrelatert og private formål og instruks om passord. I instruksen er også bruk av KI beskrevet (se nedenfor).

HR-leder forteller at opplæring i informasjonssikkerhet og personvern er delegert til lederne, som skal sørge for tilstrekkelig opplæring. Nytilsatte ledere får et introduksjonsprogram som HR-leder sender ut. Det innebærer gjennomgang med HR, kommunedirektør, økonomi og arkiv. Programmet skal sørge for at nye ledere er i stand til å ivareta lederrollen.

HR-leder sier videre at sikkerhetsinstruksen ligger i Compilo som en leseliste. Lederne må sørge for at denne blir gjort kjent blant ansatte. Hun innrømmer at kommunen har en vei å gå for å få mer systematisk opplæring og evaluering.

Hverken kommunalsjef for helse og omsorg eller oppvekst har fått opplæring i informasjonssikkerhet og personvern, ifølge dem selv. Kommunalsjef for helse og omsorg sier at siden hun har 17 års erfaring som leder i kommunen har det kanskje blitt noen hull i opplæringen som kommunalsjef. Oppfølging kan knyttes til rutiner som ligger i Compilo. Ansvaret for opplæring innen helse- og omsorgsområdet ligger hos enhetslederne. Hun har tillit til at enhetslederne følger opp dette.

Flere nevner at IT-tjenesten sender ut opplæringsvideoer til alle ansatte på epost. Kommunalsjefen for helse og omsorg har etterspurt oversikt over deltagelsen, og har ikke fått tilbakemelding om at helse sin deltagelse er svak. Samtidig tror hun det er en stor strekk i laget blant de ansatte i hennes sektor når det gjelder kommunal epost, og om de fanger opp disse opplæringsvideoene. De ansatte har egen bruker, men ikke egen PC. De må logge inn felles utstyr.

Også økonomisjefen viser til informasjonsvideoer fra IT. Han mener at det er blitt ganske mange av dem, og at han for sin egen del har sluttet å se på disse videoene. Utover dette har

ikke han deltatt i noen opplæringstiltak av denne typen, men er gjort kjent med temaet gjennom ledermøter. Han trekker også fram ROS-analyser som en anledning for ansatte for opplæring.

Teknisk sjef viser også til informasjonsvideoene fra IT. Hun har ikke fulgt opp om ansatte i hennes avdeling har gjennomført disse videoene.

Kommunalsjef for oppvekst har deltatt i samlinger med KiNS gjennom vertskommunesamarbeidet med Namsos kommune. Det var gjennomgang og øvelse på en tenkt hendelse. Kommunalsjef for oppvekst viser til at nytilsatte ledere og andre ansatte får en innledende opplæring sammen med kommunedirektør, HR-leder og IT-leder, noe det er rutine for.

Kommunedirektøren har deltatt på ulike opplæringer, men ikke i senere tid. Kommunen har en enkel og lavterskel opplæringsløsning som går til alle ansatte på epost. På overordnet nivå har det ikke vært noen spesielle kurs på informasjonssikkerhet den senere tid. De holdt på med dette da styringsdokumentene ble bygget opp, forteller han.

Han forteller videre at Kommunen var medlem i KiNS, men meldte seg ut på grunn av økonomi. Namsos kommune er med i KiNS. Overhalla blir derfor informert om arbeidet via IT-tjenesten.

Policy for bruk av kunstig intelligens (KI)

Vi har tidligere i rapporten beskrevet dokumenter for bruk av **KI**. I Compilo finner vi et dokument ved navnet Bruk av KI. Her beskrives ansattes tilgang til bruk av Microsoft Copilot. Det står følgende om Copilot, og hvordan denne skiller seg fra andre lignende verktøy:

> Det som skiller Copilot fra andre verktøy er at sikkerhetsnivået er høyere enn verktøy som finnes på internett, fordi alle data blir slettet når du logger av tjenesten eller lukker nettleservinduet.

Til slutt i dokumentet oppfordres det til bruk KI, men det blir understreket at det aldri må deles personlig informasjon om brukere og ansatte, eller annen sensitiv informasjon. Det går fram at KI ikke skal brukes i fagsystem, og det oppfordres til å sjekke fakta.

HR-leder/personvernombudet har utarbeidet KI-policy sammen med IT-leder. Alle ansatte har tilgang til Copilot. Den ligger ikke på leselisten til ansatte, og hun vet for lite om bruken, men hun antar at bruken er utbredt.

IT-leder mener at det mangler dokumenter på KI, og at det nå er et stort tema hvordan kommunen skal håndtere dette. Det kan bli et styrende dokument på sikt, kanskje i samarbeid med Namsos kommune.

Kommunalsjef for oppvekst forteller at temaet diskuteres, men at hun opplever usikkerhet rundt dette. Hun forteller at KI i tekstproduksjon, kildekritikk og personvern inngår i opplæringen på ungdomstrinnet.

Kommunalsjef for helse og omsorg sier at det ikke er spesifikk opplæring i bruk av KI, men at ansatte er oppfordret til å være forsiktige og bruke Copilot. Hun viser også til sikkerhetsinstruksen, og det som står der om sensitiv informasjon om KI.

Økonomisjefen sier at KI brukes noe, mest til spørrehjelp og tekstforbedring. Han kjenner ikke til at kommunen har noen policy for KI. Han sier at de stoler på leverandørens kompetanse. KI har heller ikke vært tema i opplæringssammenheng.

Teknisk sjef forteller at KI brukes til saksfremlegg, hvor teksten kan kjøres gjennom en språkmodell. Det er retningslinjer i kommunen om at det ikke skal deles personsensitiv informasjon. Hun har tillit til at ansatte har fått med seg dette. Hun viser også til at ansatte må være bevisste på å kvalitetssikre det som kommer fra KI.

Kommunedirektøren sier at KI har vært tema flere ganger i ledergruppa og ledersamlinger. Han viser til dokumentet som er belyst ovenfor, og beskriver det som en førsteversjon for policy for bruk av KI, men ikke god nok. Det er mye spørsmål om bruken av KI, og det må sees i sammenheng med hvilke muligheter, trusler og risikoer det er knyttet til bruken av KI, både i lokal- og storsamfunnet.

På spørsmål om han kjenner til bruken av KI i organisasjonen, sier kommunedirektøren at administrasjonen kan benytte integrert verktøy, Copilot, til tekstbehandling og støtte. Det er en del ansatte som er ivrig og andre ikke, noe som gjør bruken variabel. Han er trygg på at bruken av KI-verktøy brukes forsvarlig, at taushetsbelagt informasjon blir ivaretatt og at det ikke blir brukt til å skape falske dokumenter. Det jobbes med bevisstgjøring av dette og at man ikke skal bruke åpne løsninger.

2.5.3 Revisors vurdering

- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i policy og informasjon om informasjonssikkerhet og personvern
- Kommunen bør ha policy for bruk av kunstig intelligens (KI)

Kommunen har delvis sørget for opplæring i informasjonssikkerhet og personvern for ledere og ansatte.

Det er sikkerhetsinstrukser for ledere og ansatte. I ledernes sikkerhetsinstruks går det fram at de skal sørge for at eksisterende og nyansatte skal gjøre seg kjent med sikkerhetsinstruksen for ansatte, herunder sørge for opplæring i nye systemer og at personvern og informasjonssikkerhet årlig settes på dagsordenen. I sikkerhetsinstruksen for ansatte framgår instruks for taushetsbelagt informasjon, bruk av jobb-epost og bruk av KI, for å nevne noe. Intervjuinformasjonen tyder på at opplæringstiltakene følges opp i varierende grad.

IT-tjenesten sender også ut opplæringstiltak på e-post, men kommunens ledere har ikke oversikt over om ansatte deltar i dette. Det kan være risiko for at ansatte slutter å se disse opplæringsvideoene etter hvert som det blir flere av dem.

Kommunen har en enkel policy for bruk av kunstig intelligens, som er under utvikling.

Kommunens ledere og ansatte bruker KI til ulike oppgaver, som tekstskaping. Det er uklart om ansatte har fått opplæring eller informasjon utover sikkerhetsinstruksen og dokumentet som heter Bruk av KI.

3 OPPFØLGING AV VERTSKOMMUNEAVTALE

3.1 Problemstilling

I dette kapitlet har vi undersøkt problemstillingen:

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

3.2 Revisjonskriterier

- Det skal være en skriftlig samarbeidsavtale mellom vertskommunen og Overhalla kommune som
    - er oppdatert i henhold til gjeldende regelverk og sikkerhetsbehov
    - ivaretar hvilke oppgaver og myndighet som vertskommunen skal utføre for samarbeidskommunen, som sikrer informasjonssikkerhet og personvern
    - følges opp med rapportering og samhandling
- Kommunen bør ha inngått leveranseavtale med Namsos kommune, som ivaretar
    - 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)
- Kommunen må ha databehandleravtale med vertskommunen som sikrer informasjonssikkerhet og personvern i tråd med regelverket.

3.3 Samarbeidsavtalen

I dette kapitlet presenterer vi innholdet i samarbeidsavtalen, som er vertskommuneavtalen mellom Overhalla (samarbeidskommune) og Namsos kommune (vertskommune). I tillegg presenterer vi intervjuinformasjon fra intervju med kommunedirektør og IT-leder i Overhalla kommune, samt leder og driftsleder ved IT-tjenesten i Namsos kommune.

3.3.1 Funn

Samarbeidsavtalen, som er tilgjengelig i Compilo, er signert av rådmannen i Overhalla kommune den 21. mai 2019. Prosjektleder Nye Namsos/rådmann i Namsos har signert avtalen på vegne av Namsos kommune. Det er et administrativt vertskommunesamarbeid.

Som vedlegg til samarbeidsavtalen er det et dokument som er kalt Leveranseavtale. Vi omtaler den i neste delkapittel.

Samarbeidsavtalen har 9 punkt. I tillegg til om avtalen er *oppdatert* etter gjeldende sikkerhetsbehov, beskriver vi i dette kapitlet innholdet i punktene om *oppgaver* og *rapportering og samhandling.*

Kommunedirektøren sier i intervju at samarbeidet gjerne er på det tekniske nivået, men legger til at Overhalla kommune likevel har et ansvar for tjenestene som baserer seg på disse tekniske løsningene. Avtalen som ble inngått i 2019 var hensiktsmessig da, men kommunedirektøren sier at situasjonen er en helt annen nå enn for 6-7 år siden. Det er behov for å videreutvikle samarbeidet. Det har vært flere endringer i Namsos kommune, som kommunesammenslåing og påvente av ny kommunedirektør som har medført at en gjennomgang av samarbeidsavtalen er satt på vent.

IT-leder i Overhalla forteller at avtalen ble videreført fra samkommunen til vertskommunen i 2019, uten at det var noen stor prosess. IT-leder forteller han at han deltok i revideringen av samarbeidsavtalen i 2019.

IT-leder sier at Flatanger kommune har inngått en ny avtale, og at det vil være hensiktsmessig å ta utgangspunkt i den når avtalen skal revideres. I den nye avtalen må avklaring rundt ressurser, og tilgang til disse komme med, understreker han. Det er ikke satt noen plan for revidering.

Revisor har intervjuet leder for IT-tjenesten i Namsos kommune, sammen med driftsleder i samme organisasjon. De omtales i det følgende som IT-tjenesten. Ingen av dem var involvert i utarbeidelsen av samarbeidsavtalen. De er tydelige på at avtalen med Overhalla kommune bør revideres. Samarbeidet mellom de to kommunene har vokst fram organisk,[15] slik at avtalen er noe de ikke forholder seg til i praksis.

[15] Digdir: refererer til «digitale økosystemer», som oppstår organisk, gjennom naturlig samarbeid, felles verdier osv. https://samarbeid.digdir.no/eformidling/et-okosystem-er-mer-enn-en-samling-felleslosninger/1006

Om o*ppgavene* som vertskommunen utfører for samarbeidskommunen står det at vertskommunen har ansvar for organisering av felles infrastruktur, IKT-oppgaver og programvare tilsvarende det som i dag [før 2020] er innenfor MNS[16] for samarbeidskommunen. Videre henvises det til leveranseavtalen, og nærmere beskrivelse av oppgavene der.

I avtalens punkt om rapportering og samhandling, står følgende:

- Overhalla skal orienteres fortløpende om viktige forhold
- Kontaktmøte årlig i oktober på kommunedirektørnivå
  - Evaluering av samarbeidsavtale og leveranseavtale
  - Forbedringsmuligheter
  - Gjensidig informasjon om utviklingstrekk som kan bety endringer
- Felles utviklingsarbeid, IKT-strategier og sikkerhetsstrategier
- E-fagråd – samle og koordinere innspill fra IKT-brukerne og samarbeidskommunene

Flere av punktene, for eksempel om evaluering av avtaler, forbedringsmuligheter, utviklingsarbeid og e-fagråd er ikke fulgt opp, ifølge kommunedirektøren og de andre vi intervjuet. Kommunedirektøren opplyser at en kan få til mer systematikk rundt en felles arena for å diskutere og følge opp informasjonssikkerhet og personvern. Det er mye som foregår i hverdagen, men det mangler fellesarenaer for ledelsesnivået. Det er årlig budsjettmøte, men informasjonssikkerhet kommer ikke regelmessig opp i de møtene.

Heller ikke de kjenner til at det finnes et e-fagråd. De forteller at det i det daglige er IT-leder i Overhalla som i praksis formidler det som et e-fagråd eventuelt skulle ivaretatt. Innspill fra IT-leder i Overhalla registreres i supportsystemet eller en chat som også fungerer som kanal. Namsos kommune har et informasjonssikkerhetsutvalg, og her burde også samarbeidskommunene involveres, ifølge de to fra IT-tjenesten. De trekker fram at Namsos kommune er i rekrutteringsprosess i forbindelse med ny kommunedirektør. Revidering av samarbeidsavtalen er satt på vent på grunn av ny kommunedirektør i Namsos.

Innenfor helse er det møter mellom IT og helse om elektronisk pasientjournal (EPJ). Kommunene i vertskommunesamarbeidet har ulike skolesystem. Det jobbes med å få de samme systemene, og IT-leder prøver å påvirke kommunene til å velge samme system. Samtidig er det lederne for de ulike sektorene som beslutter hvilke system og programvare som skal brukes.

[16] Midtre Namdal Samkommune (organisert som forsøk fra 2009 – 2012, organisert etter tidl. kommunelovs kapittel 5B, Samkommune, 2012 - 2019.

3.3.2 Revisors vurdering

- Det skal være en skriftlig samarbeidsavtale mellom vertskommunen og Overhalla kommune som
    - er oppdatert i henhold til gjeldende regelverk og sikkerhetsbehov
    - ivaretar hvilke oppgaver og myndighet som vertskommunen skal utføre for samarbeidskommunen, som sikrer informasjonssikkerhet og personvern,
    - følges opp med rapportering og samhandling

Det ble inngått en skriftlig samarbeidsavtale mellom Overhalla kommune og Namsos kommune senest i 2019. Revisors vurdering er at samarbeidsavtalen mellom Overhalla kommune og vertskommunen ikke er oppdatert etter gjeldende regelverk og sikkerhetsbehov

Revisor bygger vurderingen på at avtalen, som ble revidert i 2019, i hovedsak var en videreføring av avtalen som gjaldt i samkommunen i årene før, og at det ikke ble gjort vesentlige endringer i forbindelse med revideringen i 2019. Det er betryggende at kommunedirektøren i Overhalla anser det som sitt ansvar, også de tjenestene som kommunen får utført fra vertskommunen.

Etter revisors vurdering beskriver ikke selve samarbeidsavtalen hvilke oppgaver og myndighet vertskommunen har for å sikre informasjonssikkerhet og personvern, Den viser til leveranseavtale, som er vedlegg til samarbeidsavtalen.

Leveranseavtalen, vedlegget til samarbeidsavtalen blir nærmere presentert og vurdert i neste delkapittel.

Etter revisors vurdering følges ikke samarbeidsavtalen opp med rapportering og samhandling som systematisk ivaretar informasjonssikkerhet og personvern.

Etter det revisors vurdering ivaretas samhandlingen i praksis, ved at det er tett samarbeid mellom IT-leder i Overhalla og IT-tjenenesten i vertskommunen. Det er årlig kontaktmøte på kommunedirektørnivå, men det handler i hovedsak om budsjettspørsmål og i liten grad informasjonssikkerhet, personvern, evaluering og forbedring. Det pågår dialog om revidering av samarbeidsavtalen og tilhørende avtaler, men det er ikke iverksatt konkret arbeid med dette.

Punktene i samarbeidsavtalen om felles utviklingsarbeid, IKT-strategier og sikkerhetsstrategier, er ikke fulgt opp, og det gjelder heller ikke etablering av e-fagråd.

3.4 Leveranseavtale

I dette delkapitlet presenterer vi innhold i leveranseavtalen, og intervjuinformasjon om avtalen.

3.4.1 Funn

Leveranseavtalen er datert 27. mars 2019, og er vedlegg til samarbeidsavtalen. Leveranseavtalen utdyper punkt 3 i samarbeidsavtalen, *oppgaver som legges til vertskommunen*. I leveranseavtalen fremgår det at det også vil være tilleggsavtaler som regulerer kjøp/salg av arbeidskraft samt tilleggstjenester. Videre vises det i leveranseavtalen til at det er utarbeidet egen databehandleravtale som regulerer rettigheter og plikter etter personvernlovgivningen mellom Behandlingsansvarlig (Overhalla kommune) og Databehandler (Namsos kommune). Vi har sett om leveranseavtalen ivaretar de fire grunnprinsippene, slik de er definert fra NSM.

Det framgår i punkt 2 i avtalen at med IKT infrastruktur menes de tekniske løsningene som kreves for å ha et funksjonelt IKT- system i kommunene.

IT-tjenesten i vertskommunen forteller at de ikke har stor kjennskap til leveranseavtalen. I likhet med samarbeidsavtalen, forteller de at det er et samarbeid som har vokst seg fram, uavhengig av avtalene, og at det er behov for å gjøre endringer av avtalen. Det er særlig behov for mer dokumentert oversikt over hva som er felles for kommunene og hva Overhalla har ansvar for selv.

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

Punkt 5 i leveranseavtalen handler om maskinvare. Her er lagringsløsninger (server), skriver- og kopiløsning og løsning for brukerutstyr beskrevet. Når det gjelder brukerutstyr, går det fram at pc, nettbrett og tilbehør er den enkelte kommunes ansvar, men forutsettes anskaffet i tråd med IT-avdelingens anbefalinger og i tråd med felles innkjøpsavtaler. I punkt 7 er telefonløsning omtalt. Det går fram at Namsos kommune har ansvar for enhetlig kommunikasjon i samarbeid med eksterne leverandører. Hovedbærer (enheter) for talekommunikasjon er mobiltelefon og fasttelefon (IP). Forutsetning for enhetlig kommunikasjon er at alle deltakerne i leveranseavtalen har felles kontostruktur hos leverandørene og i IT-løsningene.

Både IT-leder i Overhalla og IT-tjenesten forteller at han har oversikt over Overhalla kommunes enheter og sørger for innlevering av utstyr ved ansattavgang. Utstyret er rullet inn i Intune.[17]
Når det gjelder programvare, punkt 8 i avtalen, er det brukerlisens for Office365 for alle brukere. Den enkelte kommune er ansvarlig for inn- og utmelding av brukere. Økning i uttak av lisenser kan skje fortløpende, men reduksjon kan skjer kun ved årlig rapportering. Videre, går det fram at oppvekstområdet har egne lisensavtaler. Det er en porteføljeoversikt over felles programvare i avtalen, som viser programvare, fagområde og systemansvarlig. Navnene på systemansvarlig er ikke ansatte i Overhalla kommune per i dag.

I intervju med IT-leder ble det vist til sikkerhetsplattformen Heimdal. IT-leder installere noe, ellers har Heimdal en portefølje med programvare (hvitlisting) som ansatte kan installere selv. IT-tjenesten har godkjent det. IT-tjenesten bekrefter at det er en streng kontroll på dette, og at ansatte ikke kan installere noe uten at det inngår i porteføljen.
Kapittel 3 i leveranseavtalen handler om brukerkatalog og områder. I dette punktet beskrives tilgangsløsninger, og at alle som bruker vertskommunens løsninger inngår i en felles brukerkatalog: Active Directory (AD).[18] AD definerer hvem som er aktive brukere av løsningene, hvilken del av organisasjonen de tilhører, tilhørighet i grupper og tilgang til de ulike dataområder. Videre går det fram at det er den enkelte kommune som er ansvarlig for å melde inn og ut brukere av brukerkatalogen ved hjelp av et felles system.[19]

IT-leder forteller at det er den enkelte kommune som melder inn og ut brukere av AD. Dette skjer gjennom HRM-systemet (lønnssystemet). Ansatte som slutter, fjernes fra dette systemet og tilgangene blir også fjernet. Tilgang til fagsystemer er utenfor AD. IT-leder har det overordna ansvaret, og har et årshjul han følger når han gjennomgår og sjekker tilganger. Han sjekker tilganger fire ganger i året. Dette gjelder tilganger som ligger utenfor AD.

IT-leder sier at det er kontroll på systemene og programmene som ligger i AD. Tilganger innenfor skole er også styrt av AD. Elevers tilganger er styrt gjennom folkeregisteret, der det foregår månedlig vasking. Ved flytting, deaktiveres og slettes kontoene.

[17] En skybasert tjeneste for endepunktsadministrasjon (UEM) som sikrer og styrer apper, mobilenheter, PC-er og virtuelle maskiner (Microsoft).

[18] En sentralisert katalogtjeneste fra Microsoft som brukes til å administrere brukere, datamaskiner, sikkerhetsrettigheter og nettverksressurser i et Windows-miljø (digi.no)

[19] BOSS – Bruker Oppretting Satt i System

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

Ovenfor viste vi til hva avtalen sier om brukerutstyr, og at det i punkt 5 går fram at pc, nettbrett og tilbehør er den enkelte kommunes ansvar, men forutsettes anskaffes i tråd med IT-avdelingens anbefalinger og i tråd med felles innkjøpsavtaler.

Når det gjelder anskaffelser, forholder Overhalla seg til fylkeskommunale avtaler på utstyr, ifølge IT-leder. Ingen kan kjøpe utstyr, utenom IT-leder. IT-tjenesten Namsos kommune har ikke en sentral rolle her, men de forteller at de har en del kontakt med controller i Overhalla når det gjelder rammeavtaler med fylkeskommunen. På grunn av rammeavtale for IT-utstyr og programvare bør kommunene være samkjørt, ifølge IT-tjenesten.

Controller i Overhalla forteller at anskaffelsesprosessen for IT-utstyr og programvare kan være kjørt av andre aktører, som andre kommuner og fylkeskommunen. Når det gjelder fagprogrammer, er det fagledelsen som signerer på sine avtaler. Etter anbudet er det ulikt hvordan han blir koblet på og hvordan avtalene følges opp. En gang i året sendes det forespørsel til enhetene om å gjennomgå behandlingsoversikten og se om den er oppdatert (gjelder egentlig databehandleravtaler).
Leveranseavtalen inneholder ikke bestemmelser om IKT-arkitektur eller sikkerhetsoppdateringer.
Ifølge IT-leder har ikke kommunen et flytskjema over IKT-arkitekturen, men en beskrivelse av hvordan dette fungerer. Det er bra oversikt over dette, mener han. Når det gjelder sikkerhetsoppdatering, er det sentral styring med sikkerhetsoppdateringer, ifølge IT-leder. Kommunen styrer selv, skytjenester som ligger utenfor felles system og egne nettverkssegment. Det er leverandørene som sørger for oppdatering av programvare. Ikke alt kan styres, og IT-leder forteller at de ligger litt etter med oppdatering, feilretting og lukking av sikkerhetshull.

Kontroll og av sikkerhetstilstand og ledelsens gjennomgang (oppdage)

I leveranseavtalens punkt 5, om maskinvare, går det fram at det er satt opp brannmurer for hovednett og gjestenett. Videre står det at bytte av brannmur følger en utskiftingsplan.

I oversikten over hva som inngår som programvare og lisenser, i punkt 8, framgår det at årlig vedlikehold av brannmur, antivirus og sikkerhetsløsning inngår i avtalen. Videre inngår sikkerhetssertifikater knyttet til fellesløsninger, mens lokale sertifikater må ivaretas av kommunen selv.

Punkt 9 i driftsavtalen gjelder kompetanse og driftsressurser. IT-tjenesten i Namsos har ansvar for å drifte den definerte, tekniske infrastrukturen. Det framgår at tjenesten har vanlig kontortid. Tiltak for å sikre at brukerretta tjenester er operative utenom kontortid, inngår ikke i avtalen.

IT-tjenesten sier at de daglig er inne og kontrollerer alarmer og automatiske rutiner dersom det skjer noe. Det er ikke noen som har det som dedikert oppgave, men det er driftsleder eller en annen som gjør det.

Kapittelet 3.3, om samarbeidsavtalen, går det fram at avtalene i liten grad gjennomgås av ledelsen for informasjonssikkerhet og personvern.

Håndtere, gjenopprette og lære av hendelser (håndtering og gjenoppretting)

Revisor observerer ikke innhold i leveranseavtalen som beskriver hendelseshåndtering og gjenoppretting. Revisor observerer heller ikke at avtalen omtaler prioritering av hva som skal gjenopprettes først, eller hvem som har ansvar for gjenoppretting.

Som vi beskrev ovenfor, er det ikke 24/7-vaktordning for deltakerkommunene. IT-tjenesten forteller at det er automatikk i systemene, med isolering av PC-ene. Ansatte i tjenesten ser an situasjonen og gjenoppretter den påfølgende dagen.

Varslingsrutiner mellom kommunene, var tema på beredskapsøvelsen. Hvis det de øvde på hadde skjedd, var erfaringen at de burde sitte sammen fysisk. Det er viktig å øve på kommunikasjonskanal utenfor Microsoft også, for ikke å glemme den når noe skjer, ifølge IT-tjenesten.

På spørsmål om det er en beredskapsplan for IT-hendelser innenfor vertskommunesamarbeidet, er tilbakemeldingen at det er det ikke.

3.4.2 Revisors vurdering

- Kommunen bør ha inngått leveranseavtale med Namsos kommune, som ivaretar
    - 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)

Etter revisors vurdering ivaretar leveranseavtalen delvis tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern.

Leveranseavtalen har ikke blitt oppdatert etter 2019, da den ble revidert sammen med samarbeidsavtalen. Det er ikke betryggende at vertskommunens IT-tjeneste knapt nok kjenner til avtalen. Etter revisors vurdering er framstår samarbeidet om tekniske og organisatoriske sikkerhetstiltak med liten grad av systematikk og dokumentasjon.

Etter revisors vurdering ivaretar leveranseavtalen delvis oversikt enheter, programvare og tilganger, men tjenestene som utføres for Overhalla kommune, er ikke forankret i avtalen.

Revisor bygger vurderingen på at kjennskapen til og bruken av avtalen ikke gjelder i den praktiske utføringen av tjenestene for Overhalla kommune. I praksis kan sikkerhet være bra, men de er ikke forankret i en avklart avtale.

Etter revisors vurdering berører leveranseavtalen i liten grad sikkerhet i anskaffelser, IKT-arkitektur og sikkerhetsoppdateringer (beskytte og oppdatere).

Etter revisors vurdering ivaretar Overhalla anskaffelser av utstyr selv, gjennom fylkeskommunens avtaler, eller samarbeid med andre kommuner på utstyr og programvare. Det er noe kontakt med vertskommunen. Heller ikke IKT-arkitektur eller sikkerhetsoppdateringer er berørt i avtalen, og det er uklart hva som skjer fra vertskommunen og hva Overhalla har selv.

Etter revisors vurdering inneholder leveranseavtalen kontroll av viktige sikkerhetstilstander ved at det er satt opp brannmurer for hovednett og gjestenett, og at årlig vedlikehold av brannmur, antivirus og sikkerhetsløsning inngår i avtalen. Utskifting av brannmur inngår i en utskiftingsplan

Etter revisors vurdering ivaretar vertskommunen sikkerhetsrutiner, men det er uklart hvordan brukerretta tjenester er sikret opprettholdelse utenom kontortid.

Etter revisors vurdering inneholder leveranseavtalen ikke beskrivelse av håndtering, gjenoppretting og læring av hendelser (håndtering og gjenoppretting).

Selv om det er mye automatikk i systemene, kan det framstå som at systemer kan være utsatte ved hendelser, blant annet siden det ikke er oppfølging hele døgnet. Revisor kan heller ikke se at avtalen, eller annen informasjon viser system som skal prioriteres ved hendelser, eller

hvem som har ansvar. Revisor vil trekke fram øvelsen som deltakerkommunene har hatt som positiv.

3.5 Databehandleravtale

I dette delkapitlet presenterer vi databehandleravtale og intervjuinformasjon om den.

3.5.1 Funn

Namsos kommune behandler data på vegne av behandlingsansvarlig (kommunedirektøren) i Overhalla kommune gjennom IKT-tjenenestene som vertskommunen kommunen yter for Overhalla kommune. Leveranseavtalen, som ble gjennomgått i forrige kapittel, hadde et punkt informasjonssikkerhet. Her blir det vist til databehandleravtale. Revisor har etterspurt og fått tilsendt to versjoner av databehandleravtale. Den første er mellom Overhalla kommune, ved behandlingsansvarlig og Midtre Namdal, som databehandler.[20] Den gjaldt fra 23.11.2018 – 31.12.2019. Den andre er mellom Overhalla kommune, ved behandlingsansvarlig og Namsos kommune, som databehandler. Den gjelder fra 01.01.2020 og har ikke tidfestet dato for utløp.

Den databehandleravtalen som gjelder fra 2020 regulerer behandlingsansvarlig og databehandlers ansvar og plikter, behandlingens område, system, formål, registrerte, opplysninger og behandlinger. Videre beskriver den databehandlers anledning til å bruke underleverandører. Gjeldende databehandleravtale er identisk med den forrige avtalen, med unntak av punkt 5, om behandlingens område, system, formål, registrerte, opplysninger og tekniske og organisatoriske tiltak. Her er det dels opplistet andre system i gjeldende avtale. Databehandleravtalen har to vedlegg: Vedlegg 1, om informasjonssikkerhet og vedlegg 2 om underleverandører. I vedlegget om informasjonssikkerhet er det opplista 38 minimumskrav.[21] 10 av disse er krysset av som ikke oppfylt, og beskrevet som under arbeid eller ikke fulgt opp. Det er de samme minimumskravene som i forrige avtale, unntatt for to krav.

I vedlegget om underleverandører, er det listet opp tre system og underleverandører.

Kommunedirektøren forteller at de har etterspurt en ny databehandleravtale fra Namsos kommune, men at han ikke kjenner til at det har kommet på plass.

[20] Samkommunen ble oppløst fra 1.1.2020, og erstattet av vertskommunesamarbeid.

[21] Artikkel 32

3.5.2 Revisors vurdering

- Kommunen må ha databehandleravtale med vertskommunen som sikrer informasjonssikkerhet og personvern i tråd med regelverket.

Revisor vurderer at kommunen har databehandleravtale med vertskommunen.

Etter revisors vurdering framstår ikke avtalen, og avtalens vedlegg, oppdatert i tråd med hva Overhalla kommune har etterlyst av behov.

4 KONKLUSJONER OG ANBEFALINGER

4.1 Konklusjon

I denne forvaltningsrevisjonen er følgende problemstillinger undersøkt:

- Har kommunen etablert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i regelverket?
- Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos kommune (vertskommune), som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern?

Revisors overordna konklusjon på den første problemstillingen er at Overhalla kommune har etablert sentrale elementer i et styringssystem for informasjonssikkerhet og personvern. Kommunens styrende dokumenter inneholder delvis sikkerhetsmål, sikkerhetsstrategi og beskrivelse av sikkerhetsorganisasjon, men revisor stiller spørsmål ved om dette har vært så forankret i organisasjonen. Ledelsessystemet (styrende dokumenter) for informasjonssikkerhet og personvern er gjenstand for revidering årlig, men inntrykket er at dette er enkel revidering som i hovedsak utføres IT-leder.

Kommunens system for internkontroll inneholder en stor del av de styrende dokumentene, prosedyrer og rutiner for informasjonssikkerhet og personvern. Noen dokumenter finnes også i systemet Elements (sak- og arkivsystem) og systemet for virksomhetsstyring, Framsikt. Revisor vil trekke fram at det i den nylig vedtatte, helhetlige ROS-analysen er tatt inn flere elementer som gjelder informasjonssikkerhet og personvern.

Overhalla kommune har personvernombud i egen organisasjon. Kombinasjonen mellom denne funksjonen og stillingen som HR-leder, kan utfordre uavhengigheten som funksjonen som personvernombud skal ha til kommunens ledelse. Funksjonen som personvernombud kommer dessuten i tillegg til full stilling som HR-leder, noe som kan medføre risiko for at det ikke er tilstrekkelig ressurser for å utføre funksjonen. Revisor vil likevel trekke fram at personvernombudet er oppmerksomt på dette, og informasjonsgrunnlaget i forvaltningsrevisjonen viser at hun bidrar med viktig støtte i personvernspørsmål for ledere i organisasjonen.

Det er etablert et system for behandlingsprotokoller, men det er noen mangler i noen av behandlingene for obligatoriske opplysninger. Kommunen har ikke et system for

databehandleravtaler, men databehandleravtaler blir i stor grad praktisert. Controller har en rolle her. Kommunen har praksis for å gjennomføre DPIA, men det er i mindre grad etablert et system for dette.

Revisor konkluderer med at det skjer opplærings- og informasjonstiltak knyttet til informasjonssikkerhet og personvern, men det er i liten grad satt i system. Kommunen har et arbeid på gang, med utforming av policy for bruk av kunstig intelligens (KI). Dokumentasjonen viser at det er etablert beskrivelser av bruk av KI i kommunen, som synliggjør nødvendigheten av varsomhet når det gjelder personvern og annen taushetsbelagt informasjon. Det er likevel viktig å ha oppmerksomhet på forsvarlig bruk av KI, for eksempel gjennom opplæringstiltak.

På den andre problemstillingen konkluderer revisor med at Overhalla kommune ikke har etablert tilfredsstillende avtaler med Namsos kommune som sikrer organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern. Utviklingen skjer raskt innenfor dette området, og nye sikkerhetsutfordringer oppstår kontinuerlig. Det er viktig at Overhalla har et avtaleverk med vertskommunen som er tydelig på ansvar og oppgaver. Oppfølgingen av vertskommune på informasjonssikkerhet og personvern er i hovedsak gjennom tilknytningen og kontakten IT-leder har med IT-tjenesten. Fraværet av systematikk og at oppfølgingen i hovedsak hviler på enkeltpersoner, gjør kommunen sårbar.

4.2 Anbefalinger

Revisor anbefaler kommunedirektøren i Overhalla kommune å iverksette en gjennomgang av styringssystemet for informasjonssikkerhet og personvern i kommunen som omfatter

- gjennomgang og revidering av styrende dokumenter, som involverer organisasjonen,
- vurdering av personvernfunksjonen med tanke på uavhengighet og ressurstilgang,
- vurdering av behov for rutiner og prosedyrer knyttet til behandlingsprotokoller, databehandleravtaler og vurdering av personvernkonsekvenser,
- utarbeiding av systematisk opplæring i informasjonssikkerhet og personvern, som også omfatter bruk av KI

Revisor anbefaler videre, kommunedirektøren i Overhalla kommune om å ta initiativ til gjennomgang og revidering av alle avtaler som gjelder tekniske og organisatoriske tiltak for å ivareta informasjonssikkerhet og personvern.

KILDER

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

Justis- og beredskapsdepartementet. Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). 25. juni 2004. FOR-2004-06-25-988. Lovdata.

Kommunal- og distriktsdepartementet. Forskrift om kontrollutvalg og revisjon. 17. juni 2019. FOR-2019-06-17-904. Lovdata.

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

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

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

Justis- og beredskapsdepartementet. Lov om nasjonal sikkerhet (sikkerhetsloven). 1. juni 2018. LOV-2018-06-01-24. Lovdata.

Nasjonal sikkerhetsmyndighet (NSM). 2020. Grunnprinsipper for IKT-sikkerhet. Nettside. Publisert 14. september 2020, oppdatert 6. mars 2025. (Åpnet 11. mai 2026).

Nasjonal sikkerhetsmyndighet (NSM). 2020. Veileder i sikkerhetsstyring. Nettside. Publisert 29. mai 2020, oppdatert 5. mars 2025. (Åpnet 11. mai 2026).

Jøsang, A. 2025. Cybersikkerhet – teknologier og styring. 3. utg.

Nettsider:

https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/

overhalla.kommune.no

Overhalla kommune: Lesetilgang til systemet for internkontroll – Compilo

5 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 behandling av personopplysninger (Personopplysningsloven)
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltnings-forskriften)
- Forskrift om virksomheters arbeid med forebyggende sikkerhet (Virksomhetsikkerhets-forskriften)
- Lov om kommuner og fylkeskommuner (kommuneloven)
- Veileder i sikkerhetsstyring, Nasjonal sikkerhetsmyndighet[22]
- NMSs grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet
- Virksomhetenes plikter knyttet til personvernregelverket, Datatilsynet

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. Sikkerhetsstyring er hjemlet i § 4-1; forebyggende sikkerhetsarbeid skal være en del av virksomhetens styringssystem. Virksomhetssikkerhetsforskriften definerer i § 3 kravet om at

[22]

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, IKT-sikkerhet 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.

<u>Sikkerhetsmål og sikkerhetsstrategi</u>

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[23] 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:

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

- 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.

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

Sikkerhetsloven § 4-2 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.

Personopplysninger

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.

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[24] 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.

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.

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

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

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.

Kommuner skal ha personvernombud. 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, anbefaler Datatilsynet, i tråd med artikkel 37-39 i personvernforordningen, at 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.

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

- Kommunen skal ha et styringssystem for sikkerhet som omfatter informasjons-sikkerhet, som angir
    - Sikkerhetsmål
    - Sikkerhetsstrategi
    - Sikkerhetsorganisasjon, hvor roller og ansvar framgår
- Kommunen skal føre protokoll over hvilke personopplysninger de behandler.
- Informasjonssikkerhet skal inngå i kommunens internkontrollsystem.
- Kommunen skal regelmessig gjennomføre og dokumentere risikovurderinger som grunnlag for informasjonssikkerhetstiltak.
- Kommunen må gjennomføre risikovurderinger og dokumenterte vurderinger av personvernkonsekvenser.
- Kommunen bør ha rutiner og prosedyrer for å redusere risiko for avvik og uønskede hendelser.
- Kommunen må ha system og rutiner som bidrar til at ansatte må melde avvik.
- Kommunen skal ha et personvernombud
    - nødvendig uavhengighet
    - nødvendige ressurser
- Kommunen skal ha rutiner for personvernombudets arbeid som sikrer involvering og regelmessig dialog med ledelsen.
- Kommunen må sørge for at ansatte får tilstrekkelig opplæring i informasjonssikkerhet.

Problemstilling 2: Har Overhalla kommune etablert tilfredsstillende avtaler med og oppfølging av Namsos 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 Namsos kommune, som er vertskommune for IKT-tjenester i Overhalla kommune. Vi er opptatt av om avtalen, eller avtalene ivaretar organisatoriske og tekniske tiltak for informasjonssikkerhet og personvern.

§§ 20-1 – 20-10 i kommuneloven handler om interkommunalt samarbeid gjennom vertskommunesamarbeid. Samarbeidet om IKT-tjenester som Overhalla kommune har med Namsos er et administrativt vertskommunesamarbeid, etter § 20-2. I administrative vertskommunesamarbeid instruerer kommunestyret kommunedirektøren i egen kommune til å delegere myndigheten til kommunedirektøren i vertskommunen.

En samarbeidskommune kan gi vertskommunen instruks om hvordan den delegerte myndigheten skal utøves i saker som bare gjelder samarbeidskommunen eller dens innbyggere.

Samarbeidsavtale (vertskommuneavtale)

I § 20-4 i kommuneloven heter det at, når et vertskommunesamarbeid opprettes, skal det inngås en skriftlig samarbeidsavtale mellom deltakerne i vertskommunesamarbeidet. I tredje ledd, bokstav c. framgår det at samarbeidsavtalen skal inneholde hvilke oppgaver og hvilken myndighet som skal legges til vertskommunen. I bokstav e. heter det at det skal framgå hvilke av vertskommunens vedtak deltakerne skal underrettes om.

I denne problemstillingen knytter vi Overhalla kommunes oppfølging av vertskommunen innen IKT-samarbeid til internkontrollbestemmelsene i kommuneloven.

I Kommunal- og distriktsdepartementets (KMD) Veileder om kommunelovens internkontrollbestemmelser uttrykkes det at kommunedirektøren i samarbeidskommunen fortsatt har ansvar for å følge opp samarbeidet, og at dette gjelder uavhengig av om det er et interkommunalt oppgavefellesskap, interkommunalt politisk råd, vertskommune, interkommunalt selskap eller aksjeselskap som utfører oppgaven. Ut fra dette har revisor utledet følgende kriterier:

- Det skal være en skriftlig samarbeidsavtale mellom vertskommunen og Overhalla kommune som
    - er oppdatert i henhold til gjeldende regelverk og sikkerhetsbehov
    - ivaretar hvilke oppgaver og myndighet som vertskommunen skal utføre for samarbeidskommunen, som sikrer informasjonssikkerhet og personvern
    - følges opp med rapportering og samhandling

Nasjonal sikkerhetsmyndighet har utgitt en veileder om grunnprinsipper for IKT-sikkerhet for å beskytte informasjonssystemer mot uautorisert tilgang, skade eller misbruk. Grunnprinsippene

fokuserer på teknologiske og organisatoriske tiltak, og hovedfokuset er på tilsiktende handlinger.

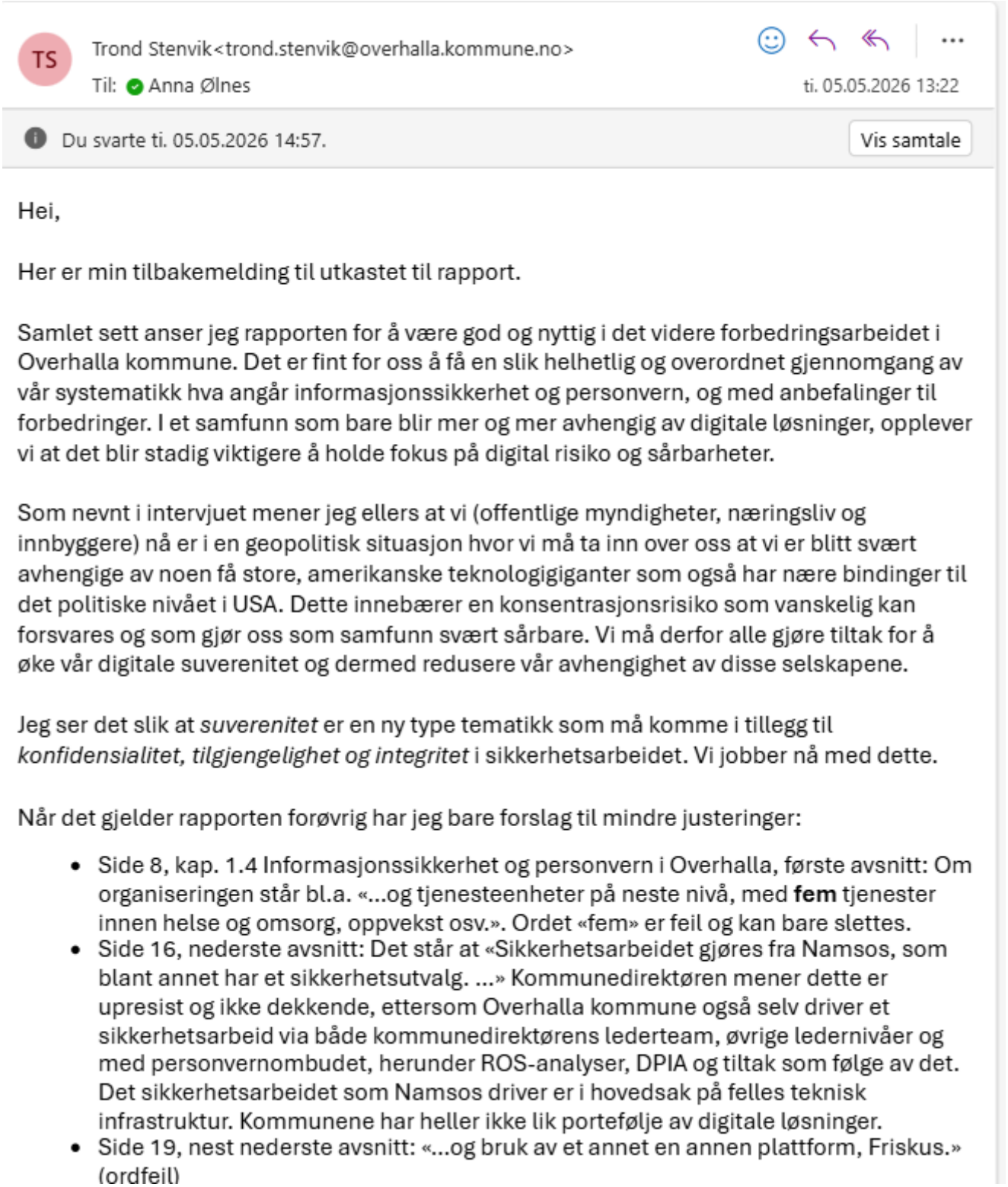
Grunnprinsippene for IKT-sikkerhet er delt inn i fire kategorier som er utgangspunkt for revisjonskriteriene som er gjengitt under. I denne forvaltningsrevisjonen vurderer vi om samarbeidsavtalen og underliggende avtaler ivaretar tekniske og organisatoriske tiltak for informasjonssikkerhet og personvern:

- Kommunen bør ha inngått leveranseavtale med Namsos kommune, som ivaretar
    - 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)

Artikkel 28 nr 1 i personvernforordningen handler om 'databehandler'. Dersom en behandling skal utføres på vegne av en behandlingsansvarlig [kommunedirektøren], skal den behandlingsansvarlige bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordning og vern av den registrertes rettigheter. I artikkel 28, nr 3 står det at behandling utført av en databehandler skal være underlagt en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett som er bindende for databehandleren med hensyn til den behandlingsansvarlige, og der gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt. I denne forvaltningsrevisjonen vurderer vi om:

- Kommunen må ha databehandleravtale med vertskommunen som sikrer informasjonssikkerhet og personvern i tråd med regelverket.

VEDLEGG 2 – UTTALELSE



TS

Trond Stenvik<trond.stenvik@overhalla.kommune.no>

Til: Anna Ølnes

ti. 05.05.2026 13:22

Du svarte ti. 05.05.2026 14:57.

Vis samtale

Hei,

Her er min tilbakemelding til utkastet til rapport.

Samlet sett anser jeg rapporten for å være god og nyttig i det videre forbedringsarbeidet i Overhalla kommune. Det er fint for oss å få en slik helhetlig og overordnet gjennomgang av vår systematikk hva angår informasjonssikkerhet og personvern, og med anbefalinger til forbedringer. I et samfunn som bare blir mer og mer avhengig av digitale løsninger, opplever vi at det blir stadig viktigere å holde fokus på digital risiko og sårbarheter.

Som nevnt i intervjuet mener jeg ellers at vi (offentlige myndigheter, næringsliv og innbyggere) nå er i en geopolitisk situasjon hvor vi må ta inn over oss at vi er blitt svært avhengige av noen få store, amerikanske teknologigiganter som også har nære bindinger til det politiske nivået i USA. Dette innebærer en konsentrasjonsrisiko som vanskelig kan forsvares og som gjør oss som samfunn svært sårbare. Vi må derfor alle gjøre tiltak for å øke vår digitale suverenitet og dermed redusere vår avhengighet av disse selskapene.

Jeg ser det slik at *suverenitet* er en ny type tematikk som må komme i tillegg til *konfidensialitet, tilgjengelighet og integritet* i sikkerhetsarbeidet. Vi jobber nå med dette.

Når det gjelder rapporten forøvrig har jeg bare forslag til mindre justeringer:

- Side 8, kap. 1.4 Informasjonssikkerhet og personvern i Overhalla, første avsnitt: Om organiseringen står bl.a. «...og tjenesteenheter på neste nivå, med **fem** tjenester innen helse og omsorg, oppvekst osv.». Ordet «fem» er feil og kan bare slettes.
- Side 16, nederste avsnitt: Det står at «Sikkerhetsarbeidet gjøres fra Namsos, som blant annet har et sikkerhetsutvalg. ...» Kommunedirektøren mener dette er upresist og ikke dekkende, ettersom Overhalla kommune også selv driver et sikkerhetsarbeid via både kommunedirektørens lederteam, øvrige ledernivåer og med personvernombudet, herunder ROS-analyser, DPIA og tiltak som følge av det. Det sikkerhetsarbeidet som Namsos driver er i hovedsak på felles teknisk infrastruktur. Kommunene har heller ikke lik portefølje av digitale løsninger.
- Side 19, nest nederste avsnitt: «...og bruk av et annet en annen plattform, Friskus.» (ordfeil)

- Side 23, nest nederste avsnitt: «Personvernombudet er ikke komfortabel med kobinasjonen av å være personvernombud og HR-leder, og ser helst at noen andre utfører personvernombudsfunksjonen.» HR-leder mener hun ikke har sagt det slik, men at temaet har vært drøftet med kommunedirektøren og hvor hun stilte spørsmål ved oå inneha de to rollene, sett opp mot Datatilsynets presisering om uavhengighet for personvernombudet.

Takk for arbeidet og rapporten så langt!

Med vennlig hilsen
Trond Stenvik
Kommunedirektør
Overhalla kommune

Mobil: 97140392
overhalla.kommune.no

Overhalla kommune
- Positiv, frisk og framsynt

RM Revisjon Midt-Norge