ROMERIKE REVISJON IKS

FORVALTNINGSREVISJONSRAPPORT NR. 13-2025

INFORMASJONSSIKKERHET OG PERSONVERN

GJERDRUM KOMMUNE

NOVEMBER 2025

INNHOLD

Figuroversikt

Tabelloversikt

SAMMENDRAG

Romerike revisjon har gjennomført en forvaltningsrevisjon av informasjonssikkerhet og personvern i Gjerdrum kommune. Prosjektet ble bestilt av kontrollutvalget i Gjerdrum kommune den 14.10.2024 i sak 50/24. Formålet med undersøkelsen har vært å avdekke eventuelle svakheter i informasjonssikkerheten og behandlingen av personopplysninger i Gjerdrum kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

Hovedfunn

1. Overordnede styrende dokumenter for informasjonssikkerhet er ikke oppdatert, og roller og ansvar er ikke tilstrekkelig avklart.
2. Det mangler risikovurderinger innenfor enkelte tjenesteområder i kommunen.
3. Ledelsens gjennomgang av informasjonssikkerhet er ikke gjennomført.
4. Det er mangler i kommunens arbeid med å føre protokoll over behandling av personopplysninger, samt å dokumentere personkonsekvensvurderinger og databehandleravtaler.

Kommunen har overordnede dokumenter for informasjonssikkerhet, men disse er ikke oppdaterte i henhold til ny den nye styringsmodellen som ble vedtatt for DGI i mars 2025. Rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet ikke er tilstrekkelig avklart, særlig når det gjelder hvilket ansvar som er lagt til digitaliseringsteamet og hva som tillegges kommunalsjefer, enhetsledere og virksomhetsledere.

Kommunens digitaliseringsteam har i dag en sentral rolle i gjennomføringen av risikovurderinger og har opprettet et system for gjennomføring av risikovurderinger. Arbeidet med risikovurderinger ser imidlertid ikke ut til å omfatte alle tjenesteområdene i kommunen. Det er ikke gjennomført risikovurderinger i teknisk sektor. Kommunen har ikke en prosedyre for risikovurderinger som klargjør ansvaret for at disse gjennomføres og følges opp.

Det gjennomføres ikke ledelsens gjennomgang i kommunedirektørens ledergruppe, i henhold til etablerte standarder for informasjonssikkerhet og kommunens egne styrende dokumenter.

Revisjonen konkluderer med at Gjerdrum kommune i noen grad har sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret. Kommunen har et personvernombud og gjennomfører vurderinger av personvernkonsekvenser (DPIA). Flere av de gjennomførte DPIAene har imidlertid mangler knyttet til versjonslogg, uttalelser og aksept av restrisiko, samt leders signatur. Kommunen etablerte en behandlingsprotokoll for personopplysninger i 2022, men arbeidet med protokollen er ikke videreført siden 2023 og den fremstår som uferdig. Det er uklart hvem som har det overordnede ansvaret for at denne ferdigstilles

og vedlikeholdes. Kommunen kan ikke dokumentere databehandleravtaler for flere digitale læremidler.

Basert på det som kommer frem i undersøkelsen anbefaler revisjonen at kommunedirektør sørger for:

1. at kommunen oppdaterer styrende dokumenter, slik at det gis en tydelig beskrivelse av dagens styringssystem for informasjonssikkerhet
2. å tydeliggjøre og dokumentere oppgave-, rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet
3. å etablere rutiner og praksis for å gjennomføre, dokumentere og følge opp risikovurderinger av informasjonssikkerheten innenfor alle tjenesteområdene i kommunen
4. at ledelsens gjennomgang av informasjonssikkerhet gjennomføres årlig
5. at behandlingsprotokollen ferdigstilles, og at roller og ansvar knyttet til å oppdatere protokollen klargjøres
6. at alle databehandleravtaler dokumenteres
7. at DPIAer som gjennomføres dokumenteres i tilstrekkelig grad

1 INNLEDNING

1.1 Bakgrunn for prosjektet

Kontrollutvalget i Gjerdrum kommune bestilte i møte 14.10.2024 (sak 50/24) en prosjektplan for en forvaltningsrevisjon av informasjonssikkerhet og personvern. Prosjektplanen ble vedtatt 25.11.2024 (sak 58/24).

Innbrudd i en kommunes IT-systemer kan ha store konsekvenser. Det har vært flere hendelser på Romerike om bruk av digitale tjenester innenfor kommunal forvaltning, hvor applikasjoner uten tilstrekkelig sikkerhetsvurdering har behandlet sensitive personopplysninger. Østre Toten kommune ble utsatt for et dataangrep i 2021 hvor alle sikkerhetskopier i kommunen ble slettet og alle data ble kryptert. Dette gjorde at ingen av de 1300 ansatte i kommunen kunne bruke datasystemene og sensitive personopplysninger, blant annet fra helse- og omsorgstjenestene, NAV og barnevernstjenestene, kom på avveie (Datatilsynet 2022).

Gjerdrum har som ett av de ti målene i kommuneplanens samfunnsdel 2018-2030 at Gjerdrum skal være en digital kommune. Kommunen skal ifølge samfunnsdelen rustes til å utnytte ny teknologi innenfor alle tjenesteområder, delta aktivt i digitaliserings- og teknologiprosjekter, realisere fordeler med ny teknologi og sikre oppdaterte digitale kommunikasjonsplattformer.

Romerike revisjon gjennomførte i 2019 en forvaltningsrevisjon om digitaliseringsarbeidet i Gjerdrum kommune. En av problemstillingene i revisjonen handlet om i hvilken grad kommunen hadde en tilfredsstillende internkontroll for å sikre godt personvern og god informasjonssikkerhet. Revisjonen viste at det var gjennomført få risikovurderinger på området, og ingen på overordnet nivå i kommunen. Revisjonens vurdering var at det fremsto som noe uklart hvordan arbeidsfordelingen mellom kommunen og DGI var organisert når det gjaldt risikovurderinger. Videre viste undersøkelsen at kommunen ikke kunne dokumentere at det gjennomføres sikkerhetsrevisjoner av informasjonssystemet, slik forskriften krever.

1.2 Formål og problemstillinger

Formålet med undersøkelsen er å avdekke eventuelle svakheter i informasjonssikkerheten og behandlingen av personopplysninger i Gjerdrum kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

Undersøkelsen har følgende problemstillinger:

1. Har kommunen dokumentert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i lov, forskrift og etablerte standarder?
2. Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret i tilstrekkelig grad?

Problemstilling 1 undersøker om kommunen gjennomfører og dokumenterer risikovurderinger ved informasjonssikkerhetstiltak og anskaffelser av IT-systemer, har sikkerhetsmål og sikkerhetsstrategi,

har en sikkerhetsorganisasjon med klar rolle- og ansvarsfordeling, har praksis og rutiner som sikrer god tilgangskontroll, sørger for opplæring av ansatte om informasjonssikkerhet og evaluerer og lærer av hendelser.

Problemstilling 2 undersøker hvordan personopplysninger blir lagret og sikret i IT-systemene som brukes på skolene i Gjerdrum og i hvilken grad de ansatte ved skolene i kommunen er kjent med og etterlever kommunens retningslinjer og rutiner for personvern.

Avgrensninger
Kommunedirektørenes porteføljestyre i DGI vedtok 21.3.2025 en ny styringsmodell for DGI-samarbeidet. Den nye styringsmodellen er ment å løse utfordringer samarbeidet har hatt med langsomme beslutningsprosesser, uklare kommunikasjonslinjer og manglende ivaretakelse av lokale behov. Den nye styringsmodellen skal evalueres etter ett år for å vurdere modellens effekt og eventuelle justeringer (kommunedirektørenes porteføljestyre sak 25/4). Ettersom ny styringsmodell er iverksatt og skal evalueres våren 2026 går ikke denne undersøkelsen nærmere inn på hvordan styringsmodellen til DGI påvirker kommunens arbeid med informasjonssikkerhet og personvern. Kommunens forhold til DGI og underleverandører blir likevel omtalt der hvor det er relevant.

1.3 Metode

1.3.1 Generelt

Undersøkelsen er gjennomført i henhold til RSK 001 - Standard for forvaltningsrevisjon som er fastsatt av styret i NKRF - Kontroll og revisjon i kommunene. Standarden definerer hva som er god revisjonsskikk innen kommunal forvaltningsrevisjon. Arbeidet er kvalitetssikret i henhold til Romerike revisjon IKS sine interne rutiner.

I tråd med RSK 001 punkt 16 har revisjonen vurdert validiteten og reliabiliteten i datagrunnlaget. Dokumentanalyse gir tilgang til formelle retningslinjer, rutiner og strukturert informasjon, mens intervju bidrar med innsikt i praktisk gjennomføring, opplevde utfordringer og nyanser som ikke nødvendigvis fremgår av skriftlig materiale. For å styrke validiteten i datagrunnlaget er intervjudata sammenholdt med dokumentasjon der det er relevant, i tillegg har vi bedt om svar på skriftlige spørsmål. Intervjuene er gjennomført med personer som har oppgaver og ansvar på det reviderte området. Revisjonen mener derfor at datagrunnlaget er tilstrekkelig gyldig og pålitelig for å belyse problemstillingene.

1.3.2 Dokumentanalyse

Revisjonen har gjennomgått dokumentasjonen fra Gjerdrum kommune som er relevant for kommunens arbeid med informasjonssikkerhet og personvern. Dette omfatter blant annet strategidokumenter, rutiner, prosedyrer og planer.

1.3.3 Intervju

Revisjonen har gjennomført seks intervjuer:

- Fagansvarlig digitalisering og innovasjon
- Kommunalsjef oppvekst og psykisk helse
- Digital Pedagogisk Rådgiver

- Sikkerhetssjef i DGI
- Leder for sikkerhetsutvalget (IKT-SU)
- Personvernombud for Gjerdrum kommune

1.3.4 Spørsmål til kommunen

For å supplere innsamlet dokumentasjon og intervjudata har revisjonen sendt spørsmål til kommunen per e-post og har fått skriftlige svar på disse.

1.3.5 Verifiseringsprosesser

Oppsummering av intervju er sendt til de som er intervjuet for verifisering, og informasjon fra de verifiserte intervjureferatene er benyttet i rapporten. Rapporten er også gjennomgått i sin helhet av administrasjonen.

Revisjonen mener at gode verifiseringsprosesser knyttet til muntlige fremkommet data, og av rapporten i sin helhet, er viktig for å sikre gyldighet og pålitelighet i undersøkelsens datagrunnlag.

1.4 Kommunedirektørens uttalelse

Revisjonen mottok kommunedirektørs uttalelse til rapporten 4.11.2025. Kommunedirektøren takker for gjennomgangen og tilbakemeldingene knyttet til informasjonssikkerhet og personvern og ser rapporten som et viktig bidrag til å styrke kommunens sikkerhetspraksis og etterlevelse av gjeldende krav. Kommunedirektøren har noen kommentarer til rapportens beskrivelser. Blant annet vises det til at den nye styringsmodellen i DGI skal sikre at informasjonssikkerhet og personvern ivaretas bedre fremover. Kommunedirektørens uttalelse er gjengitt i vedlegg 1.

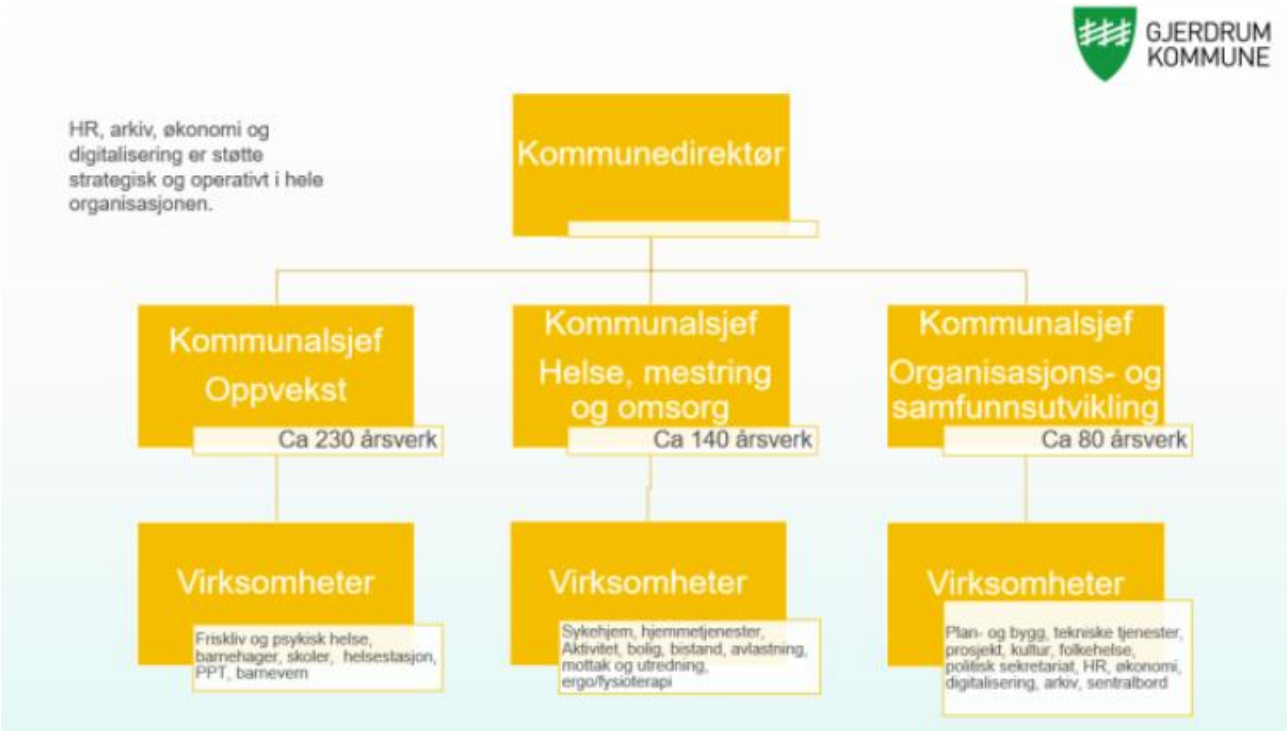
1.5 Revisjonskriterier

Revisjonskriterier er de krav og forventninger som kommunen vurderes opp mot. Kriteriene utledes fra lover og forskrifter, kommunestyrets vedtak og hva som anses som god forvaltningsskikk og faglig anerkjente normer på området. I dette prosjektet er revisjonskriteriene blant annet hentet fra kommuneloven, personopplysningsloven, eForvaltningsforskriften og etablerte standarder for informasjonssikkerhet og personvern. Kriteriene er nærmere presentert innledningsvis i kapittel 2 og 3, og i sin helhet i vedlegg 2 i rapporten.

1.6 Organisering i Gjerdrum kommune

Figur 1 viser den administrative organiseringen i Gjerdrum kommune. Kommunedirektørens ledergruppe, bestående av kommunalsjefer og relevante stabsressurser, utgjør det første administrative nivået, mens det andre administrative nivået består av virksomheter ledet av virksomhetsledere.

Figur 1 Administrativ organisering i Gjerdrum kommune, gjeldende fra 1.4.2024



Kilde: Kommunens hjemmeside

Gjerdrum kommune er en del av IKT-samarbeidet Digitale Gardermoen (DGI). DGI fungerer som kommunens IT-avdeling. Samarbeidet består av Romerikskommunene Gjerdrum, Nes, Hurdal, Eidsvoll og Nannestad. I 2022 overtok konsulent og IT-selskapet Sopra Steria driftsansvaret i DGI (DGI u.å).

Ny styringsmodell i DGI ble vedtatt av kommunedirektørene i kommunedirektørutvalget i slutten av april 2025 og sikkerhetsutvalget heter nå «IKT-Sikkerhetsforum». Ettersom det het «sikkerhetsutvalget» da revisjonen gjennomførte datainnsamling og intervju, har vi valgt å bruke det gamle navnet gjennomgående i rapporten.

1.7 Begrepsforklaringer

Personopplysninger: I personvernforordningen blir begrepet personopplysninger definert som enhver opplysning om en identifisert eller identifiserbar fysisk person. En identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet (personvernforordningen artikkel 4 nr. 1).

Behandling: Enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke. Dette kan for eksempel være innsamling, registrering, organisering, strukturering, lagring, tilpasning/endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring (personvernforordningen artikkel 4 nr. 2).

Behandlingsansvarlig: En behandlingsansvarlig er den virksomheten eller enheten som bestemmer formålet med, og midlene for, behandlingen av personopplysninger, jf. personvernforordningen (GDPR) artikkel 4 nr. 7. Kommunen ved kommunedirektør står ofte som behandlingsansvarlig i kommunenes personvernerklæringer. Dette gjelder også for personvernerklæringen til Gjerdrum kommune (udatert g).

Behandlingsprotokoll: En behandlingsprotokoll er en oversikt virksomheten er lovpålagt å føre, over sine behandlinger av personopplysninger, jf. personvernforordningen (GDPR) artikkel 30. Protokollen skal blant annet beskrive hvilke personopplysninger som behandles, til hvilke formål, med hvilket rettslig grunnlag, hvem som har tilgang til opplysningene, hvor lenge de lagres og hvordan sikkerheten ved behandlingen ivaretas.

Databehandler: Databehandler er en aktør som behandler personopplysninger på vegne av den behandlingsansvarlige. Dette innebærer at databehandleren ikke bestemmer formål eller andre vesentlige sider ved behandlingen, men følger instruksjoner fra den behandlingsansvarlige. Eksempler på databehandlere i en kommune er IT-leverandører, systemdriftsleverandører og leverandører av skytjenester som behandler data på vegne av kommunen.

DPIA (Data Protection Impact Assessment): DPIA er en vurdering av personvernkonsekvenser. Dette er en prosess som skal bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak (Datatilsynet udatert).

Informasjonssikkerhet og IKT-sikkerhet: Informasjonssikkerhet er en fellesbetegnelse og et overordnet begrep for krav til pålitelighet og sikkerhet knyttet til (sensitiv) informasjon (NAOB, u.å.) IKT-sikkerhet (informasjons- og kommunikasjonsteknologi) er et bredere begrep som inkluderer IT-sikkerhet, men som også omfatter sikkerhet i nettverk, kommunikasjon og bruk av digitale tjenester. IKT-sikkerhet handler dermed om både teknisk beskyttelse og trygg bruk av hele den digitale infrastrukturen.

Styringssystem: En kommunes styringssystem er en systematisk tilnærming til de sentrale aktivitetene for styring og kontroll i en virksomhet. I denne rapporten blir styringssystem for informasjonssikkerhet brukt synonymt med begrepene internkontroll, styring av informasjonssikkerhet og ledelsessystem, jf. Digdir sin veileder *Internkontroll i praksis – Informasjonssikkerhet*.

1.8 Rapportens oppbygning

I kapittel 2 vil problemstilling 1 om kommunens styringssystem for informasjonssikkerhet bli besvart. I kapittel 3 besvares problemstilling 2 om personvern i skolene. I kapittel 4 presenteres revisjonens konklusjon og anbefalinger.

2 STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET

2.1 Problemstilling og revisjonskriterier

Kommunen skal ha internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Videre bør internkontrollen være en integrert del av virksomhetens helhetlige styringssystem. (eForvaltningsforskriften § 15). Det finnes flere ulike standarder og rammeverk for styringssystem for informasjonssikkerhet. Digitaliseringsdirektoratet anbefaler at offentlige virksomheter i Norge baserer seg på standarden *Ledelsessystemer for informasjonssikkerhet – krav* (NS-ISO/IEC 27001). Se vedlegg 2 for en fullstendig beskrivelse av revisjonskriteriene.

Standarden stiller en rekke krav til gjennomføring av aktiviteter, for å sikre tilfredsstillende styring av informasjonssikkerhet. Revisjonen har valgt å se nærmere på fire krav til styringssystemet som revisjonen oppfatter som sentrale for å tilfredsstille kravet om en internkontroll som er systematisk og tilpasset kommunens størrelse, egenart, aktiviteter og risikoforhold (jf. kommuneloven § 25-1). Disse fire kravene er hvorvidt kommunen har på plass styrende dokumenter for informasjonssikkerhet (kap. 2.2.2), om kommunen har en klar oppgave-, rolle- og ansvarsfordeling på området (2.2.3), om det gjennomføres ledelsens gjennomgang av informasjonssikkerhet (2.2.4) og om kommunen har et system for gjennomføring av risikovurderinger, tiltak og aksept av risikonivå (2.2.5). Innledningsvis i kapittel 2 gis en oversikt over hvordan arbeidet med informasjonssikkerhet er organisert i Gjerdrum kommune.

For problemstilling 1 er følgende krav og forventninger til kommunen utledet:

Problemstilling 1	Krav og forventninger til kommunen
Har kommunen dokumentert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i lov, forskrift og etablerte standarder?	Kommunen skal ha → utarbeidet styrende dokumenter for informasjonssikkerhet, inkludert sikkerhetsmål og sikkerhetsstrategi → organisering med klar oppgave-, rolle- og ansvarsfordeling for informasjonssikkerhet → gjennomført ledelsens gjennomgang av informasjonssikkerhet årlig → et system for gjennomføring av risikovurderinger, etablering av tiltak og aksept av risikonivå

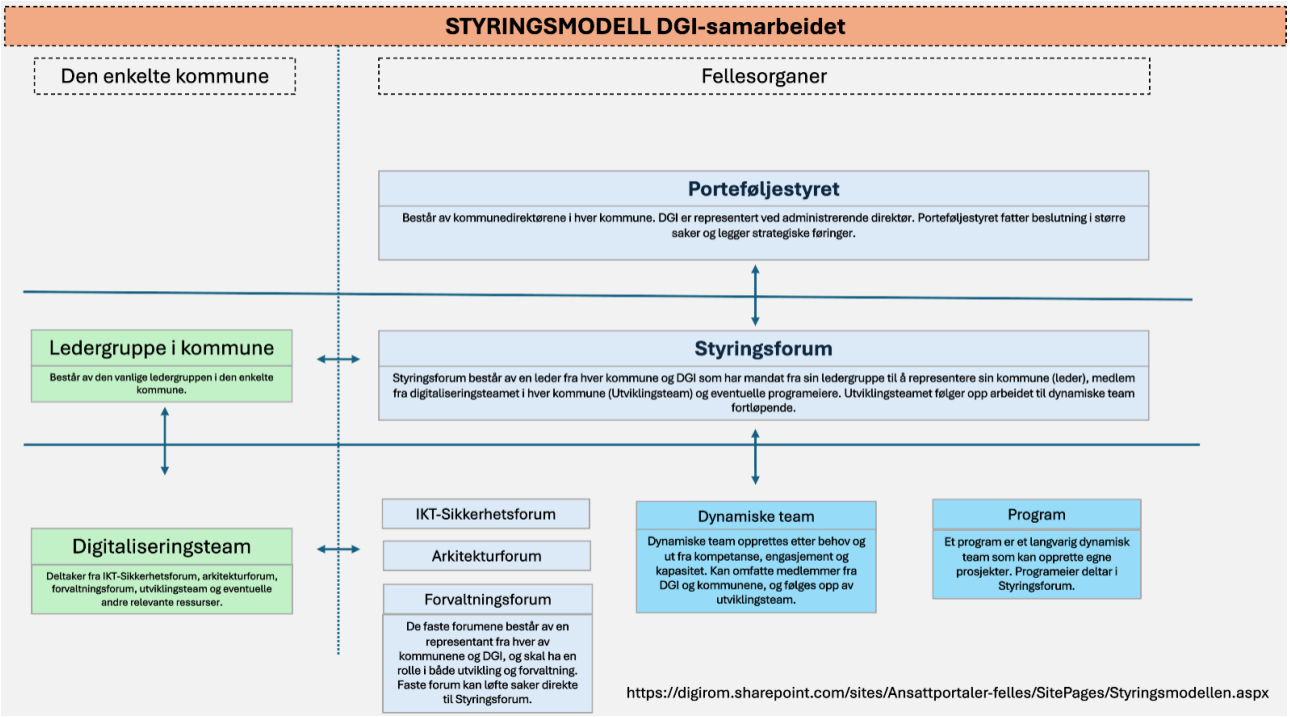
2.2 Kommunens styringssystem for informasjonssikkerhet

2.2.1 Organisering av arbeidet med informasjonssikkerhet i Gjerdrum kommune

Som tidligere nevnt er Gjerdrum kommune en del av IKT-samarbeidet Digitale Gardermoen (DGI), sammen med fire andre kommuner. DGI fungerer som kommunens IT-avdeling. DGI og eierkommunene samarbeider om retningslinjer og prosedyrer, i tillegg til større arbeidsoppgaver innenfor informasjonssikkerhet (Gjerdrum kommune 2024b).

Figuren under illustrerer forholdet mellom det felles DGI-samarbeidet på høyre side og kommunens egne fora for å ivareta arbeidet med informasjonssikkerhet på venstre side, slik det fremgår av ny styringsmodell vedtatt i porteføljestyret i DGI 21.3.2025.

Figur 2 Gjeldende styringsmodell i DGI-samarbeidet



Kilde: Digitale Gardermoen 2025a.

DGIs nye styringsmodell er delt inn i tre nivåer, hvor kommunedirektørenes porteføljestyre er øverste beslutningsorgan. Styringsforum er organisert under porteføljestyret og skal organisere og sikre gjennomføringen av initiativer fra alle de øvrige organene i styringsmodellen. Det tredje nivået består av tre faste forumer, samt dynamiske team (jf. figur 2). Ett av de faste forumene er IKT-sikkerhetsforum (tidligere IKT-sikkerhetsutvalget), som skal bidra til at krav til konfidensialitet, integritet og tilgjengelighet innenfor informasjonssikkerhet og personvern blir ivaretatt i DGI-kommunene (Digitale Gardermoen 2025).

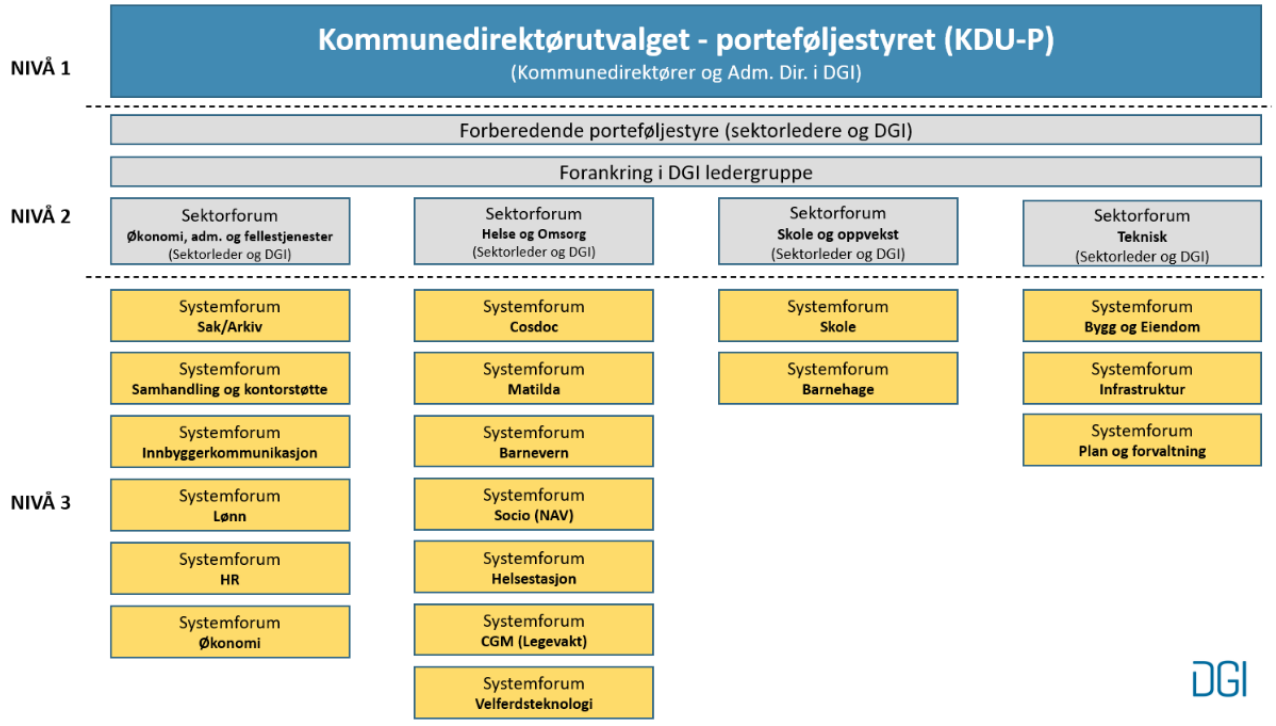
Den nye styringsmodellen skiller seg fra den gamle ved at den gamle modellen hadde 18 faste systemforum fordelt på fire sektorforumer (se figur 3). IKT-sikkerhetsforum/-sikkerhetsutvalget var

før et rådgivende organ, men er i den nye styringsmodellen blitt ett av tre faste fora som kan løfte saker til systemforum (intervju med sikkerhetssjef i DGI).

Rollen som IKT-sikkerhetsansvarlig i Gjerdrum kommune er beskrevet i kommunens sikkerhetsstrategi. Oppgavene til IKT-sikkerhetsansvarlig i kommunen er å være kommunens representant i IKT-sikkerhetsforum i DGI, være en ressursperson innen fagområdet og rådgiver internt (2021a).

Kommunens digitaliseringsteam har en sentral rolle i arbeidet med digitalisering og innovasjon i kommunen, og er dermed også sentralt i arbeidet med informasjonssikkerhet. Digitaliseringsteamets mandat er å prioritere, styre, følge opp og koordinere kommunens arbeid innenfor fagområdene digitalisering, teknologi og innovasjon med samarbeidspartnere som DGI og andre aktører (Gjerdrum kommune 2024a). Teamet er ledet av Fagansvarlig for digitalisering. Teamet består per august 2025 av to representanter fra administrasjonen, to fra virksomhetsområdet oppvekst og én representant fra virksomhetsområdet helse, mestring og omsorg. Digitaliseringsteamet har møter to ganger i uken, og de avholder ROS-møter hver fredag hvor også kommunens personvernombud deltar. Teamet har månedlige møter med kommunedirektørens ledergruppe, hvor også daglig leder i DGI deltar (intervju med fagansvarlig digitalisering og innovasjon).

Figur 3 Gammel styringsmodell i DGI-samarbeidet



Kilde: Digitale Gardermoen (2025b)

2.2.2 Styrende dokumenter for informasjonssikkerhet

Gjerdrum kommunes overordnede styrende dokumenter for informasjonssikkerhet er *Internkontroll i Gjerdrum kommune* (2024b), som beskriver kommunens internkontrollsystem, samt *Strategi for IKT sikkerhet og personvern for kommunene i Gardermoenregionen* (2021a), som er kommunens sikkerhetsstrategi. I tillegg har kommunen en instruks for informasjonssikkerhet og personvern (2023a).

Som ansvarlig for internkontrollen i kommunen skal kommunedirektøren utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering (kommuneloven § 25-1). Dokumentet *Internkontroll i Gjerdrum kommune* beskriver kommunens internkontroll og ble godkjent av kommunedirektørens ledergruppe (KGL) 19.3.2024. I tillegg til å beskrive den generelle internkontrollen i kommunen, har dokumentet et eget kapittel om personvern og informasjonssikkerhet. Her beskrives rollene og oppgavene til DGI som kommunens IT-selskap, kommunens digitaliseringsteam, personvernombudet og IKT-sikkerhetsansvarlig (Gjerdrum kommune 2024b).

Strategi for IKT sikkerhet og personvern for kommunene i Gardermoregionen er DGI-kommunens felles sikkerhetsstrategi. Gjeldende versjon av strategien (versjon 9) ble godkjent av kommunedirektørene i Gardermoregionen 17.2.2021. Strategien beskriver rollen til behandlingsansvarlig, personvernombud, IKT-sikkerhetsansvarlig og IKT-sikkerhetsutvalget. Videre står det at «utøvende dokumentasjon blir ivaretatt i felles prosedyrer, sjekklister og maler som omhandler informasjonssikkerhet og personvern. IKT-sikkerhetsutvalget har ansvar for å vedlikeholde disse dokumentene. Rådmannsforum godkjenner og vedtar prosedyrene, sjekklister og maler» (Gjerdrum kommune 2021a).

I dokumentets del 3.1 med overskriften «Sikkerhetsstrategi», oppgis det følgende:

> All behandling av informasjon for kommunene i DGI-samarbeidet skal utføres i samsvar med gjeldende lover og forskrifter når det gjelder:
>
> - **Konfidensialitet** - informasjonen er skjermet mot uautorisert innsyn i henhold til gjeldende lovverk, ut ifra graden av sensitivitet
> - **Integritet** - informasjonen er korrekt og kan ikke manipuleres av utenforstående
> - **Tilgjengelighet** - informasjonen er tilgjengelig for ansatte med tjenstlig behov, registrerte personer og offentligheten i samsvar med lov- og regelverk

Det går ikke eksplisitt frem i noen av de mottatte styrende dokumentene hva som er kommunens sikkerhetsmål. Kommunen opplyser i e-post til revisjonen at sikkerhetsmålene fremgår av sikkerhetsstrategiens kapittel 3.1. Målene er ifølge kommunen å sikre konfidensialitet, integritet og tilgjengelighet i all informasjonsbehandling, i tråd med kravene i eForvaltningsforskriftens § 15 (e-post til revisjonen 26.8.2025).

Revisjonen har mottatt dokumentet *Instruks for informasjonssikkerhet og personvern* som sist ble godkjent 04.9.2023 i kommunedirektørene porteføljestyre (KDU-P) (Gjerdrum kommune 2023a). Hensikten med instruksen er å sørge for at alle ansatte i kommunene i DGI-samarbeidet forstår sitt

ansvar ved bruk av kommunens IT-utstyr og -løsninger og bruker dette på en måte som forebygger at informasjon kommer på avveie, blir manipulert eller utilgjengelig. Det er KDU-P som er ansvarlig for prosedyren og at denne holdes ved like. Alle ansatte i kommunen er ansvarlige for å følge prosedyren, mens kommunedirektøren (eller den med delegert ansvar) er ansvarlig for at de ansatte er kjent med og følger prosedyren. IKT sikkerhetsansvarlig, personvernombud og personvernrådgivere i den enkelte kommune skal bistå dersom noen har spørsmål om prosedyren (Gjerdrum kommune 2023a).

Instruksen beskriver begreper innen informasjonssikkerhet, i tillegg til regler og krav på en rekke områder, herunder:

- Generelle regler for bruk og sikring av informasjon
- Bruk av IT-utstyr og digitale løsninger
- Arbeid utenfor kontoret og bruk av mobile enheter
- Digital kommunikasjon og dokumentasjon
- Håndtering av påloggingsinformasjon og tilgangsstyring
- Fysisk sikkerhet
- Rutiner ved avslutning av arbeidsforhold
- Arbeidsgivers innsynsrett
- Håndtering av sikkerhetslogger og sikkerhetshendelser
- Opplæring
- Rapportering av avvik

Videre har revisjonen mottatt følgende prosedyrer som kommunen har i sitt kvalitetssystem:

- Prosedyre for bruk av IKT-utstyr ved reise
- Prosedyre for bruk av databehandler
- Prosedyre for internvarsling av avvik
- Prosedyre for hendelses- og avviksbehandling i kvalitetssystemet
- Prosedyre for å starte behandling av personopplysninger

2.2.3 Klar oppgave-, ansvars- og rollefordeling for informasjonssikkerhet

Revisjonen legger til grunn at kommunen skal ha en organisering med klar oppgave-, rolle- og ansvarsfordeling for informasjonssikkerhet. Oppgaver, ansvar og roller knyttet til informasjonssikkerhet er som nevnt over beskrevet i kommunens overordnede internkontrolldokument og sikkerhetsstrategien. I tillegg er det for DGI-samarbeidet etablert en ny styringsmodell med virkning fra 21.3.2025, jf. figur 2 lenger opp.

I 2022 satte DGI ut driftsansvaret sitt til en ekstern leverandør (Digitale Gardermoen 2025c). Sikkerhetssjef i DGI forteller i intervju at dette innebærer at DGI ikke lenger står for driften av kommunenes IT-systemer. Leder i IKT-Sikkerhetsforum i DGI mener en utfordring med dette er at det i noen tilfeller er usikkert om det er kommunen, DGI eller DGIs underleverandør av driftstjenester som har ansvaret for de aktuelle oppgavene. Han etterlyser en oversikt over hvem som har ansvar for hva i forholdet mellom de tre partene. Hvem som har ansvar for å følge opp databehandleravtaler og underleverandører trekkes frem som eksempel hvor ansvarsfordelingen kan være uklar. Det er kommunen som er behandlingsansvarlig, men kommunen har ikke eget IT-driftspersonell. Det er

DGI som står for kommunikasjonen med leverandøren av driftstjenester (intervju med leder i sikkerhetsutvalget i DGI). Revisjonen kan ikke se at det går frem av kommunens styrende dokumenter hvem som har ansvar for å følge opp databehandleravtaler og underleverandører.

Som tidligere nevnt er rollene behandlingsansvarlig, personvernombud og IKT-sikkerhetsansvarlig beskrevet i kommunens sikkerhetsstrategi. Hvem som har rollen som IKT-sikkerhetsansvarlig fremgår ikke av kommunens styrende dokumenter. Gjerdrum kommune informerer i e-post 2.9.2025 at fagansvarlig digitalisering, som leder kommunens digitaliseringsteam, også innehar rollen som IKT-sikkerhetsansvarlig i kommunen.

I kommunens instruks for informasjonssikkerhet og personvern, samt prosedyrene revisjonen har mottatt, er ansvaret for etablering og revidering av prosedyrer gitt til DGI-samarbeidet. Samtlige av prosedyrene revisjonen har mottatt har en standardtekst som beskriver ansvarsforholdene. Ifølge prosedyrene er kommunedirektør eller den med delegert ansvar ansvarlig for at de ansatte er kjent med og følger prosedyrene.

Noen ansvarsområder fremstår imidlertid som uklare for revisjonen ved dokumentgjennomgangen. Ansvaret for å gjennomføre og å følge opp risiko- og sårbarhetsvurderinger fremgår ikke av dokumentene revisjonen har mottatt. Kommunen viser til digitaliseringsteamets ROS-kanal hvor alle nyanskaffelser skal risikovurderes. Videre har kommunen sendt revisjonen en beskrivelse av praksis knyttet til gjennomføring av ROS og DPIA ved anskaffelser av digitale tjenester. I beskrivelsen oppgis det at alle anskaffelser skal innom kommunens digitaliseringsteam. Videre vises det til at personen eller avdelingen som står for den aktuelle anskaffelsen gjennomfører ROS/DPIA sammen med digitaliseringsteamet (e-post 14.2.2025).

Intervjuene revisjonen har gjennomført, samt revisjonens gjennomgang av kommunens ROS-kanal bekrefter at digitaliseringsteamet har en sentral rolle ROS-arbeidet som gjøres i kommunen. Mangelen på dokumenterte ROS-analyser fra de ulike avdelingene/enhetene under virksomhetsområdet organisasjons- og samfunnsutvikling tyder imidlertid på at rutiner og praksis ikke sørger for at det gjennomføres ROS innenfor alle virksomhetsområdene i kommunen (se mer om ROS-analyser i kapittel 2.2.5).

Et annet område hvor ansvarsforholdene synes å være uklare er knyttet til kommunens behandlingsprotokoll. Kommunen har en prosedyre som beskriver ansvarsforholdene for å registrere personopplysninger i kommunens behandlingsprotokoll, men protokollen har ikke blitt oppdatert siden personvernombudets gjennomgang i 2023 (se mer om behandlingsprotokollen i kapittel 3.2.2).

2.2.4 Ledelsens gjennomgang av informasjonssikkerhet

I kommunens overordnede interndokument er en årlig gjennomgang i øverste ledelse, med tema personvern og informasjonssikkerhet, ett av elementene som er listet opp under beskrivelsen av kommunedirektørens internkontroll.

Også i kommunens sikkerhetsstrategi står det at ledelsens gjennomgang skal utføres årlig. Strategien inneholder videre en beskrivelse av hva som skal gjennomgås på ledelsens gjennomgang av informasjonssikkerhet. Gjennomgangen skal innebære å vurdere resultater fra sikkerhetsrevisjoner og kontroller, vurdere endringer med betydning for informasjonssikkerheten og

oppfølging/oppsummering/status av funn i ROS-analyser. Det nevnes ikke i strategien hvem som skal delta på gjennomgangen.

Revisjonen har ikke mottatt dokumentasjon som viser at ledelsens gjennomgang er gjennomført i henhold til krav og beskrivelser i de styrende dokumentene.

Sikkerhetssjef i DGI forteller i intervju at han tidligere har holdt en gjennomgang av punktene over for kommunedirektørenes porteføljestyre i DGI. Sikkerhetssjefen forteller at han har vært tydelig på at gjennomgangen ikke kan erstatte ledelsens gjennomgang for kommunedirektørenes ledergrupper i hver enkelt kommune.

I e-post til revisjonen bekrefter kommunen at det ikke er gjennomført ledelsens gjennomgang av informasjonssikkerhet i Gjerdrum kommune. Kommunen skriver videre at det arbeides med et årshjul for kommunedirektørens ledergruppe, hvor ledelsens gjennomgang av informasjonssikkerhet vil bli lagt inn (e-post 2.9.2025).

2.2.5 Risikovurderinger, tiltak og aksept av restrisiko

Rutinebeskrivelser for gjennomføring av risikovurderinger
For å få oversikt over mulige uønskede hendelser og bidra til at sikkerhets- og personvernarbeidet rettes mot områdene med høyest risiko er det viktig at kommunene identifiserer, analyserer og evaluerer risiko (Digdir 2025, KS 2025).

I kommunens sikkerhetsstrategi presiseres det det skal foreligge en skriftlig risikovurdering før behandling av personopplysninger eller virksomhetsdata settes i gang. Vurderingen skal som et minimum ta for seg behovet for kompetanse, virksomhetens prosesser samt krav til teknisk sikkerhet.

I kommunens overordnede internkontrolldokument vises det til at kommunen har prosedyrer for å sikre kommunen oppfyller krav knyttet til risiko- og sårbarhetsvurderinger (ROS) ved anskaffelse/innføring av systemer. Revisjonen har på forespørsel ikke mottatt en slik prosedyre. Revisjonen har imidlertid mottatt brukerveiledning for ROS og DPIA, hjelpeark til ROS, mal for gjennomføring av ROS og mal for gjennomføring av DPIA.

I dokumentet *Brukerveiledning ROS & DPIA* beskrives det hvordan gjennomføring av risiko- og sårbarhetsvurderinger (ROS) skal foregå. Først må det bestemmes hvem som skal være med på ROS. Det er ønskelig at personer som kjenner applikasjonen eller tjenesten skal være med. Dette kan for eksempel være personvernrådgiver, virksomhetsleder eller personvernombud. Deretter skjer selve identifiseringen av risiko(er). Her skal felles ROS-mal og hjelpeark brukes og det påpekes at databehandleravtale skal ses gjennom slik at man får informasjon og forståelse av applikasjonen (eller systemet) man risikovurderer. Sannsynlighet og konsekvenser inngår i vurderingen. Deretter opprettes tiltak. Et tiltak kan ifølge brukerveiledningen være å spesifisere hvordan applikasjoner skal brukes, eller opplæring i hvordan de skal brukes. Tiltakene bør følges opp jevnlig og legges inn i digitaliseringsteamets årshjul (Gjerdrum kommune udatert a). Årshjulet ligger i kommunens ROS-kanal i Microsoft 365 og oppdateres fortløpende.

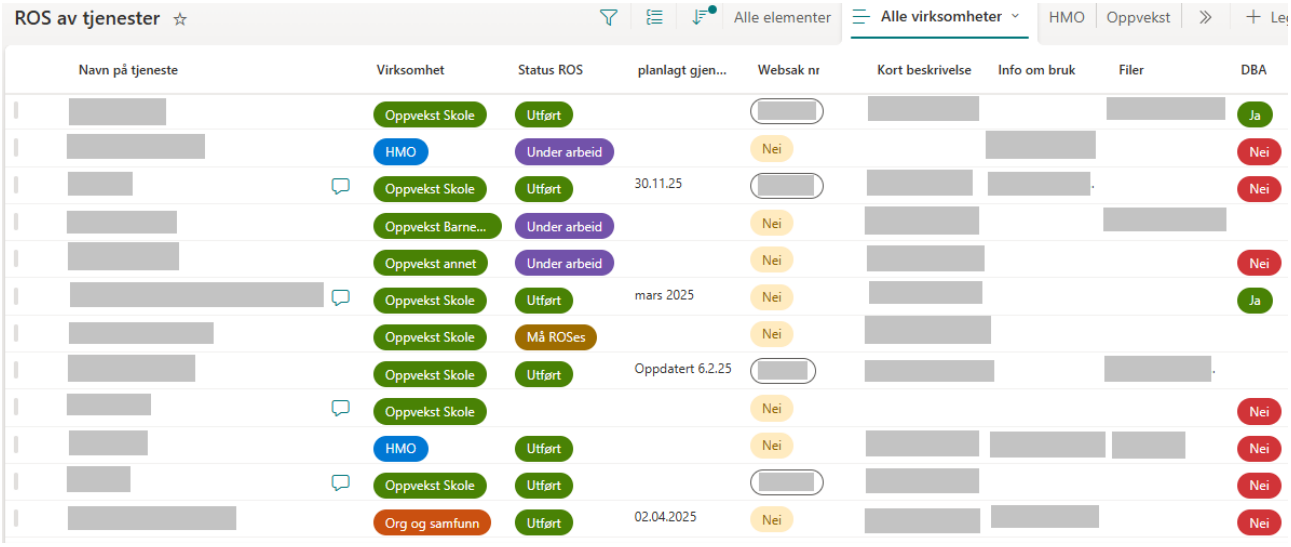
Dokumenterte risikovurderinger
Gjerdrum kommune har gjennomført overordnet ROS i 2019 og 2025. I overordnet ROS 2019 var ett av scenarioene svikt i IKT-systemer/-tjenester. I overordnet ROS 2025 var bortfall av internett/nettilgang DGI-tjenester og cyberangrep mot driftsleverandør blant scenarioene som ble gjennomgått. Kommunen opplyser til revisjonen i epost den 14.2.2025 at de i tillegg startet opp et arbeid med overordnet ROS i 2022, men at denne ikke ble ferdigstilt da kommunen ikke var tilfreds med rapporten. Fagansvarlig digitalisering og innovasjon forteller i intervju at han ikke er kjent med om det gjennomføres overordnede risikovurderinger av informasjonssikkerhet ut over kommunens scenariobaserte overordnede ROS.

Når det gjelder risikovurderinger på virksomhetsnivå, forteller fagansvarlig digitalisering at kommunen har oversikt over status for både påbegynte og gjennomførte ROS-analyser i digitaliseringsteamets ROS-kanal i Microsoft 365. Videre gjennomføres det risiko- og sårbarhetsanalyser på personvern, nyanskaffelser og teknisk ROS[1]. Ifølge digital pedagogisk rådgiver har digitaliseringsteamet ukentlige arbeidsmøter hvor teamet gjennomfører ROS-analyser.

Revisjonen har fått tilgang til kommunens ROS-kanal i Microsoft 365. ROS-analysene som ligger inne i denne kanalen er utført fra 30.9.2024 og oppdateres så vidt vi kan se fortløpende. Per september 2025 var 55 systemer/tjenester/prosesser lagt inn i ROS-kanalen. 29 av disse var på dette tidspunktet markert som utført. De øvrige tjenestene er markert med «Under arbeid», «Må ROSses», «Ikke godkjent», «Ingen persondata» og «Ikke i bruk». Per september 2025 var 20 av utførte ROS tilknyttet virksomhetsområdet oppvekst, 7 på virksomhetsområdet helse, mestring og omsorg og 2 er tilknyttet organisasjons- og samfunnsutvikling. De to ROS-analysene som er gjennomført innenfor organisasjons- og samfunnsutvikling er ROS av KI-verktøy. Kommunens ROS-kanal inneholder ikke ROS-analyser knyttet til tjenesteområder som plan- og bygg, vann og avløp. Figur 4 viser hvordan kommunens ROS-kanal ser ut.

[1] Risiko- og sårbarhetsanalyse som omhandler tekniske systemer og tjenester i kommunen.

Figur 4 Gjerdrum kommunes ROS-kanal



Kilde: Skjermutklipp av kommunens ROS-kanal. Revisjonen har sladdet navn på tjenesten og andre detaljer i grått.

Sikkerhetssjefen i DGI forteller i intervju at han deltar i gjennomføring av risikovurderinger sammen med kommunen ved behov. Hans inntrykk av ROS-arbeidet i Gjerdrum kommune er at de strever med å gjennomføre ROS i teknisk sektor. Teknisk sektor omfatter blant annet vann, kloakk og adgangskontroll, og sikkerhetssjefen vektlegger at skadepotensialet i denne sektoren er stort (28.4.2025).

Revisjonen har gjennomgått 23 ROS-analyser.[2] De fleste av disse er gjennomført etter kommunens mal. I flere av ROS-analysene er ikke versjonsloggen fylt ut og det fremgår ikke hvem som deltok i analysen og når den ble gjennomført eller revidert. I samtlige av de gjennomgåtte ROS-analysene er det identifisert risikoområder og gjort en vurdering av disse.

Tiltak for å dempe risiko

Digitaliseringsrådgiver forteller i intervju at det opprettes tiltak for å dempe risiko dersom en risikovurdering av en applikasjon viser høy risiko. ROS-malen kommunen benytter legger opp til at tiltak skal registreres for hvert av de identifiserte risikomomentene. Videre skal det registreres hvem som har ansvar for gjennomføringen av tiltaket, frist for gjennomføringen og status. Det er i de aller fleste ROS-analysene revisjonen har gjennomgått beskrevet risikoreduserende tiltak. Malen kommunen benytter skiller ikke mellom eksisterende og nye tiltak, og det er i flere tilfeller uklart om tiltakene som listes opp er tiltak som kommunen allerede har iverksatt eller om det er nye tiltak som skal iverksettes. For noen av ROS-analysene opplyses det om hvem som har ansvar for tiltakene,

[2] Revisjonen gikk kun gjennom ROS-analysene som ligger inne i kommunens ROS-kanal. For noen av tjenestene ligger det ikke inne skjema for ROS, men kun DPIA. For noen av tjenestene er det vist til en arkivsak. Revisjonen har ikke etterspurt ROS-analysene som er lagret andre steder enn i ROS-kanalen.

frist for gjennomføring og status, men dette mangler i flere av ROS-analysene. Forventet risikobilde etter gjennomførte tiltak er fylt ut i de fleste av ROS-analysene, men mangler i noen.

Som nevnt lenger opp skal tiltak ifølge kommunens brukerveileder for ROS følges opp jevnlig og legges inn i årshjul. Fagansvarlig digitalisering forteller i intervju at årshjulet digitaliseringsteamet benytter er nyanskaffet (9.4.2025). Revisjonen har sett årshjulet i kommunens ROS-kanal, men kan ikke se at det ligger tiltak knyttet i ROS i årshjulet per august 2025.

Aksept av restrisiko
Digitaliseringsrådgiver forteller i intervju at aktuell kommunalsjef godkjenner restrisiko etter at risikoreduserende tiltak er gjennomført. Praksisen med kommunalsjefens aksept av restrisiko bekreftes i intervju med konstituert kommunalsjef for oppvekst. Revisjonen kan imidlertid ikke se at det går frem av styrende dokumenter eller i brukerveiledningen for ROS hvem som har ansvaret for å akseptere restrisiko i kommunens ROS-analyser.

Kommunen skriver i e-post til revisjonen at ved ROS-analyser som gjennomføres i forbindelse med anskaffelser av digitale systemer har den som er ansvarlig for anskaffelsen ansvar for å ta stilling til eventuell restrisiko etter å ha gjennomført risikoreduserende tiltak. Ettersom alle nyanskaffelser går via digitaliseringsteamet vil teamet deretter gi tilbakemelding dersom de vurderer restrisiko som for høy. Digitaliseringsteamet kan også vurdere om saken tas videre med sikkerhetsrådet i DGI eller IKT-Sikkerhetsforum (e-post 14.2.2025). Det er ikke videre definert eller dokumentert hva som menes med «for høy» restrisiko.

ROS-malen som brukes i kommunen inneholder en kolonne som kalles «Aksept». Revisjonen antar at dette er aksept av restrisiko. Aksept er registrert for omtrent halvparten av ROS-analysene revisjonen har gjennomgått. ROS-malen inneholder ikke noe felt for signering av aksept, og det fremgår ikke av noen av ROS-analysene revisjonen har gjennomgått hvem som har akseptert restrisiko og når dette ble gjort.

2.3 Revisjonens vurdering

Revisjonens vurdering er at kommunen har utarbeidet styrende dokumenter for informasjonssikkerhet. Kommunen har blant annet en sikkerhetsstrategi som er felles for kommunene i DGI-samarbeidet. Etter revisjonens oppfatning kommer det ikke tydelig frem i strategien hva som er kommunens sikkerhetsmål. En ny styringsmodell ble vedtatt i DGI i mars 2025, men styringsdokumenter, inkludert instrukser og prosedyrer, er ikke oppdatert i henhold til den nye modellen.

Revisjonens vurdering er at kommunen i noen grad har klar oppgave, ansvars- og rollefordeling knyttet til informasjonssikkerhet, men at det er flere ansvarsområder som er uklare.

Revisjonen kan ikke se at ansvaret for gjennomføringen av risiko- og sårbarhetsvurderinger er nevnt i kommunens styrende dokumenter. Kommunen mangler også prosedyren for risiko- og sårbarhetsvurderinger, som er omtalt i styrende dokumenter. En konsekvens av dette kan være at ansvaret for å gjennomføre ROS-analyser ikke er avklart, og at det dermed ikke blir gjennomført jevnlige risiko- og sårbarhetsvurderinger i alle tjenesteområdene i kommunen. Mangelen på ROS-analyser innenfor teknisk sektor tyder på at dette er tilfellet i Gjerdrum kommune. Revisjonens

inntrykk er at digitaliseringsteamet i praksis har hatt hovedansvaret for gjennomføringen av ROS-analyser av kommunens systemer, applikasjoner og prosesser, men dette fremgår ikke av styrende dokumenter eller i beskrivelsene av digitaliseringsteamets mandat.

Videre har kommunen en prosedyre som beskriver ansvarsforholdet knyttet til registrering av personopplysninger i kommunens behandlingsprotokoll, men i praksis har ikke arbeidet med behandlingsprotokollen blitt videreført siden personvernombudets gjennomgang i 2023. Revisjonen stiller spørsmål ved om de ansvarlige for å registrere i og følge opp behandlingsprotokollen er klar over sitt ansvar.

Kommunen gjennomfører ikke ledelsens gjennomgang årlig, slik det blir anbefalt i etablerte standarder for informasjonssikkerhet og lagt til grunn i kommunens egne styrende dokumenter. Konsekvensen av dette kan være at arbeidet med informasjonssikkerhet i kommunen ikke er tilstrekkelig forankret i kommuneledelsen, og dermed at det ikke er tilstrekkelig styring og kontroll av området.

ROS-arbeidet som er gjennomført i digitaliseringsteamet, og da særlig innenfor virksomhetsområdet oppvekst og helse, mestring og omsorg, er etter revisjonens vurdering systematisert gjennom teamets ROS-kanal, ukentlige møter dedikert til gjennomføring av ROS og ved bruk av kommunens mal for ROS-analyser. Det er gjennomført en rekke ROS-analyser siden digitaliseringsteamet ble opprettet i 2024. Flere av ROS-analysene mangler imidlertid informasjon om når ROS-analysen ble gjennomført og hvem som deltok i analysen. Mangelfull loggføring av dato og deltakere kan gjøre det utfordrende å følge opp ROS-arbeidet, særlig ved endringer i bemanning.

Revisjonens gjennomgang av utførte risikoanalyser viser at det langt på vei etableres tiltak for å redusere risiko. Det fremstår imidlertid som uklart for revisjonen hvordan kommunen sikrer at tiltakene følges opp og hvor oppfølgingen av tiltakene dokumenteres.

Revisjonen kan ikke se at styrende dokumenter beskriver hvem som har ansvar for å akseptere restrisiko etter gjennomføringen av ROS og risikoreduserende tiltak. Det fremgår heller ikke av de gjennomførte ROS-analysene revisjonen har gjennomgått hvem som i praksis har akseptert risiko og når dette ble gjort.

3 PERSONVERN I SKOLEN

3.1 Problemstilling og revisjonskriterier

Enhver har rett til å bestemme over egne personopplysninger. Kommunen er ansvarlig for å sikre personopplysningene til både innbyggere som bruker kommunens tjenester og for egne ansatte. Dersom kommunen ikke sørger for at personopplysninger som er registrert i kommunens systemer er sikret i tilstrekkelig grad, kan opplysningene komme på avveie. Dette kan både ha konsekvenser for den enkelte og konsekvenser for kommunen i form av tap av tillit og gebyrer fra Datatilsynet (NOU 2022:11, 59).

Det har skjedd en digital omveltning i skolesektoren de siste ti årene, der en rekke digitale læremidler er tatt i bruk i undervisningen. Dette innebærer at det behandles flere personopplysninger i skolene enn før, og personopplysningene som samles inn om elever kan gi et omfattende og detaljert bilde av den enkelte elevs faglige og sosiale atferd gjennom årene elevene går på skolen. Barns rett til personvern er i dag prisgitt at kommunen gjør de nødvendige vurderingene av digitale læremidler som brukes i skolen og at de tar beslutninger som ikke bryter med personvernreglementet. Kommunen må blant annet sørge for å ha kontroll på ansvarsforholdet mellom kommune og leverandører, ha oversikt over hvilke personopplysninger som behandles og sørge for at personopplysningene til elevene ikke kommer på avveie (Datatilsynet 2025).

I dette kapitlet svarer vi på problemstillingen om hvorvidt kommunen har sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er tilstrekkelig sikret.

For problemstilling 2 er følgende krav og forventninger til kommunen utledet:

Problemstilling 2	Krav og forventninger til kommunen
Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret i tilstrekkelig grad?	Kommunen skal ha → utpekt et personvernombud med ansvar og oppgaver i tråd med GDPR artikkel 37- 39 → protokoll over hvilke personopplysninger kommunen behandler → rutiner og praksis som sikrer at kommunen har databehandleravtaler med eksterne leverandører som behandler personopplysninger → rutiner og praksis for å gjennomføre og dokumentere vurderinger av personvernkonsekvenser (DPIA)

3.2 Personvern i skolesektoren

3.2.1 Personvernombudet

Kommunen skal ifølge personvernforordningen utpeke et personvernombud som skal involveres i alle spørsmål som gjelder vern av personopplysninger. Oppgavene til personvernombudet er å gi råd om vern av personopplysninger, gi råd om vurderingen av personvernkonsekvenser og samarbeide med og fungere som kontaktpunkt for tilsynsmyndigheten. Personvernombudet skal blant annet kontrollere kommunens fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene. Personvernombudet skal rapportere direkte til det øverste ledelsesnivået (personvernforordningen § 37 - 39).

Gjerdrum har et personvernombud med 20 prosent stilling i kommunen. Personvernombudet er også ombud for tre andre kommuner, med Nes kommune som vertskommune.

Personvernombudets roller og oppgaver er beskrevet i kommunens sikkerhetsstrategi (Gjerdrum kommune 2021a). Noen av oppgavene er ifølge strategien å kontrollere at kommunens praksis er i tråd med personvernlovgivningen og kommunens interne prosedyrer knyttet til personvern, bidra til revisjon av kommunens behandlingsaktiviteter og gi råd om personvernkonsekvensvurderinger (DPIA) samt opplæring av ansatte og holdningsskapende arbeid (se også kapittel 2.2.3).

Revisjonen har intervjuet personvernombudet i Gjerdrum kommune. Ved intervjutidspunktet hadde hun hatt rollen som personvernombud i kommunen i litt over et år. Personvernombudet forteller i intervju at hun har brukt mye tid på å bli kjent med kommunene i sitt første år som personvernombud. I Gjerdrum kommune har hun deltatt i ukentlige ROS-møter og har deltatt på nyansattdag for å snakke om personvern. Nåværende personvernombud har imidlertid ikke vært involvert i arbeidet med behandlingsprotokollen i Gjerdrum kommune (e-post 1.5.2025). Kommunen har en egen side om personvernombudet på sine nettsider med ombudets roller og kontaktinformasjon. Kommunens personvernerklæring på nettsidene viser til at personvernombudet kan bistå innbyggerne ved spørsmål om personvern.

Personvernombudet skal rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige (personvernforordningen artikkel 38, tredje punkt). Personvernombudet har levert en årsrapport til kommuneledelsen i Gjerdrum kommune, datert 7.1.2025. I rapporten gjør personvernombudet rede for arbeidet med personvern i kommunen i løpet av det siste året, i tillegg til å komme med anbefalinger for det videre i arbeidet med personvern i kommunen. I rapporten nevnes blant annet arbeidet med ROS og DPIA på oppvekstområdet, deltakelse som personvernombud i ulike arbeidsgrupper, bistand i avvikshåndtering og ulike tiltak knyttet til opplæring og kompetanseheving (personvernombudet i Gjerdrum kommune 2025b).

3.2.2 Protokoll over behandling av personopplysninger

Etter personvernforordningen artikkel 30 skal den behandlingsansvarlige føre protokoll over behandlingsaktiviteter som utføres under deres ansvar.

Prosedyre for behandling av personopplysninger og ansvar for å oppdatere protokoll
Revisjonen har mottatt kommunens prosedyre for behandling av personopplysninger. Prosedyren skal etableres, holdes ved like, revideres og godkjennes av de ulike nivåene i DGI-samarbeidet (se

kapittel 2.2.1 for en beskrivelse av organiseringen i DGI). Kommunedirektør, eller den med delegert ansvar, er ansvarlig for at de ansatte er kjent med og følger prosedyren. Ifølge prosedyren er det kommunalsjef og enhets-/virksomhetsleder som har ansvar for at behandlingen av personopplysninger dokumenteres (Gjerdrum kommune 2022).

Ifølge Gjerdrum kommunes delegeringsreglement ligger det ansvaret for å følge opp behandlingsprotokollen hos HR-sjef, med støtte fra personvernombud og personvernrådgiver (Gjerdrum kommune). I e-post 26.8.2025 opplyser kommunen imidlertid at det er personvernombudet i samarbeid med digitaliseringsteamet som «håndterer» vedlikehold av dokumentasjon av behandling av personopplysninger. Dagens personvernombud har vært ansatt i stillingen siden starten av 2024 og oppgir i intervju at hun ikke har vært involvert i arbeid med behandlingsprotokollen så langt. Digital Pedagogisk rådgiver, som jobber med personvern på oppvekstområdet, har jobbet i kommunen siden desember 2023. Hun har heller ikke deltatt i arbeidet med behandlingsprotokollen (intervju med digital pedagogisk rådgiver).

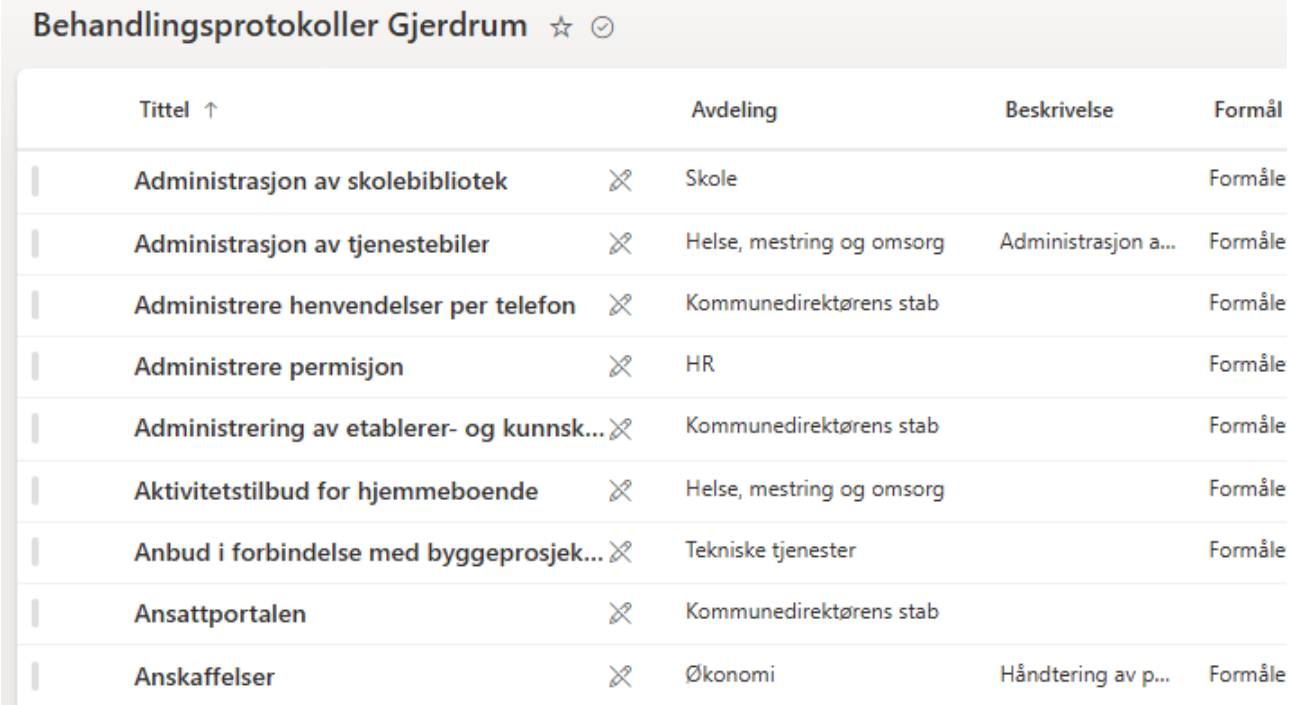
Personvernombudet påpeker i intervju på at behandlingsprotokollen burde gjøres bedre kjent og at kommunalsjef/enhetsleder bør ha fast ansvar for oppdatering og vedlikehold av protokollen.

Behandlingsprotokollen i Gjerdrum kommune
Behandlingsprotokollen skal etter personvernforordningen artikkel 30 inneholde:

a. navnet på og kontaktopplysningene til den behandlingsansvarlige
b. formålene med behandlingen
c. en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger
d. kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til
e. dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon
f. dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger
g. dersom det er mulig, en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak

Revisjonen har gjennomgått behandlingsprotokollen til Gjerdrum kommune, slik den forelå i august 2025 (se hvordan protokollen ser ut i kommunens nettløsning i figur 5). Ifølge kommunens prosedyre for å starte behandling av personopplysninger har kommunalsjef, enhets- og virksomhetsledere i kommunen ansvar for at behandlinger av personopplysninger registreres i protokollen. Under feltet «Avdeling» i protokollen (jf. figur 5) går det frem hvilken virksomhet, enhet eller avdeling behandlingen er registrert under. Protokollen inneholder ikke kontaktinformasjon til den behandlingsansvarlige ut over dette.

Figur 5 Behandlingsprotokollen til Gjerdrum kommune



Behandlingsprotokoller Gjerdrum

Tittel	Avdeling	Beskrivelse	Formål
Administrasjon av skolebibliotek	Skole		Formåle
Administrasjon av tjenestebiler	Helse, mestring og omsorg	Administrasjon a...	Formåle
Administrere henvendelser per telefon	Kommunedirektørens stab		Formåle
Administrere permisjon	HR		Formåle
Administrering av etablerer- og kunnsk...	Kommunedirektørens stab		Formåle
Aktivitetstilbud for hjemmeboende	Helse, mestring og omsorg		Formåle
Anbud i forbindelse med byggeprosjek...	Tekniske tjenester		Formåle
Ansattportalen	Kommunedirektørens stab		
Anskaffelser	Økonomi	Håndtering av p...	Formåle

Kilde: Skjermutklipp av kommunens behandlingsprotokoll.

Behandlingsprotokollen, som ligger i SharePoint, inneholder 17 punkter som skal fylles inn av den behandlingsansvarlige. Utfyllingsskjemaet i behandlingsprotokollen inneholder blant annet formålet med behandlingen/systemet, hvilke personopplysninger som registreres, om det registreres sensitive personopplysninger, hvem det registreres personopplysninger av, systemer som benyttes i behandlingen, kilde til opplysningene, hvem personopplysningene deles med og sletting og lagring av personopplysningene.

Ved revisjonens gjennomgang inneholdt behandlingsprotokollen 162 registreringer av behandlinger av personopplysninger. Registreringene er lagt inn i perioden 2022 til 2023, og det er ikke lagt inn nye registreringer etter dette. 16 av registreringene i behandlingsprotokollen er for skolene. Revisjonen har gjennomgått samtlige av disse.

Samtlige av de 16 behandlingene inneholder en beskrivelse av formålet med behandlingen, hvilke kategorier av personer det registreres personopplysninger om og hvilke opplysninger som registreres. 10 av de 16 registreringene inneholder informasjon om mottakere av personopplysningene. Se tabell 1 under for en oversikt over revisjonens gjennomgang av behandlingsprotokollen.

Det er ikke oppgitt informasjon om overføringer av personopplysninger til andre land. I e-post fra personvernombudet opplyses det om at tidligere personvernombud har rapportert om at informasjon om overføringene til tredjeland ikke er ført inn, da bidragsyterne fra første runde av protokollføring som regel ikke hadde informasjon om dette (e-post 1.5.2025).

Dersom mulig skal protokollen ifølge personvernforordningen inneholde informasjon om planlagte tidsfrister for sletting av de forskjellige kategoriene av personopplysninger. I samtlige registreringer er det lagt inn en standardtekst om at arkivverdige personopplysninger er lagret jf. arkivlovens bestemmelser og at sletting foretas iht. kommunens bevarings- og kassasjonsplan. Revisjonen har mottatt kommunens bevarings- og kassasjonsplan for Gjerdrum kommune. Planen beskriver hvilke opplysninger om enkeltelever som skal bevares, hvor opplysningene skal lagres og hvilket lovgrunnlag som ligger til grunn for bevaring av opplysningene. Planens del 2 består av en tabell med informasjon om blant annet grunnlag for bevaring (lovgrunnlag), bevaringstid og hvilket system opplysningene lagres i.

Dersom mulig skal det også gis en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Det er ikke lagt inn noe punkt om dette i behandlingsprotokollen, og revisjonen kan ikke se at det ligger informasjon om tiltak i de gjennomgåtte registreringene.

Tabell 1 Vurdering av innholdet i de registrerte behandlingene i behandlingsprotokollen på skoleområdet

Krav til innhold i behandlingsprotokolen jf. GDPR artikkel 30	Krav/ anbefalinger oppfylt?	Beskrivelse av behandlingene på skoleområdet
Navnet på og kontaktopplysningene til den behandlingsansvarlige	Delvis oppfylt	Behandlingene inneholder henvisning til avdeling eller tjeneste.
Formålet med behandlingen	Oppfylt	Samtlige av registreringene har registrert formålet med behandlingen.
En beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger	Oppfylt	I samtlige av behandlingene er det registrert hvem det er registrert personopplysninger av og hvilke opplysninger som er registrert.
Kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til	Delvis oppfylt	Mottakere av personopplysningene er registrert i 10 av de 16 registreringene.
Overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon (dersom relevant)	Ikke oppfylt	Ikke omtalt.
Planlagte tidsfrister for sletting av de forskjellige kategoriene av opplysninger (dersom mulig)	Oppfylt	Registrert en standardtekst på alle behandlingene, om at arkivverdige personopplysninger er lagret jf. arkivlovens bestemmelser og at sletting foretas iht. kommunens bevarings- og kassaksjonsplan.

Generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak (dersom mulig)	Ikke oppfylt	Ikke omtalt.

Personvernombudet i Gjerdrum kommune informerer i e-post til revisjonen 1.5.2025 at tidligere personvernombud gjennomførte et stort arbeid med behandlingsprotokollen i 2022. Dette var et felles prosjekt med flere DGI-kommuner, hvor personvernombudet reiste rundt i enhetene og registrerte behandlinger i protokollen.

Skjemaet for føring av behandlingsprotokollen inneholder registrering av dato for når personvernombudet kontrollerte registreringen og kommentarer fra personvernombudet til det som er registrert. Tidligere personvernombud har kontrollert og gitt tilbakemeldinger på registreringene i løpet av 2023. Flere av personvernombudets tilbakemeldinger handler om at det mangler registrering av systemer benyttet i behandlingen, jf. bokstav d. i artikkel 30. For noen av registreringene står det at protokollen er kopiert av en annen kommune og ikke er kontrollert av Gjerdrum kommune. Revisjonen kan ikke se at tilbakemeldingene fra personvernombudet er fulgt opp.

3.2.3 Databehandleravtaler

Etter personvernforordningen artikkel 28 skal behandlinger utført av en databehandler være underlagt en avtale eller et annet rettslig dokument som er bindende for databehandleren overfor den behandlingsansvarlige. Avtalen skal fastsette gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter.

Gjerdrum kommune har en prosedyre for bruk av databehandleravtale og en sjekkliste for databehandleravtaler (Gjerdrum kommune 2018a og 2019a). Både prosedyren og sjekklisten er utarbeidet av DGI og gjelder for alle kommunene i samarbeidet. Prosedyren for bruk av databehandleravtaler har til hensikt å sikre at det blir etablert databehandleravtaler når hele eller deler av behandlingen av personopplysninger settes ut til eksterne virksomheter. Prosedyren beskriver ansvars- og myndighetsforhold og retningslinjer for hva databehandleravtalene skal inneholde. Sjekklisten består av ulike skjema med spørsmål knyttet til innholdet i databehandleravtalen. Sjekklisten skal benyttes for å kontrollere at databehandleravtalen oppfyller kravene i personvernforordningen.

Kommunen opplyser om at inngåelse av databehandleravtale med leverandører er standard prosedyre ved alle anskaffelser. Digitaliseringsteamet gjennomgår aktuell leverandørs databehandleravtaler før den sendes til signering. Dersom databehandleravtalen er for lite spesifisert blir leverandøren bedt om å utdype og legge ved tilleggsinformasjon (e-post til revisjonen 14.2.2025).

Fagsjef digitalisering forteller i intervju at DGI har utarbeidet en felles mal for databehandleravtale for kommunene i DGI. En del av leverandørene ønsker å bruke sin egen databehandleravtale, og

fagsjef digitalisering forteller at de har godkjent dette dersom de inneholder/omtaler det samme temaene/punktene som kommunens mal.

Sikkerhetssjef i DGI forteller i intervju at malen til databehandleravtalen er lik for eierkommunene. DGI har myndighet til å undertegne databehandleravtaler av de tjenestene som forvaltes av DGI.

Revisjonen har gjennomgått kommunens dokumentasjon knyttet til de tolv ulike læringsmidlene som brukes i skolene i Gjerdrum kommune. Gjennomgangen viser at det mangler databehandleravtale for fire av disse læremidlene. På forespørsel har ikke revisjonen fått bekreftelse på at disse avtalene foreligger (e-post til revisjonen 18.6.2025). I kommunens tilbakemelding til rapporten, datert 4.11.25, oppgis det at alle digitale læringsmidler som er i bruk i dag har databehandleravtale. Manglende avtaler er imidlertid ikke dokumentert.

Samtlige av databehandleravtalene revisjonen har gjennomgått inneholder beskrivelser som tilfredsstiller kravene til innhold i databehandleravtaler, jf. personvernforordningen artikkel 28. Det eneste unntaket er at én av avtalene viser til et vedlegg med liste over underleverandører. Dette vedlegget ligger ikke i kommunens ROS-kanal.

3.2.4 Vurderinger av personvernkonsekvenser (DPIA)

Ifølge artikkel 35 i personvernforordningen skal kommunen gjennomføre vurderinger av personvernkonsekvenser (DPIA) dersom en behandling av personopplysninger vil medføre høy risiko for personers rettigheter og friheter. Denne vurderingen skal som et minimum inneholde en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålet med behandlingen, en vurdering av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålet, en vurdering av risiko for de registrertes rettigheter og friheter, og om de planlagte tiltakene for å håndtere risikoene og for å påvise at personvernreglene overholdes.

Revisjonen har mottatt kommunens mal for DPIA (udatert f), samt *Brukerveiledning for ROS og DPIA*, sistnevnte er tidligere omtalt i rapportens del 2.2.5. I brukerveiledningen står det at det skal gjennomføres DPIA i tillegg til ROS dersom risiko fortsatt vurderes som høy etter etablering og gjennomføring av tiltak. DPIA er ikke omtalt i brukerveiledningen ut over dette. Som tidligere nevnt har ikke revisjonen mottatt noen prosedyre for risiko- og sårbarhetsvurderinger i Gjerdrum kommune. Vurdering av om det skal gjennomføres DPIA inngår i kommunens prosedyre for å starte behandling av personopplysninger. Ifølge denne prosedyren er det kommunalsjef/enhets-/virksomhetsleder som er ansvarlig for at dette gjennomføres. Som omtalt i kapittel 3.2.2. er det imidlertid uklart for revisjonen hvorvidt innholdet i denne prosedyren er kjent for de ansvarlige for behandling av personopplysninger i kommunen.

Digitaliseringsrådgiver forteller i intervju at en DPIA gjennomføres når en risikovurdering vurderer det som nødvendig. Hun forteller at videre at DPIA gjennomføres i de faste ROS-møtene som avholdes av digitaliseringsteamet hver fredag.

Kommunens mal for gjennomføring av DPIA inneholder en initialvurdering som skal ende i en avgjørelse av om det skal gjennomføres en fullstendig DPIA. Dersom det vurderes som nødvendig med en fullstendig DPIA skal det gis en systematisk beskrivelse av behandlingen av personopplysninger, vurderinger av nødvendighet og proporsjonalitet og risikovurderinger. DPIA-

malen inneholder i tillegg felt for innsamling av synspunkter fra de registrerte, personvernombudets kommentar og den behandlingsansvarliges aksept av risiko.

Etter det revisjonen kan se er det gjennomført DPIA for seks av de tolv digitale læremidlene som er registrert i ROS-kanalen. Revisjonen har gjennomgått disse. Én av DPIA-ene er gjennomført i ny mal, mens de resterende er gjennomført etter en eldre mal. Det er forskjeller mellom ny og gammel mal i oppsett, men etter hva revisjonen kan se har de i stor grad samme innhold. I samtlige av gjennomgåtte DPIA er det gjennomført initialvurdering. Én av disse konkluderte med at det ikke er nødvendig å gjennomføre en full DPIA. Skjemaene for gjennomføringen av DPIA er fylt ut for samtlige av tjenestene, men noen av de gjennomførte DPIA-ene mangler behandlingsansvarliges, de registrertes og personvernombudets vurderinger, samt ledelsens vurderinger, konklusjon og signatur.

Digitaliseringsrådgiver forteller i intervju at de samler opp vurderingene av personvernkonsekvenser før de presenteres for konstituert kommunalsjef for oppvekst og psykisk helse. Hun forteller at kommunalsjef gir en kommentar og behandler vurderingene samt godkjenner eventuell restrisiko. Aksept av risiko dokumenteres i skjemaet som brukes i gjennomføringen av DPIA (jf. mal for DPIA omtalt over). Malen inneholder et felt hvor det skal fylles inn om risikoen er akseptert, samt et felt for leders signatur.

3.3 Revisjonens vurdering

Gjerdrum kommune har et personvernombud i 20 prosent stilling. Personvernombudet har deltatt i en rekke aktiviteter knyttet til personvern i kommunen, som deltakelse på kommunens nyansattdag, ukentlige ROS-møter med digitaliseringsteamet. Videre har personvernombudet levert årsrapport til kommunedirektøren om arbeidet som er gjort med personvern i kommunen. Så langt revisjonen kan vurdere har kommunen et personvernombud med ansvar og oppgaver i tråd med GDPR artikkel 37-39.

Gjerdrum kommune har en behandlingsprotokoll jf. personvernforordningen artikkel 30, hvor det i perioden 2022-2023 ble gjort et arbeid med å registrere behandlinger av personopplysninger. Protokollen er imidlertid ikke ferdigstilt og oppdatert siden personvernombudets gjennomgang i 2023, og oppfyller etter revisjonens vurdering derfor ikke kravene til behandlingsprotokoll. Etter revisjonens syn er det videre behov for å avklare roller og ansvar knyttet til registreringer av behandlinger av personopplysninger i protokollen, samt ansvaret for den overordnede oppfølgingen av protokollen. Det er viktig at kommunen har oversikt over behandlingsaktivitetene som utføres under deres ansvar, for å sikre at innbyggernes personopplysninger behandles på en forsvarlig måte.

Gjerdrum kommune har mal, prosedyre og sjekkliste for databehandleravtaler. Kommunen har imidlertid ikke klart å fremskaffe fire av de tolv databehandleravtalene knyttet til digitale læremidler som revisjonen har etterspurt. Det er etter revisjonens syn svært uheldig at kommunen mangler oversikt over egne dataavtaler. Dersom kommunen ikke kan dokumentere databehandleravtaler for eksterne leverandører som behandler personopplysninger kommunen er ansvarlig for, er dette brudd på artikkel 28 i personvernforordningen. Dette kan i ytterste konsekvens medføre sanksjoner fra Datatilsynet og tap av tillit dersom personopplysninger kommer på avveie hos databehandler.

Revisjonens vurdering er at kommunen har rutiner for å gjennomføre og dokumentere vurderinger av personvernkonsekvenser (DPIA) innenfor skoleområdet. Gjerdrum kommune har en mal for gjennomføring av DPIA og har gjennomført seks DPIA av digitale læremidler. Kommunens mal i stor grad fulgt, men det mangler i noen tilfeller vurderinger fra behandlingsansvarlige, de registrerte og personvernombud, samt leders vurdering, aksept av restrisiko og signatur.

4 KONKLUSJON OG ANBEFALINGER

Denne undersøkelsen har hatt som formål å avdekke eventuelle svakheter i informasjonssikkerheten og behandlingen av personopplysninger i Gjerdrum kommune.

Det er revisjonens konklusjon at kommunen har etablert et styringssystem for informasjonssikkerhet, men at det er noen mangler knyttet til styrende dokumenter, rolle- og ansvarsfordeling, ledelsens gjennomgang og risikovurderinger. Kommunen har overordnede styrende dokumenter for informasjonssikkerhet, men disse gir ikke et oppdatert bilde av dagens organisering. Rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet ikke er tilstrekkelig avklart, særlig når det gjelder hvilket ansvar som er lagt til digitaliseringsteamet og hva som tillegges kommunalsjefer, enhetsledere og virksomhetsledere.

Kommunens digitaliseringsteam har i praksis en sentral rolle i gjennomføringen av risikoanalyser i kommunen, men digitaliseringsteamet ser ikke ut til å være involvert i risikoanalyser i alle kommunens tjenesteområder. Det er ikke gjennomført risikoanalyser innenfor teknisk sektor. Kommunen har ikke en prosedyre for risiko- og sårbarhetsvurderinger, som sier noe om når det skal gjennomføres risikoanalyser og hvem som har ansvar for gjennomføringen av disse, samt hvem som skal akseptere restrisiko. Kommunens digitaliseringsteam har et system for gjennomføring av risikovurderinger, men dokumentasjonen på gjennomføring og oppfølging av tiltak er i mindre grad systematisert. Det gjennomføres ikke ledelsens gjennomgang av informasjonssikkerhet årlig i Gjerdrum kommune.

Revisjonen konkluderer med at Gjerdrum kommune i noen grad har sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret. Kommunen har et personvernombud og gjennomfører vurderinger av personvernkonsekvenser (DPIA). Flere av de gjennomførte DPIAene har imidlertid mangler knyttet til versjonslogg, uttalelser og aksept av restrisiko, samt leders signatur. Kommunen har startet arbeidet med å få på plass en behandlingsprotokoll, men det er uklart hvem som har det overordnede ansvaret for at denne ferdigstilles og vedlikeholdes. Kommunen kan ikke dokumentere databehandleravtaler for flere digitale læremidler.

Basert på det som kommer frem i undersøkelsen anbefaler revisjonen at kommunedirektør sørger for:

1. at kommunen oppdaterer styrende dokumenter, slik at det gis en tydelig beskrivelse av dagens styringssystem for informasjonssikkerhet
2. å tydeliggjøre og dokumentere oppgave-, rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet
3. å etablere rutiner og praksis for å gjennomføre, dokumentere og følge opp risikovurderinger av informasjonssikkerheten innenfor alle tjenesteområdene i kommunen
4. at ledelsens gjennomgang av informasjonssikkerhet gjennomføres årlig

5. at behandlingsprotokollen ferdigstilles, og at roller og ansvar knyttet til å oppdatere protokollen klargjøres
6. at alle databehandleravtaler dokumenteres
7. at DPIAer som gjennomføres dokumenteres i tilstrekkelig grad

LITTERATUR- OG KILDELISTE

Lov, forskrift og veiledere

Lov om kommuner og fylkeskommuner av 22. juni 2018 nr. 83 (kommuneloven).

Lov om nasjonal sikkerhet av 1. juni 2018 nr. 24 (sikkerhetsloven).

Lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven).

Forskrift om behandling av personopplysninger av 15. juni 2018 nr. 876.

Forskrift om elektronisk kommunikasjon med og i forvaltningen av 25. juni 2004 nr. 988 (eForvaltningsforskriften).

NSMs grunnprinsipper for IKT-sikkerhet versjon 2.1, 2024.

NSMs rammeverk for håndtering av IKT-sikkerhetshendelser.

Digitaliseringsdirektoratets (Digdir) veileder «Internkontroll i praksis – informasjonssikkerhet».

Datatilsynets veileder «Virksomhetens plikter» (nettbasert veileder).

Fra Gjerdrum kommune

Gjerdrum kommune (2018a). *Prosedyre for bruk av databehandler.*

Gjerdrum kommune (2019a). *Sjekkliste for databehandleravtaler.*

Gjerdrum kommune (2019b). *Overordnet ROS-analyse.*

Gjerdrum kommune (2021a). *Strategi for IKT sikkerhet og personvern for kommunene i Gardermoregionen.*

Gjerdrum kommune (2022a). *Prosedyre for intern varsling av avvik.*

Gjerdrum kommune (2022b). *Bevarings- og kassasjonsplan del 1 og 2*. Revidert 22.02.2022.

Gjerdrum kommune (2022c). *Prosedyre for å starte behandling av personopplysninger*.

Gjerdrum kommune (2023a). *Instruks for informasjonssikkerhet og personvern.*

Gjerdrum kommune (2024a). *Digitalisering og innovasjon. Slik gjør vi det i Gjerdrum kommune.*

Gjerdrum kommune (2024b). *Internkontroll i Gjerdrum kommune*.

Gjerdrum kommune (2024c). *Delegeringsreglement. Reglem* https://delegering.kf.no/delegering/publikum/3032

Gjerdrum kommune (2025a). *Overordnet ROS. 28.05.2025.*

Gjerdrum kommune (2025b). Digitaliseringsteamets presentasjon for KLG 10.12.2025.

Gjerdrum kommune (udatert a). *Brukerveiledning ROS & DPIA*.

Gjerdrum kommune (udatert b). *Databehandleravtale*, mal.

Gjerdrum kommune (udatert c). *Hjelpeark til ROS.*

Gjerdrum kommune (udatert d). *Prosedyre for hendelses- og avviksbehandling i kvalitetssystemet.*

Gjerdrum kommune (udatert e). *Mal for DPIA*.

Gjerdrum kommune (udatert f). *Mal for ROS*.

Gjerdrum kommune (udatert g). Personvernerklæring for Gjerdrum kommune. https://www.gjerdrum.kommune.no/tjenester/om-kommunen/personvern/personvernerklaring/ [Hentet 26.9.2025].

Fra Digitale Gardermoen

Digitale Gardermoen (2025a) Saksfremlegg i KDU-P 21.3.2025 med vedlegg. Sak 20/4, arkivsak 25/470-1.

Digitale Gardermoen (2025b). Syringsmodellen slik den fremgår av DGIs interne side om styringsmodellen i SharePoint. https://digirom.sharepoint.com/sites/DGIStyringsmodell/SitePages/Styringsmodell.aspx [hentet 22.9.2025].

Digitale Gardermoen (2025c): *Om DGI*. Hentet fra: https://www.dgi.no/om-dgi/ [Hentet 22.9.2025].

Fra personvernombudet

Personvernombudet i Gjerdrum kommune (2025a). E-post fra personvernombudet til revisjonen, 1.5.2025.

Personvernombudet i Gjerdrum kommune (2025b). Årsrapport for personvernarbeidet i Gjerdrum kommune 2024. Datert 7.1.2025.

Nettsider

Datatilsynet (2019): *Hva er en databehandler?* Hentet fra: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsansvarlig-og-databehandler/hva-er-en-databehandler/

Datatilsynet (2022): *Overtredelsesgebyr til Østre Toten kommune*. Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2022/overtredelsesgebyr-til-ostre-toten-kommune/

Datatilsynet (udatert): *Ordliste.* Hentet fra: https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/.

NAOB (udatert): *Informasjonssikkerhet*. Hentet fra: https://naob.no/ordbok/informasjonssikkerhet

Øvrige kilder

Datatilsynet (2025). *Funn fra skoletilsynet. Samlerapport fra Datatilsynets brevkontroll med skolesektoren*. Mai 2025.

NOU 2022: 11 *Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk*.

VEDLEGG 1 KOMMUNEDIREKTØRS UTTALELSE

GJERDRUM KOMMUNE
Organisasjons- og samfunnsutvikling

Romerike Revisjon Iks
Ringvegen 4
2050 Jessheim

Deres ref.:	Vår ref.:	Dato:
	24/3261 - 8 / ANNEBF-GJE	04.11.2025

Tilbakemelding på foreløpig rapport - forvaltningsrevisjon om informasjonssikkerhet og personvern

På vegne av kommunedirektør oversender vi våre innspill til den foreløpige rapporten:

Vi takker for gjennomgangen og tilbakemeldingene knyttet til informasjonssikkerhet og personvern. Vi ser rapporten som et viktig bidrag til å styrke vår sikkerhetspraksis og etterlevelse av gjeldende krav, og vi vil bruke forbedringsområdene som grunnlag for systematisk og risikobasert arbeid når endelig rapport er behandlet.

Det er noen beskrivelser i rapporten som vi ønsker å kommentere:

"Rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet ikke er tilstrekkelig avklart, særlig når det gjelder hvilket ansvar som er lagt til digitaliseringsteamet og hva som tillegges kommunalsjefer, enhetsledere og virksomhetsledere."

> Kommentar: Dette er behandlet i delegeringsreglementet under punktet internkontroll hvor intensjonen er at informasjonssikkerhet er en integrert del av overordnet internkontroll. Vi er imidlertid enige i at punktet bør tydeliggjøres.

«Kommunen har startet arbeidet med å få på plass en behandlingsprotokoll, men det er uklart hvem som har det overordnede ansvaret for at denne ferdigstilles og vedlikeholdes.»

> Kommentar: Behandlingsprotokoll kom på plass for flere år siden. Vi ser imidlertid at eierskapet til denne er påvirket av overføring av ansvar mellom av- og påtroppende personvernombud.

«Kommunens digitaliseringsteam har i praksis en sentral rolle i gjennomføringen av risikoanalyser i kommunen, men digitaliseringsteamet ser ikke ut til å være involvert i risikoanalyser i alle kommunens tjenesteområder. Det er ikke gjennomført risikoanalyser innenfor teknisk sektor.

Postadresse	Besøksadresse	Telefon	Kontonr.	E-post
Gjerdrum kommune Postboks 10 2024 Gjerdrum	Herredshuset Gjerivegen 1 2024 Gjerdrum Åpningstid: 09:00 – 15:30	66 10 60 00	3207 45 39873 Org.nr. 864 949 762	post@gjerdrum.kommune.no Hjemmeside www.gjerdrum.kommune.no

Kommunen har ikke en prosedyre for risiko- og sårbarhetsvurderinger, som sier noe om når det skal gjennomføres risikoanalyser og hvem som har ansvar for gjennomføringen av disse, samt hvem som skal akseptere restrisiko.»

Kommentar: Det ble før sommeren etablert en ny styringsmodell (omtalt i punkt 2.2.1). Den nye styringsmodellen ivareta informasjonssikkerheten og personvernet i kommunene bedre enn tidligere:

- Alle nye initiativ/anskaffelser/prosjekter skal involvere IKT-sikkerhetsforum.
- Forvaltningsforum får ansvar for å forvalte og vedlikeholde kommunenes systemoversikter. Det pågår en kartlegging av alle applikasjoner og skytjenester i kommunene med tanke på bl.a. ROS, DPIA, kontrakter, databehandleravtaler og roller.
- Et dynamisk team har fått mandat til å organisere felles håndtering av risikovurderinger i kommunesamarbeidet. Foreløpig forslag er at Forvaltningsforum får ansvaret for å følge opp manglende risikovurderinger og sørger for revidering der det er behov.

"Kommunen mangler databehandleravtaler for flere digitale læremidler."

Kommentar: Alle digitale læremidler som er i bruk i dag har databehandleravtale.

Med hilsen

Anne Britt Fagerli
seniorrådgiver

Dokumentet er elektronisk godkjent og har derfor ingen signatur

VEDLEGG 2 REVISJONSKRITERIER

Revisjonskriterier og kilder

Revisjonskriterier er de normer og krav som stilles til kommunens virksomhet som er omfattet av en forvaltningsrevisjon. Revisjonskriteriene er dermed målestokken som kommunens praksis vurderes opp mot. Revisjonskriterier kan utledes fra lover og forskrifter, kommunestyrets vedtak og hva som anses som god forvaltningsskikk og faglig anerkjente normer på området.

I denne undersøkelsen er revisjonskriteriene utledet fra følgende kilder:

- Lov om kommuner og fylkeskommuner av 22. juni 2018 nr. 83 (kommuneloven)
- Lov om behandling av personopplysninger av 15. juni 2018 nr. 38 (personopplysningsloven)
- Forskrift om behandling av personopplysninger av 15. juni 2018 nr. 876
- Forskrift om elektronisk kommunikasjon med og i forvaltningen av 25. juni 2004 nr. 988 (eForvaltningsforskriften)
- Veiledere basert på anerkjente standarder for informasjonssikkerhet:
    - *Ledelsessystemer for informasjonssikkerhet - krav* (ISO/IEC 27001).
    - Datatilsynets veileder «Virksomhetens plikter» (nettbasert veileder)
    - Digitaliseringsdirektoratets (Digdir) veileder «Internkontroll i praksis – informasjonssikkerhet» (nettbasert veileder)
    - Kommunal- og moderniseringsdepartementet (KMD) og Direktoratet for forvaltning og IKT (Digdir) 2015, Veileder til eForvaltningsforskriften, del 1. Elektronisk samhandling med og i forvaltningen – eForvaltningsforskriften. Rolf Riisnæs, advokat dr. juris, Wikborg, Rein & Co. Advokatfirma DA.
    - KS 2025. Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus
    - NSMs grunnprinsipper for IKT-sikkerhet versjon 2.1, 2024
    - NSMs rammeverk for håndtering av IKT-sikkerhetshendelser

Styringssystem for informasjonssikkerhet (internkontroll)

Ledelsessystem for informasjonssikkerhet

Kommunens styringssystem for informasjonssikkerhet skal ivareta kommunens internkontroll på området informasjonssikkerhet. Ifølge lov om kommuner og fylkeskommuner (kommuneloven) § 25-1 skal kommuner ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges. Etter paragrafens andre avsnitt skal internkontrollen være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Kommunedirektøren er ansvarlig for internkontrollen i kommunen.

Etter forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) § 15 andre avsnitt skal kommunen som forvaltningsorgan ha en internkontroll på

informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør videre være en integrert del av virksomhetens helhetlige styringssystem.

Det er vesentlig at styringssystemet for informasjonssikkerhet og personvern i en kommune er godt forankret i ledelsen (KS 2025). Både NSMs grunnprinsipper for informasjonssikkerhet 2.1. og Digitaliseringsdirektoratets (Digdir) nettbaserte veileder, *Internkontroll i praksis*, er basert på gjeldende versjon av standarden *Ledelsessystemer for informasjonssikkerhet - krav* (ISO/IEC 27001). I begge veilederne blir ledelsens styring og oppfølging trukket fram som sentralt for å lykkes med implementeringen av informasjonssikkerheten i en virksomhet. Ifølge digitaliseringsdirektoratets veileder er kommuneledelsens viktigste oppgaver blant annet å gi overordnede føringer for det kontinuerlige arbeidet med informasjonssikkerhet og følge opp at føringer blir etterlevd og fungerer som forutsatt.

Kommuneledelsen bør gjennomføre «ledelsens gjennomgang» av informasjonssikkerhet og personvern (Digdir 2025, KS 2025). Digdirs veileder anbefaler at fagansvarlig for informasjonssikkerhet forbereder gjennomgangen og at den gjennomføres i toppledergruppen. Ledelsens gjennomgang benyttes til å følge med på, følge opp og vedlikeholde styringsaktivitetene. Formålet med ledelsens gjennomgang er å avklare status på virksomhetens arbeid med styring av informasjonssikkerhet, avklare status på områder og tjenester der virksomhetsledelsen er spesielt opptatt av informasjonssikkerheten og å reagere og følge opp der det er nødvendig. Aktiviteten bør gjennomføres minst en gang årlig av toppledelsen i virksomheten.

Styrende dokumenter for informasjonssikkerhet

Som ansvarlig for internkontrollen i kommunen skal kommunedirektøren utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering (kommuneloven § 25-1). Kommunedirektøren skal dokumentere internkontrollen i den formen og det omfanget som er nødvendig (§ 25-1 d). Kommunen skal ifølge kommuneloven § 25-1 ha nødvendige rutiner og prosedyrer og evaluere skriftlige prosedyrer og andre tiltak for internkontroll og forbedre disse ved behov. I KS-veilederen er kommunene anbefalt å utarbeide rutiner og prosedyrer for når, hvordan og hvem som skal utføre oppgaver. Kommunen anbefales å beskrive organiseringen av arbeidet, herunder roller og ansvar for sikkerhet og personvern.

Ifølge Digitaliseringsdirektoratets veileder «Virksomhetens plikter» er god kommunikasjon en forutsetning for god styring og kontroll. Dokumentasjon trekkes frem som en viktig del av dette. Ifølge veilederen må kommunen ha tydelige føringer for hvordan kommunikasjon og dokumentasjon skal foregå. Ifølge veilederen må for eksempel kommunedirektøren sikre at gjennomførte styringsaktiviteter dokumenteres, mens fagansvarlig for informasjonssikkerhet systematisk må utarbeide statusrapporter som grunnlag for risikovurderinger og saksnotat til ledelsens gjennomgang.

Etter eForvaltningsforskriften § 15 skal forvaltningsorganet ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi), som skal danne grunnlaget for internkontrollen på informasjonssikkerhetsområdet. Ifølge veilederen til eForvaltningsforskriften skal sikkerhetsmålene beskrive hva som ønskes oppnådd på informasjonssikkerhetsområdet. Videre skal sikkerhetsmålene understøtte og bidra til realisering av kommunens overordnede mål og etterlevelse av lover og regler (Kommunal- og

moderniseringsdepartementet 2015). Datatilsynets veileder, *Virksomhetens oppgaver*, beskriver sikkerhetsmålene som «ledelsens beslutninger om hva IKT skal brukes til i virksomheten og hvordan den skal benyttes for å nå virksomhetens mål». Videre skal målene ifølge veilederen være retningsgivende for sikkerhetsstrategien.

Hvordan kommunen skal nå sine sikkerhetsmål skal beskrives i kommunenes sikkerhetsstrategi (KMD 2015).

Oppgave-, rolle- og ansvarsfordeling for informasjonssikkerhet

Sikkerhetsstrategien skal omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Dette innebærer blant annet fordeling av oppgaver, roller og ansvar, organisatoriske og tekniske strategiske valg og beskrivelse av virkemidlene virksomheten skal bruke for å nå sikkerhetsmålene (Datatilsynet 2015).

Ifølge KS sin veileder *Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet* er en klar ansvarsfordeling, delegering og beskrivelse av roller en vesentlig del av styringssystemet for personvern og informasjonssikkerhet. Ifølge KS-veilederen bør det fordeles og dokumenteres ansvar for informasjonsverdier, kritikalitet og behandlingsprotokoller, gjennomføring av risikovurderinger av ulike behandlinger og løsninger, gjennomføring av personvernkonsekvensvurderinger og oppfølging av eksterne leverandører.

Vurdering og håndtering av risiko

Ifølge Digdir sin veileder *Internkontroll i praksis – informasjonssikkerhet* er vurdering av risiko «hjertet» i internkontrollen. Risiko som angår informasjonssikkerhet må ifølge veilederen identifiseres, analyseres og evalueres. Risikovurderingen kan gjelde hele kommunen på strategisk nivå, enkelte oppgaver eller tjenester, eller spesifikke informasjonssystemer eller deler av disse. KS-veilederen peker på viktigheten av å gjennomføre risikovurderinger for å få oversikt over mulige uønskede hendelser og bidra til at sikkerhets- og personvernarbeidet retter fokus mot områder med høyest risiko.

Etter at en risikovurdering er gjennomført skal risiko håndteres. Sikkerhetstiltak etableres og forvaltes for å redusere risiko, gjennom å redusere konsekvenser av uønskede hendelser eller sannsynligheten for at de inntreffer (Digdir-veilederen). Der hvor det er identifisert høy risiko må kommunedirektøren sikre at tiltak blir iverksatt, og forsikre seg om at risiko blir redusert (KS-veilederen).

Et av NSMs grunnprinsipper handler om å identifisere virksomhetens toleransegrenser for risiko knyttet til IKT. Dette innebærer at ledelsen må fastsette hvilke grenser for risiko kommunen aksepterer og hva som er uakseptabel risiko. I veilederen til KS vises det til at risikoforståelse og aksept av restrisiko er et lederansvar. Ifølge KS-veilederen bør kommunedirektøren som minimum kjenne til resultatet av risikovurderingene og ta stilling til uakseptabel risiko. Ifølge veilederen er det avgjørende at aksept av restrisiko besluttes og dokumenteres for å kunne jobbe risikobasert og prioritere tiltak for aktiviteter som innebærer høy risiko.

På bakgrunn av gjennomgangen over knyttet til styringssystem for informasjonssikkerhet legger revisjonen til grunn følgende revisjonskriterier for problemstilling 1:

Problemstilling 1	Krav og forventninger til kommunen
Har kommunen dokumentert et styringssystem for informasjonssikkerhet som tilfredsstiller krav i lov, forskrift og etablerte standarder?	Kommunen skal ha → utarbeidet styrende dokumenter for informasjonssikkerhet, inkludert sikkerhetsmål og sikkerhetsstrategi → organisering med klar oppgave-, rolle- og ansvarsfordeling for informasjonssikkerhet → gjennomført ledelsens gjennomgang av informasjonssikkerhet årlig → et system for gjennomføring av risikovurderinger, etablering av tiltak og aksept av risikonivå

Sikring av personopplysninger

Behandlingen av personopplysninger er regulert i lov om behandling av personopplysninger (personopplysningsloven). Personvernforordningen (GDPR) er innlemmet i personopplysningsloven.

Behandlingsansvarlig er en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. GDPR art. 4 punkt 7. Det betyr at Gjerdrum kommune er behandlingsansvarlig for personopplysninger som kommunen samler inn og benytter. Ledelsen kan delegere oppgaver knyttet til behandling av personopplysninger, men selve behandlingsansvaret kan ikke delegeres (Datatilsynet, 2019).

For å ivareta en forsvarlig behandling av personopplysningene, plikter kommunen å sette i verk egnede tiltak for å sikre og påvise at personopplysninger behandles i samsvar med regelverket. Tiltakene skal være både tekniske og organisatoriske[3], og tiltakene skal gjennomgås på nytt og oppdateres ved behov (personvernforordningen artikkel 24).

Personvernforordningens artikkel 5, første punkt, beskriver prinsipper for behandling av personopplysninger. Ifølge artikkel 5 skal personopplysninger:

a. behandles på en lovlig, rettferdig og åpen måte
b. samles inn for spesifikke, uttrykkelig angitte og berettigede formål (formålsbegrensning)
c. være adekvate, relevante og begrenset til det som er nødvendig (dataminimering)
d. være korrekte og om nødvendig oppdaterte (riktighet)
e. lagres slik at det ikke er mulig å identifisere de registrerte i lengre perioder enn det som er nødvendig (lagringsbegrensning)

[3] Med tekniske og organisatoriske tiltak menes både IT-sikkerhetstiltak (som kryptering, tilgangsstyring og sikkerhetskopiering) og organisatoriske løsninger (som rutiner, retningslinjer og opplæring) som skal sikre forsvarlig behandling av personopplysninger.

f. behandles på en måte som sikrer tilstrekkelig sikkerhet for personopplysningene, herunder vern mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak (integritet og konfidensialitet)

Personvernombud

Etter personvernforordningen artikkel 37 skal den behandlingsansvarlige (kommunen) utpeke et personvernombud. Etter artikkel 38 i personvernforordningen skal kommunen sikre at personvernombudet på riktig måte og i rett tid involveres i alle spørsmål som gjelder vern av personopplysninger.

Personvernombudets oppgaver er i etter artikkel 39 i personvernforordningen å informere og gi råd om vern av personopplysninger, gi råd om vurderingen av personvernkonsekvenser og samarbeide med og fungere som kontaktpunkt for tilsynsmyndigheten. Videre skal personvernombudet kontrollere overholdelsen av personvernforordningen, statens personvernregler og kommunens personvernsretningslinjer. Dette innebærer blant annet kontroll med kommunens fordeling av ansvar, holdningsskapende tiltak og opplæring av personellet som er involvert i behandlingsaktivitetene. På anmodning av kommunen skal personvernombudet gi råd om vurdering av personvernkonsekvenser og kontrollere gjennomføringen av disse vurderingene.

Ifølge tredje punkt i artikkel 38 av personvernforordningen skal kommunen og databehandler sikre at personvernombudet ikke mottar instrukser om utførelsen av personvernombudets oppgaver. Videre skal personvernombudet rapportere direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige eller databehandleren.

Behandlingsprotokoll

Artikkel 30 i personvernforordningen krever at kommune fører protokoll over behandlingsaktiviteter. Behandlingsprotokollen skal ifølge artikkel 30 inneholde følgende informasjon:

a. navnet på og kontaktopplysningene til den behandlingsansvarlige og, dersom det er relevant, den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet,
b. formålene med behandlingen,
c. en beskrivelse av kategoriene av registrerte[4] og kategoriene av personopplysninger[5],
d. kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til, herunder mottakere i tredjestater eller internasjonale organisasjoner,
e. dersom det er relevant, overføringer av personopplysninger til en tredjestat eller en internasjonal organisasjon, herunder identifikasjon av nevnte tredjestat eller internasjonale organisasjon og, ved overføringer nevnt i artikkel 49 nr. 1 annet ledd, dokumentasjon på nødvendige garantier,
f. dersom det er mulig, de planlagte tidsfristene for sletting av de forskjellige kategoriene av opplysninger,

[4] Med 'registrert' menes den fysiske personen som personopplysningene vedrører
[5] Med kategorier av personopplysninger menes typer opplysninger som behandles om de registrerte, eksempelvis identifikasjonsopplysninger, økonomiske opplysninger eller særlige kategorier som helseopplysninger

g. dersom det er mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene nevnt i artikkel 32 nr. 1.

Databehandleravtaler

Etter personvernforordningen artikkel 28 skal behandlinger utført av en databehandler være underlagt en avtale eller et annet rettslig dokument som er bindende for databehandleren med hensyn til den behandlingsansvarlige. Avtalen skal fastsette gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte, samt den behandlingsansvarliges rettigheter og plikter (artikkel 28 tredje punkt).

Datatilsynets veileder om virksomhetens plikter under personvernforordningen gir en beskrivelse av hva en databehandleravtale må inneholde i henhold til artikkel 28. Databehandleravtalen må beskrive:

- Behandlingens art, hva som er formålet med behandlingen og avtalens varighet
- Kategorier av registrerte som omfattes, og hva slags personopplysninger som behandles
- Databehandlers plikter og rettighetene til den behandlingsansvarlige, herunder
    - Den behandlingsansvarlige er ansvarlig for at personopplysninger blir behandlet i samsvar med personvernforordningen og personopplysningsloven (jf. artikkel 24).
    - Den behandlingsansvarlige har både en rett og en forpliktelse til å bestemme hvilke formål, og hvilke hjelpemidler som kan brukes i behandlingen (jf. artikkel 4 nr. 7).
    - Den behandlingsansvarlige skal gi databehandleren dokumenterte instrukser for hvordan personopplysninger skal behandles (jf. artikkel 28 nr. 3 bokstav a). Instruksene skal være en del av avtalen eller lagt ved som et vedlegg til avtalen.
    - Den behandlingsansvarliges rett til å si opp avtalen dersom databehandleren ikke lenger oppfyller lovens krav etter artikkel 28 nr. 1.
- Databehandlers forpliktelser, herunder:
    - Bare behandle personopplysninger etter skriftlig instruks fra den behandlingsansvarlige
    - Plikt til at autoriserte personer behandler personopplysningene fortrolig
    - Plikt til å ha tilfredsstillende sikkerhetstiltak
    - Bruk av annen databehandler (underleverandør)
    - Bistand til å svare på anmodninger som gjelder de registrertes rettigheter
    - Bistand til den behandlingsansvarlige
    - Avslutning av avtalen
    - Tilgjengeliggjøring av informasjon for den behandlingsansvarlige

Vurdering av personvernkonsekvenser (DPIA)

Personvernforordningens artikkel 35 krever at kommunen ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter, skal gjennomføre en vurdering av personvernkonsekvenser, også kalt DPIA (Data Protection Impact Assessment). Etter syvende punkt i artikkel 35 skal vurderingen skal minst inneholde:

a. en systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen

b. en vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene
c. en vurdering av risikoene for de registrertes rettigheter og friheter
d. de planlagte tiltakene for å håndtere risikoene og for å påvise at personvernreglene overholdes

Dersom et personvernombud er utpekt, skal kommunen rådføre seg med vedkommende i forbindelse med utførelsen av en vurdering av personvernkonsekvenser (artikkel 35, punkt 2).

Følgende revisjonskriterier legges til grunn for problemstilling 3:

Problemstilling 2	Krav og forventninger til kommunen
Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret i tilstrekkelig grad?	Kommunen skal ha → utpekt et personvernombud med ansvar og oppgaver som tilfredsstiller GDPR artikkel 37- 39 → protokoll over hvilke personopplysninger kommunen behandler → rutiner og praksis som sikrer at kommunen har databehandleravtaler med eksterne leverandører som behandler personopplysninger → rutiner og praksis for å gjennomføre og dokumentere vurderinger av personvernkonsekvenser (DPIA)