ROMERIKE REVISJON IKS

RAPPORT NR. 2-2026

INFORMASJONSSIKKERHET OG PERSONVERN

ULLENSAKER KOMMUNE

FORVALTNINGSREVISJON

JANUAR 2026

INNHOLD

FIGURER

SAMMENDRAG

Romerike revisjon har gjennomført en forvaltningsrevisjon av informasjonssikkerhet og personvern i Ullensaker kommune. Prosjektet ble bestilt av kontrollutvalget i Ullensaker kommune den 17.10.2024 i sak 37/24. Formålet med forvaltningsrevisjonen har vært å avdekke eventuelle svakheter i informasjonssikkerheten og ivaretakelsen av personvern i Ullensaker kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

Hovedfunn

1. Ullensaker kommune har et styringssystem for informasjonssikkerhet, men det er mangler knyttet til styrende dokumenter for informasjonssikkerhet, rolle- og ansvarsfordeling.
2. Ledelsens gjennomgang av informasjonssikkerhet er ikke gjennomført.
3. Kommunen har langt på vei tilstrekkelige tiltak som fanger opp og hindrer datainnbrudd, men gjennomfører ikke jevnlige inntrengingstester som anbefalt.
4. Kommunen har i noen grad sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret.

Kommunen har styrende dokumenter for informasjonssikkerhet, men rolle- og ansvarsfordelingen er uklar på noen områder. Enhet innovasjon og digitalisering har ansvar for systemer som brukes på tvers i organisasjonen, mens hver enhet har ansvar for det som anskaffes innenfor sin enhet. Det er imidlertid uklart hvem som har ansvar for å ha oversikt over den samlede porteføljen av applikasjoner og systemer i kommunen. Videre ansvarliggjør kommunens plan for hendelseshåndteringen en rolle som i lengre tid ikke har vært besatt. Det er ikke gjennomført ledelsens gjennomgang av informasjonssikkerhet i Ullensaker kommune, slik det er anbefalt i etablerte standarder for informasjonssikkerhet.

Kommunen har en rekke tiltak for å fange opp og hindre forsøk på datainnbrudd. Dette består blant annet av sikkerhetsovervåkning, system og prosedyrer for styring av identiteter og tilganger, gjennomføring av risikovurderinger, samt en rekke opplæringsaktiviteter knyttet til informasjonssikkerhet. Kommunen gjennomfører ikke inntrengingstester jevnlig som anbefalt.

Kommunen har utpekt et personvernombud i henhold til personvernforordningen. Ombudet rapporterer imidlertid ikke direkte til kommunens øverste ledelsesnivå. Kommunen har en behandlingsprotokoll, men praksisen med å føre samtlige digitale læremidler samlet i protokollen gir etter revisjonens syn ikke tilstrekkelig informasjon om personopplysningene som samles inn for de enkelte læremidlene. Kommunen har maler som tilfredsstiller kravene i personvernforordningen for databehandleravtaler og gjennomføring av vurderinger av personvernkonsekvenser (DPIA). Kommunen mangler imidlertid oversikt over databehandleravtalene samt tilstrekkelig dokumentasjon av ansvarsforhold knyttet til DPIA.

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

1. å oppdatere styrende dokumenter, slik at det gis en riktig beskrivelse av dagens styringssystem for informasjonssikkerhet
2. å tydeliggjøre og dokumentere oppgave-, rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet
3. å gjennomføre ledelsens gjennomgang av informasjonssikkerhet årlig
4. at det gjennomføres jevnlige inntrengingstester
5. å etablere rutiner for direkte rapportering fra personvernombudet til kommuneledelsen
6. at behandlingsprotokollen tilfredsstiller kravene i personvernforordningen
7. tilstrekkelig dokumentasjon av risikovurderinger og vurderinger av personvernkonsekvenser for digitale læremidler som er i bruk i skolene
8. å skaffe oversikt over kommunens databehandleravtaler og sikre at databehandleravtaler som mangler kommer på plass

1 INNLEDNING

1.1 Bakgrunn for prosjektet

1.1.1 Kommunal IKT-sikkerhet – sårbart og viktig

Den økende digitale kompleksiteten i samfunnet fører til store utfordringer i kommunesektoren, hvor det er mange små enheter som har ansvar for viktige systemer og tjenester. I tillegg har kommunene ofte problemer med å skaffe tilstrekkelig kompetanse på IKT-sikkerhet (NOU 2015:13).

Solid IKT-sikkerhet og et tilstrekkelig personvern i kommunene er avgjørende for å beskytte innbyggernes personopplysninger og sikre viktige samfunnsfunksjoner. Et datainnbrudd i en kommunes IKT-systemer kan ha store konsekvenser. For eksempel ble Østre Toten kommune utsatt for et alvorlig cyberangrep i 2021, der alle sikkerhetskopier ble slettet og alle data kryptert. Angrepet førte til full stans i datasystemene for kommunens 1300 ansatte. Sensitive personopplysninger fra helse- og omsorgstjenester, NAV og barnevern kom på avveie (Datatilsynet 2022). I februar 2022 ble Drammen kommunes vannsystem utsatt for et hackerangrep, kort tid etter et lignende angrep i USA der hackerne forsøkte å forgifte drikkevannet. Hackerne i USA klarte å øke nivået av lut, brukt til pH-justering, til over 100 ganger normalnivået. Som en følge av dette ble norske kommuner advart om mulige lignende sårbarheter. Angrepet i Drammen rammet heldigvis kun en server uten direkte forbindelse til selve vannforsyningen (Kommunal rapport 2022).

Hvordan kommuner håndterer sensitive personopplysninger, kan også være sårbart. På Romerike har flere hendelser vist utilstrekkelig sikkerhetsnivå ved digitale tjenester. Sensitive opplysninger om en familiekonflikt lå offentlig tilgjengelig på Ullensaker kommunes postliste i halvannen uke høsten 2023 (Romerike blad 2024a). I en annen hendelse delte en lærer i samme kommune personlig helseopplysninger om en elev på storskjerm foran klassen (Romerike blad 2024b). I 2022 mistet en hjemmesykepleier en utskrevet liste med svært sensitive personopplysninger (Romerike blad 2024 c). Fellesnevneren for hendelsene er fravær eller mangel på tekniske løsninger, rutiner og opplæring.

1.1.2 Kontrollutvalgets bestilling av prosjektet

Kontrollutvalget i Ullensaker kommune bestilte en forvaltningsrevisjon om IT-sikkerhet og personvern 17. oktober 2024 (sak 37/24). Revisjonen ble samtidig bedt om å utarbeide en prosjektplan, som ble vedtatt av utvalget 12. desember 2024 (sak 43/24).

En av problemstillingene i planen handlet om IT-sikkerhet i kommunens vann- og avløpssystemer:

> I hvilken grad har kommunen satt inn tilstrekkelige tiltak for å fange opp og hindre forsøk på datainnbrudd på kommunens vann- og avløpssystemer, samt etablert planverk for å håndtere denne typen hendelser.

Etter at prosjektplanen ble vedtatt, ble revisjonen gjort oppmerksom på at innsyn i dette feltet kunne kreve sikkerhetsklarering. Kontrollutvalget ble orientert om dette 30. januar 2025 (sak 2/25), og ba revisjonen avklare situasjonen nærmere. Våre undersøkelser viste at vi ikke kunne besvare problemstillingen uten å søke om sikkerhetsklarering, og at deler av rapporten i så fall måtte sladdes.

Kontrollutvalget vedtok derfor 13. mars 2025 (sak 8/25) å endre problemstillingen, slik at den heller handlet om IT-sikkerhet innen helsetjenester til hjemmeboende.

1.2 Formål og problemstillinger

Formålet med undersøkelsen er å avdekke eventuelle svakheter i informasjonssikkerheten og ivaretakelsen av personvern i Ullensaker kommune, slik at feil kan rettes og systemer kan gjøres sikrere.

Undersøkelsen har følgende problemstillinger:

1. Har kommunen dokumentert et styringssystem for informasjonssikkerhet og personvern som tilfredsstiller krav i lov, forskrift og etablerte standarder?
2. I hvilken grad har kommunen satt inn tilstrekkelige tiltak for å fange opp og hindre forsøk på datainnbrudd på kommunens tjenester til hjemmeboende, samt etablert planverk for å håndtere denne typen hendelser?
3. Har kommunen sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret i tilstrekkelig grad?

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.

Problemstilling 2 om tiltak for å fange opp og hindre forsøk på datainnbrudd er rettet mot enhet tjenester til hjemmeboende. Mange sentrale tiltak som trekkes frem i etablerte standarder og retningslinjer for å sikre informasjonssikkerhet er imidlertid tiltak som vanligvis gjennomføres av kommunenes it-avdelinger. Gjennomgangen av kommunens arbeid med disse tiltakene vil dermed gjelde for hele kommunen. For tiltak knyttet til etterlevelsen av kommunens prosedyrer og planverk, samt opplæring av ansatte rettes undersøkelsen særskilt til enhet tjenester til hjemmeboende.

1.3.2 Dokumentanalyse

Revisjonen har innhentet og gjennomgått aktuelle dokumenter fra kommunen.

1.3.3 Intervju

For å få supplerende informasjon til de skriftlige kildene, har revisjonen intervjuet utvalgte aktører i Ullensaker kommune som er involvert i eller har ansvar for informasjonssikkerhet og personvern. Revisjonen har intervjuet følgende:

- Rådgiver for informasjonssikkerhet og personvern
- Seniorrådgiver avdeling digitale tjenester
- Personvernombudet i Ullensaker kommune
- Digitaliseringsrådgiver oppvekst
- Enhetsleder og fag- og kvalitetskonsulent ved tjenester til hjemmeboende
- Kommunedirektøren

Intervjuene er gjennomført i perioden 10.4.2025-20.8.2025. Alle intervjuene er referatført og referatene er verifisert i etterkant av aktuell informant, for slik å sikre intervjudataenes pålitelighet.

1.3.4 Stikkprøver

For å undersøke kommunens etterlevelse av aktuelle artikler i personopplysningsforordningen har revisjonen etterspurt dokumenter knyttet til et utvalg digitale læremidler. Revisjonen har plukket ut ti tilfeldige læremidler fra kommunens oversikt over godkjente digitale læremidler. Revisjonen har etterspurt registreringer i behandlingsprotokollen, risikovurderinger, vurderinger av personvernkonsekvenser (DPIA) og databehandleravtaler for disse ti læremidlene.

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 ble sendt administrasjonen i sin helhet til gjennomgang og uttalelse 5.12.2025. Vi har mottatt tilbakemeldinger til faktagrunnlaget og feil er rettet opp.

Revisjonen mener 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 9.1.2026 og uttalelsen er lagt ved rapporten i vedlegg 1.

Kommunedirektørens uttalelse til rapporten inneholder faktakorrigeringer, kommentarer til vurderinger og konklusjoner, samt tilleggsinformasjon om gjennomførte tiltak og pågående arbeid knyttet til informasjonssikkerhet og personvern.

1.5 Revisjonskriterier

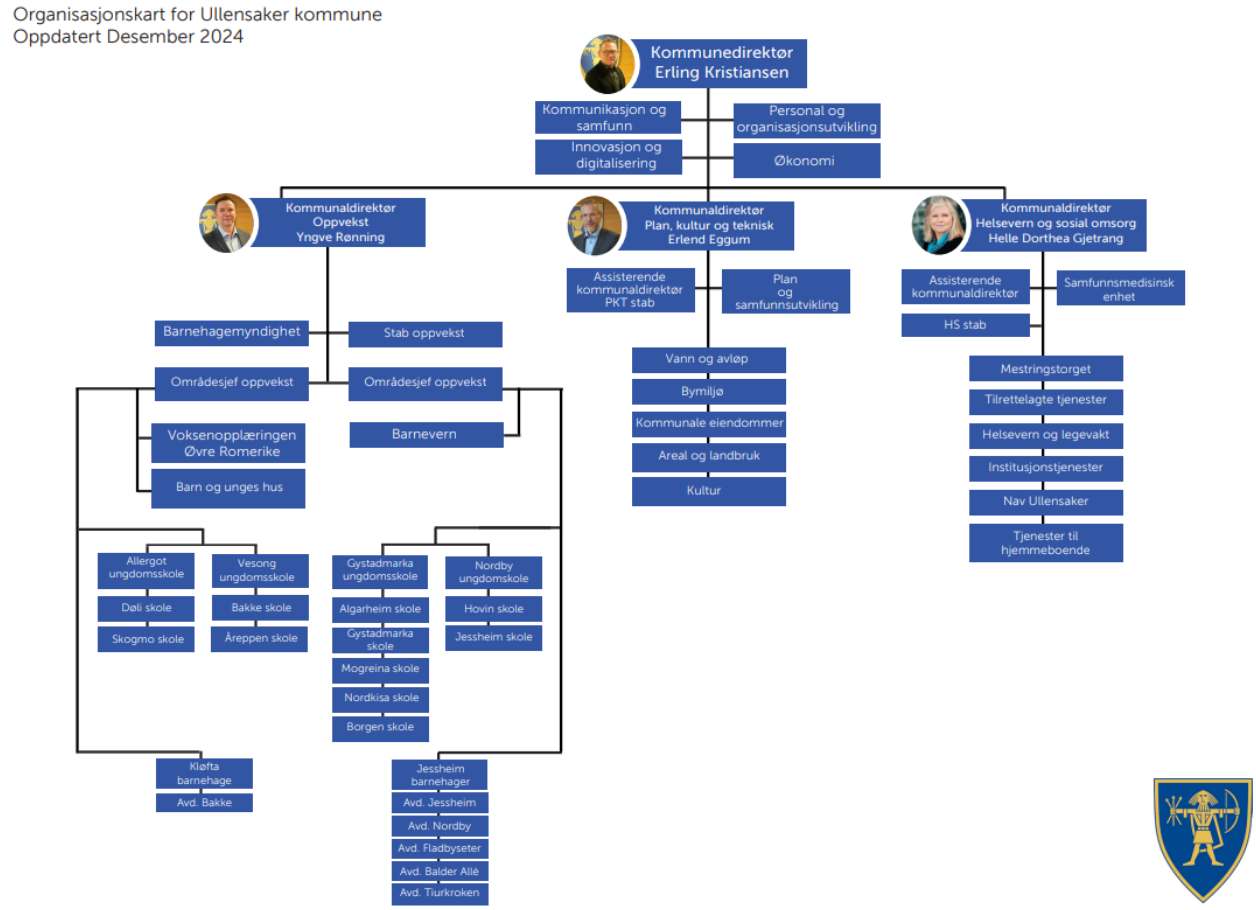
Revisjonskriterier er de krav og forventninger som kommunen vurderes opp mot. Kriteriene utledes fra lover og forskrifter, kommunestyrets vedtak og hva som anses som god forvaltningsskikk og faglig anerkjente normer på området. I dette prosjektet er revisjonskriteriene blant annet hentet fra kommuneloven, personopplysningsloven, eForvaltningsforskriften og standarder for

informasjonssikkerhet basert på ISO/IEC 27001. Kriteriene er nærmere presentert innledningsvis i kapittel 2, 3 og 4, og i vedlegg 2 i rapporten.

1.6 Organisering av arbeidet med informasjonssikkerhet og personvern i Ullensaker kommune

I Ullensaker kommune er IKT-drift, herunder rådgiver for informasjonssikkerhet og personvern og digitaliseringsrådgiver oppvekst, organisert under enhet innovasjon og digitalisering (se figur 1).

Figur 1 Organisasjonskart for Ullensaker kommune



Kilde: Ullensaker kommune

Ullensaker har tidligere vært med i IKT-samarbeidet Digitale Gardermoen (DGI), men gikk ut av dette samarbeidet i 2021. Kommunen har i dag en egen IT-avdeling (avdeling digitale tjenester), som er organisert under enhet innovasjon og digitalisering. Enhet innovasjon og digitalisering har dedikerte ressurser knyttet kommunens arbeid med informasjonssikkerhet og personvern.

Problemstilling 3 undersøker arbeidet med personvern ved skolene i Ullensaker. Kommunen har elleve barneskoler og fire ungdomsskoler. Skolene er organisert under virksomhetsområdet oppvekst.

Problemstilling 2 tar for seg arbeidet med hendelseshåndtering i enhet for tjenester til hjemmeboende som er organisert under virksomhetsområdet helsevern og sosial omsorg. Enheten består av:

- Hjemmesykepleie og praktisk bistand øst inkludert felles natt-tjeneste
- Hjemmesykepleie og praktisk bistand nordvest
- Hjemmesykepleie og praktisk bistand sør
- Lavterskel og mestring (inneholder blant annet kartleggingsteam, mestringsteam, digital hjemmeoppfølging, friskliv, med mer)
- Fysioterapi, ergoterapi og hjelpemidler (inkludert serviceteknikere)
- Aktivitet og fellestjenester, med ti underavdelinger. Underavdelingene består av tre dagsenter, tre kaféer, to «hjerterom», ett sentralkjøkken, samt service og transport

Kilde: Intervju med enhetsleder 19.6.2025.

1.7 Begrepsforklaringer

Informasjonssikkerhet og IKT-sikkerhet: Informasjonssikkerhet er krav til pålitelighet og sikkerhet knyttet til (sensitiv) informasjon (NAOB udatert). Informasjonssikkerhet handler om å sikre at informasjon i alle former ikke blir kjent for uvedkommende, ikke blir endret utilsiktet eller av uvedkommende og å sikre at informasjonen er tilgjengelig ved behov (Digdir udatert). IKT-sikkerhet (informasjons- og kommunikasjonsteknologi) handler om å beskytte IKT-systemer og informasjonen i disse. Med andre ord handler IKT-sikkerhet om beskyttelse av det som er sårbart fordi det er koblet til eller er avhengig av informasjons- og kommunikasjonsteknologi (Meld. St. 38 2016-2027, s. 14).

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 og styring av informasjonssikkerhet og ledelsessystem, jf. Digdir sin veileder *Internkontroll i praksis – Informasjonssikkerhet*.

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, lagring, utlevering og sletting av personopplysninger (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.

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.

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.

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 u.å).

1.8 Rapportens oppbygning

Kapittel 2 tar for seg problemstilling 1 i undersøkelsen og handler om kommunens styringssystem for informasjonssikkerhet. Kapittel 3 tar for seg problemstilling 2 om kommunens tiltak for å fange opp og hindre forsøk på datainnbrudd på kommunens IKT-systemer for tjenester til hjemmeboende. Kapittel 4 tar for seg problemstilling 3, som handler om kommunens arbeid med å sikre personopplysninger på skoleområdet. Det siste kapitlet oppsummerer funnene fra revisjonen gjennom 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 vi 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 Ullensaker 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

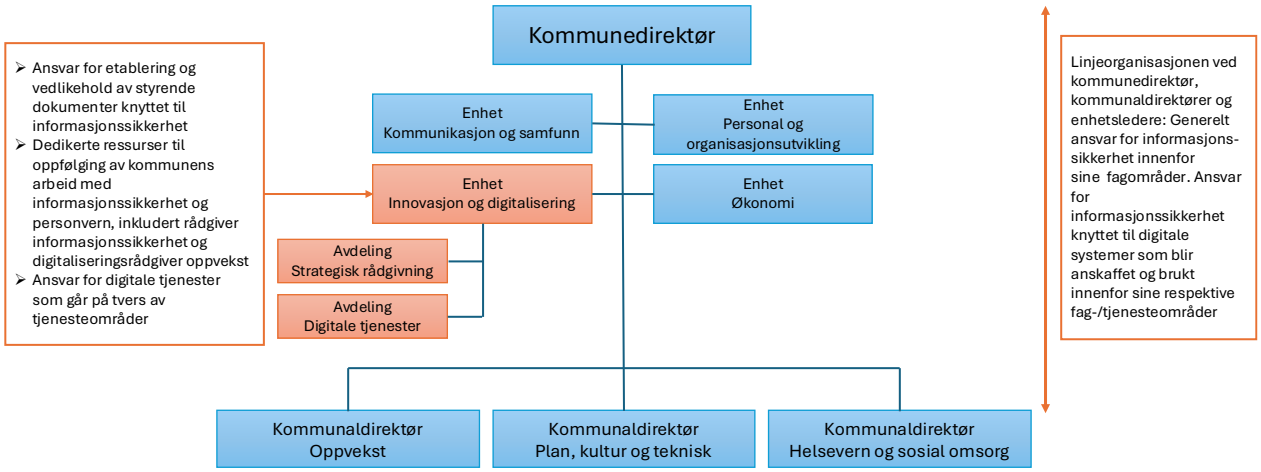
2.2 Kommunens styringssystem for informasjonssikkerhet

2.2.1 Organisering av arbeidet med informasjonssikkerhet i Ullensaker kommune

Arbeidet med informasjonssikkerhet i Ullensaker kommune er fordelt mellom enhet innovasjon og digitalisering og de ulike fag- og tjenesteområdene. Enhet innovasjon og digitalisering har ansvaret for informasjonssikkerheten knyttet til IT-systemene som går på tvers av de ulike tjenesteområdene. Enhetslederne har ansvaret for informasjonssikkerheten innenfor sine tjenesteområder (intervju med seniorrådgiver digitale tjenester; e-post til revisjonen 20.8.2025).

Enhet innovasjon og digitalisering har et særskilt ansvar og har blant annet ansvar for å vedlikeholde prosedyrer, sjekklister og maler knyttet til informasjonssikkerhet og personvern. Rådgiver for informasjonssikkerhet og personvern skal gi råd om hvordan kommunen best mulig kan ivareta informasjonssikkerhet og personvern. Rådgiver for informasjonssikkerhet og personverns oppgaver er blant annet å etablere og forvalte internkontrollsystemet for informasjonssikkerhet og personvern. Det innebærer også å samarbeide med andre enheter i kommunen for å etablere god informasjonssikkerhet (Ullensaker kommune 2021d).

Figur 2 Illustrasjon av organiseringen av arbeidet med informasjonssikkerhet i kommunen



Kilde: Revisjonens illustrasjon, basert på kommunens organisasjonskart, styrende dokumentasjon og beskrivelser fra intervjuer.

2.2.2 Styrende dokumenter for informasjonssikkerhet

Som ansvarlig for internkontrollen i kommunen skal kommunedirektøren utarbeide en beskrivelse av virksomhetens hovedoppgaver, mål og organisering, samt ha nødvendige rutiner og prosedyrer og evaluere skriftlige prosedyrer og andre tiltak for internkontroll og forbedre disse ved behov (kommuneloven § 25-1).

Ullensaker kommune har en retningslinje for internkontroll som beskriver den generelle internkontrollen i kommunen. Retningslinjen beskriver roller og ansvar i linjeorganisasjonen, samt de ulike elementene som inngår i kommunens internkontroll. Blant annet vises det til at kommunedirektøren skal gjennomføre ledelsens gjennomgang årlig (jf. kapittel 2.2.4) og at kommunaldirektørene skal sikre at risikovurderinger er tilfredsstillende ivaretatt i egen sektor (jf. kapittel 2.2.5) (Ullensaker kommune 2021c).

Mens kommuneloven § 25-1 stiller krav til internkontroll i kommunen generelt, stiller eForvaltningsforskriften krav til internkontroll på informasjonssikkerhetsområdet spesielt. Kommunen skal etter forskriftens § 15 ha sikkerhetsmål og en sikkerhetsstrategi som beskriver mål og strategi for kommunens internkontroll.

Revisjonen har mottatt dokumentet *Strategi for informasjonssikkerhet og personvern i Ullensaker kommune*, som ifølge kommunen utgjør fundamentet for kommunens internkontroll på området (e-post 25.8.2025). Strategien består av en styrende, utøvende og kontrollerende del. I den styrende delen vises det til krav i personopplysningsloven, norm for informasjonssikkerhet og den kommunale beredskapsplikten om regelmessig internkontroll i form av etablering og vedlikehold av planlagte og systematiske tiltak.

Kommunen opplyser i e-post til revisjonen at kommunen i sin strategi på fagområdet både implisitt og eksplisitt har definert sikkerhetsmål som sikrer konfidensialitet, integritet og tilgjengelighet (e-post 25.8.2025).

Under overskriften «Styrende dokumentasjon» i strategien oppgis følgende:

> All behandling av informasjon for kommunen 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.

Disse målene er imidlertid ikke omtalt som sikkerhetsmål i strategien.

Videre beskriver den styrende delen av kommunens strategi for informasjonssikkerhet rollene behandlingsansvarlig, personvernombud og rådgiver informasjonssikkerhet og personvern.

Ifølge den utøvende delen av kommunens sikkerhetsstrategi blir utøvende dokumentasjon ivaretatt i felles prosedyrer, sjekklister og maler om informasjonssikkerhet og personvern. Videre skal det ifølge strategien gjennomføres en risikovurdering før personopplysninger behandles, før et informasjonssystem blir tatt i bruk og ved endringer i forhold som kan påvirke informasjonssikkerheten.

I den kontrollerende delen av kommunens strategi for informasjonssikkerhet vises det til at uønskede hendelser blir håndtert i henhold til gjeldende prosedyrer (se kapittel 3.2.5) og at det gjennomføres ledelsens gjennomgang årlig (se kapittel 2.2.4).

En ny strategi for innovasjon og digitalisering ble vedtatt i kommunestyret 2.12.2025.

Ut over dokumentene nevnt over har Ullensaker kommune en rekke andre regler, prosedyrer og sjekklister som skal bidra til å ivareta informasjonssikkerheten i kommunen. På forespørsel om å få tilsendt dokumentasjon på internkontrollsystemet, organisering, roller og ansvar, samt rutiner og prosedyrer knyttet til informasjonssikkerhet har revisjonen mottatt disse dokumentene:

- Reglement for informasjonssikkerhet og personvern
- Prosedyre for arbeidsgivers innsyn i arbeidstakeres e-post og personlige filer
- Prosedyre for brukertilgang til sak-arkivsystemet
- Prosedyre for dokumentstyring i kvalitetssystemet
- Prosedyre for håndtering av IKT-sikkerhetshendelser
- Prosedyre for ledelsens gjennomgang av internkontrollsystemet
- Prosedyre for når ansatt slutter i Ullensaker kommune
- Prosedyre for retting og sletting av personopplysninger
- Prosedyre for tapt eller stjålet data- og telefonutstyr
- Prosedyre for varsling av hendelser på kommunens IT-tjenester
- Prosedyre for å håndtere personvernavvik
- Prosedyre for å underrette den registrerte ved brudd på personopplysningssikkerheten

2.2.3 Oppgave-, rolle- og ansvarsfordeling

Revisjonen legger til grunn at kommunen skal ha en organisering med klar oppgave-, rolle- og ansvarsfordeling for informasjonssikkerhet. De generelle ansvarsområdene for kommunedirektør, kommunaldirektør og enhetsleder er beskrevet i kommunens retningslinje for internkontroll (Ullensaker kommune 2021c). Ifølge retningslinjen har kommunedirektøren ansvar for å gjennomføre ledelsens gjennomgang og foreta en overordnet risikovurdering av alle områdene i kommunen. Enhetsledere har ansvar for å etablere et helhetlig system for internkontroll i egen virksomhet, mens kommunaldirektørene har ansvar for å påse at underliggende enheter har etablert system for internkontroll. Retningslinjen for internkontroll beskriver det generelle linjeansvaret i internkontrollen og omtaler ikke rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet spesielt. Linjeansvaret går imidlertid igjen i kommunens prosedyrer og retningslinjer, inkludert kommunens reglement for informasjonssikkerhet og personvern og prosedyre for håndtering av IKT-sikkerhetshendelser.

Det fremgår ikke i dokumentasjonen revisjonen har gjennomgått hvordan roller og ansvar knyttet til informasjonssikkerhet er fordelt mellom tjeneste-/fagområdene og enhet innovasjon og digitalisering. Revisjonen får opplyst i intervjuer at de ulike tjenesteområdene har ansvar for informasjonssikkerheten innenfor sine tjenesteområder, mens enhet innovasjon og digitalisering har ansvaret for informasjonssikkerheten knyttet til IT-systemene som går på tvers av de ulike tjenesteområdene (intervjuer med seniorrådgiver digitale tjenester og kommunedirektør, samt e-post til revisjonen 5.1.2026).

Rollene behandlingsansvarlig, personvernombud og rådgiver informasjonssikkerhet og personvern er som nevnt lenger opp beskrevet i kommunens strategi for informasjonssikkerhet (2021d). Oppsummert er disse tre rollene beskrevet slik i strategien:

- **Behandlingsansvarlig** (Ullensaker kommune, ved kommunedirektøren) har ifølge strategien ansvaret for at all behandling av personopplysninger, og annen sensitiv informasjon, foregår etter gjeldende lov- og regelverk. Det samme gjelder for den informasjon som behandles av eksterne aktører og interkommunale selskaper på vegne av kommunen.
- **Personvernombudet** skal være en uavhengig ressursperson som skal gi råd om hvordan den behandlingsansvarlige best mulig kan ivareta personverninteressene.
- **Rådgiver informasjonssikkerhet og personvern**, i enheten innovasjon og digitalisering, skal være en ressurs som gir råd om hvordan kommunen best mulig kan ivareta informasjonssikkerhet og personvern. Rådgiver informasjonssikkerhet og personvern skal samarbeide med og bistå personvernombudet.

I strategi for informasjonssikkerhet og personvern vises det til en retningslinje for systemforvaltning i Ullensaker kommune (Ullensaker kommune 2021e). Revisjonen mottok ikke denne retningslinjen på forespørsel om dokumentasjon som viser kommunens organisering av arbeidet med informasjonssikkerhet og personvern. Det er derfor uklart for revisjonen om retningslinjen er oppdatert og gjeldende for dagens praksis og om den er kjent i organisasjonen. Rådgiver personvern og informasjonssikkerhet informerer i e-post til revisjonen 25.11.2025 om at kommunen arbeider med en ny forvaltningsmodell i forbindelse med ny strategi for enhet innovasjon og digitalisering.

Retningslinjen beskriver fire roller i systemforvaltningen: Systemeier, systemforvalter (digitaliseringsrådgiver), systemadministrator og superbruker. Systemforvalter/ digitaliseringsrådgivere er ifølge retningslinjen plassert i kommunens IT-tjeneste (avdeling digitale tjenester, under enhet innovasjon og digitalisering). De øvrige rollene er plassert i linjeorganisasjonen. I intervjuer med seniorrådgiver avdeling digitale tjenester, digitaliseringsrådgiver oppvekst og enhetsleder tjenester til hjemmeboende beskrives rolle- og ansvarsfordelingen mellom digitale tjenester og tjenesteområdene noe ulikt.

Ullensaker kommune har en digitaliseringsrådgiver på oppvekstområdet. Stillingen er organisert under avdeling strategisk rådgivning i enhet innovasjon og digitalisering. Innenfor oppvekstområdet er det opprettet et digitaliseringsråd som et prøveprosjekt, som varer frem til årsslutt 2025. Digitaliseringsrådet jobber ifølge digitaliseringsrådgiver med risikovurderinger av digitale læringsressurser og mer strategiske avgjørelser, som innføring av kunstig intelligens (intervju med digitaliseringsrådgiver oppvekst).

Enhetsleder for tjenester til hjemmeboende forteller i intervju at de har systemeiere og koordinatorer for de ulike løsningene. Hun forteller at dersom det er ønske om å innføre et nytt system i enheten, så går de via avdeling digitale tjenester. Digitale tjenester vurderer da blant annet konsekvenser for personvern. Enhetsleder forteller i intervju at avdelingsledere har bestillingsmyndighet for utvidede roller, men kun innenfor sine respektive fagsystem (se kapittel 3.2.2 for en beskrivelse av tilganger til digitale systemer). Kommunen oppgir i tilbakemelding til faktabeskrivelsen at de har digitaliseringsrådgivere knyttet til helsevern og sosial omsorg.

Digitaliseringsrådgiver oppvekst forteller i intervju at det før var sektorene som hadde ansvar for risikovurderinger av digitale læremidler. Det var da den aktuelle læreren som meldte inn ønske om å innføre et digitalt læremiddel som skulle gjennomføre risikovurderingen, men få støtte til gjennomføringen. Digitaliseringsrådgiver forteller videre at kommunen nå har et prøveprosjekt med

et digitaliseringsråd for skolesektoren, som vurderer risiko av digitale læremidler og har myndighet til å godkjenne anskaffelser av nye digitale læremidler. Det er også digitaliseringsrådet som aksepterer restrisiko. Når dette rådet har godkjent læremiddelet, melder de fra til avdeling digitale tjenester om at læremidlet kan kjøpes inn. Digitaliseringsrådet består av digitaliseringsrådgiver oppvekst, pedagogisk digital veileder og fire lærere. Digitaliseringsrådgiver forteller videre at hver skole har en superbruker, som har utvidede tilganger til de digitale løsningene som brukes ved skolene. I tillegg har rektor ved hver skole mulighet til å gi tilganger til systemene skolene bruker.

Digitaliseringsrådgiver oppvekst forteller i intervju at skoleområdet hadde et etterslep på risikovurderinger av digitale læremidler da hun startet i stillingen i juni 2023. Det ble da satt i gang et arbeid med risikovurderinger av digitale læremidler og begrense tilgangene tilgangen til digitale læremidler som var i bruk i skolene. Hun forteller at det nå er gjennomført risikovurderinger av 120 læringsressurser. Hun mener kommunen i dag har oversikt over systemer hvor elevers personopplysninger lagres.

Ullensaker kommune har tidligere hatt en rolle med tittelen fagansvarlig digitale tjenester. Det henvises til denne rollen i flere av kommunens prosedyrer, blant annet *Prosedyre for håndtering av IKT-sikkerhetshendelser* (Ullensaker kommune 2023c) og *Prosedyre for varsling av hendelser på kommunens IT-tjenester* (Ullensaker kommune 2021b). Seniorrådgiver ved avdeling digitale tjenester forteller i intervju at kommunen nylig har ansatt en avdelingsleder for digitale tjenester som starter opp 1. oktober og som vil ta over ansvar og oppgaver som hittil har ligget til fagansvarlig digitale tjenester. Revisjonen har mottatt et dokument som gir en oversikt over oppgavene knyttet til stillingen fagansvarlig digitalisering. Dokumentet er ikke datert, men ifølge kommunen viser dokumentet hvordan oppgavene til den tidligere fagansvarlige har vært delegert til øvrige ressurspersoner i perioden stillingen ikke har vært besatt. Oppgavene er fordelt mellom personer ansatt i enhet innovasjon og digitalisering. Hvem som har ivaretatt rollen som ivaretar fagansvarlig digitaliserings rolle ved beredskaps-/sikkerhetshendelser står imidlertid som uavklart i dette dokumentet, med henvisning til at dette skal avgjøres i strategisk styringsgruppe (Ullensaker kommune, udatert h; e-post til revisjonen 5.1.2026). Revisjonen har videre mottatt en liste over stedfortredere, som viser stedfortredere ved hendelser.

Ifølge seniorrådgiver digitale tjenester har ikke ansvarsforholdene knyttet til informasjonssikkerhet ligget fast til én rolle, men til enkeltpersoner. Dette har ført til at ansvarsforholdene har endret seg ut ifra hvem som til enhver tid har vært ansatt i kommunen. Seniorrådgiver ved digitale tjenester forteller i intervju at han for eksempel savner en avklaring på hvem som stoppe innkjøp av applikasjoner og maskinvarer som ikke har tilstrekkelig sikkerhet.

Kommunen opplyser om at det er startet opp et arbeid med ny forvaltningsmodell i forbindelse med ny strategi for enhet innovasjon og digitalisering (e-post til revisjonen 25.9.2025).

2.2.4 Ledelsens gjennomgang

Det er anbefalt å gjennomføre ledelsens gjennomgang av informasjonssikkerhet årlig (Digdir 2025; Datatilsynet 2025).

Ifølge Ullensaker kommunes retningslinjer for internkontroll skal kommunedirektøren årlig evaluere året som har gått gjennom ledelsens gjennomgang. Videre sier retningslinjen at kommunedirektøren skal foreta en risikovurdering av alle områdene i kommunen og prioritere fokusområder for

kommende år (Ullensaker kommune 2021c). Revisjonen har mottatt kommunens mal for den årlige risikovurderingen. Informasjonssikkerhet og personvern er ett av fem områder hvor det skal gjøres en risikovurdering. Etter malen skal det for hvert av de fem områdene gjøres en vurdering av om felles reglement er etablert, oppdatert og etterlevd, samt beskrive begrunnelser for vurderingen, eventuelle utfordringer og tiltak for området (Ullensaker kommune udatert b).

Kommunedirektør forteller i intervju at ledelsens gjennomgang av informasjonssikkerhet og personvern ikke gjennomføres i kommunens øverste ledelse[1]. Kommunedirektør viser til at strategisk ledergruppe følger med på området informasjonssikkerhet og personvern ved at kommunalsjefer og enhetsledere tar opp temaer og utfordringer som dukker opp. Informasjonssikkerhet og personvern er derfor ikke et tema som gjennomgås til faste tidspunkter, for eksempel en gang i året. Ved brudd på personopplysningsloven, kan for eksempel strategisk ledergruppe gjennomgå lærdommer fra hendelsen og vurdere hvordan hendelsen kan lukkes. Et eksempel er en hendelse fra 2022, hvor sensitive personopplysninger om en elev ble vist på storskjerm foran en skoleklasse. I etterkant av denne hendelsen ble det ifølge kommunedirektør blant annet innført en regel i kommunen om at Outlook ikke skal være åpen i situasjoner hvor det kan være fare for at uvedkommende ser skjermen.

Kommunen informerer i e-post til revisjonen 5.1.2026 at kommunens prosedyre for ledelsens gjennomgang i løpet av 2025 har blitt revidert. Ny prosedyre ble vedtatt av SLG 24.11.2025 (Ullensaker kommune 2025d). Revisjonen har mottatt denne prosedyren. I den reviderte prosedyren presiseres det at ledelsens gjennomgang av internkontrollsystemet inkluderer informasjonssikkerhet og personvern (Ullensaker kommune 2025c).

2.2.5 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). Videre skal identifisert risiko håndteres ved å etablere og følge opp tiltak, samt fastsette hvor stor restrisiko kommunen aksepterer (NSM 2024).

Ifølge Ullensaker kommunes strategi for informasjonssikkerhet og personvern skal det gjennomføres en risikovurdering før personopplysninger behandles og før man tar i bruk et informasjonssystem (Ullensaker kommune 2021d). Ifølge kommunens prosedyre for gjennomføring og oppfølging av risikovurderinger er kvalitetssystemet TQM kommunens hovedverktøy for å gjennomføre, dokumentere og følge opp risikovurderinger. Ifølge prosedyren er det enhetsledere som er ansvarlig for å gjennomføre risikovurderinger av bestemte områder eller arbeidsprosesser (Ullensaker kommune 2022b). Et unntak fra dette er risikovurderinger av digitale læremidler som brukes i skolene, hvor kommunen har et prøveprosjekt med et digitaliseringsråd som risikovurderer, aksepterer risikonivå og godkjenner digitale læremidler (intervju med digitaliseringsrådgiver). Revisjonen er ikke kjent med om kommunen planlegger å videreføre denne ordningen etter at prøveprosjektet utgår ved årsslutt 2025.

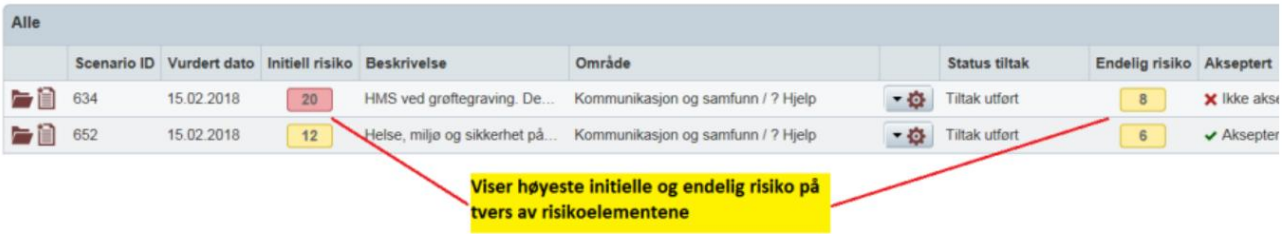
[1] Kommunens øverste ledelse er kommunedirektørens strategiske ledergruppe (SLG), som består av kommunedirektør, kommunaldirektørene, samt enhetslederne for de fire støttefunksjonene kommunikasjon og samfunn, innovasjon og digitalisering, personal og organisasjonsutvikling og økonomi.

Revisjonen har mottatt veileder for risikovurdering av informasjonssikkerhet og personvern av IT-systemer (Ullensaker kommune 2023e). Veilederen inneholder en tabell med risikoelementer som bør vurderes under gjennomføringen av en risikovurdering (Ullensaker kommune 2023e). Kommunen har en mal for risikovurderinger som skal brukes i de tilfellene risikovurderingene ikke kan gjennomføres direkte i TQM. Revisjonen har mottatt denne malen (Ullensaker kommune udatert d).

Videre har administrasjonen i et møte illustrert for revisjonen hvordan risikovurderinger registreres i TQM, samt oversendt en presentasjon som kommunen bruker i et kurs for opplæring i ROS (Ullensaker kommune 2025a). Prosessen med å gjennomføre risikovurderinger starter med å beskrive scenarioet (hva som skal risikovurderes). Deretter identifiseres det hvilke uønskede hendelser som er relevante for den aktuelle risikovurderinger, aktuelle risikoreduserende tiltak, samt at det gjennomføres en endelig risikovurdering med aksept av gjenværende risiko. Etter at risikovurderingen er ferdigstilt skal det registreres i TQM hvem som er ansvarlig for revisjon av risikovurderingen, i tillegg til dato for neste gjennomgang (Ullensaker kommune 2025a).

Figuren under viser hvordan oversikten over risikovurderinger ser ut i TQM. Oversikten viser hva risikonivået var innledningsvis og hva som var endelig risikonivå etter gjennomførte tiltak. Oversikten viser videre hvorvidt restrisiko er akseptert.

Figur 3 Illustrasjon av hvordan oversikt over risikoanalyser ser ut i TQM



Kilde: Ullensaker kommune 2025a

Revisjonen har gjennomgått to risikovurderinger som er gjennomført ved enheten tjenester til hjemmeboende. Disse er gjennomført i TQM. Risikovurderinger er, etter hva revisjonen kan vurdere, gjennomført i henhold til prosessen som er beskrevet over.

Når en risikovurdering er gjennomført opprettes det ifølge rådgiver informasjonssikkerhet og personvern en tiltaksplan i TQM. Rådgiver som står for gjennomføringen av risikovurderingen eller avdelingsleder som har skrivetilgang til vurderingene oppretter tiltak og delegerer disse til ansatte som skal ha ansvaret for gjennomføringen av tiltaket. Det settes lukkefrister på tiltakene og de som får ansvar for tiltaket varsles automatisk gjennom systemet. Rådgiver for informasjonssikkerhet og personvern forteller videre at det er enhetslederne som er ansvarlige for å godkjenne risikovurderinger innenfor sine enheter.

Digitaliseringsrådgiver oppvekst forteller i intervju at de ikke bruker malen i TQM når de gjennomfører ROS-analyser på skoleområdet, fordi de mener malen i TQM blir for omfattende. De bruker i stedet et forenklet excel-ark.

Kommunen gjennomførte i 2024 en overordnet risikovurdering av internkontrollen for henholdsvis enhet digitale tjenester og på kommunenivå. Risikovurderingen som ble gjennomført på

kommunenivå vurderte at reglement for informasjonssikkerhet og personvern er etablert, men at reglementet er under revisjon av enhet innovasjon og digitalisering i samarbeid med personvernombudet. Videre viser risikovurderingen til at det er varierende etterlevelse av reglementet i enhetene og behov for økt bevisstgjøring og forståelse. I risikovurderingen står det videre at det er et ønske om mer oppfølging fra personvernombudet og at det pågår et arbeid rundt vann og avløp og nye krav til sikkerhet (Ullensaker kommune 2025e). Overordnet risikovurdering av internkontrollen gjennomført av enhet innovasjon og digitalisering har likelydende vurderinger for om retningslinjer om informasjonssikkerhet og personvern er etablert og oppdatert. Under etterlevelse av rutinene suppleres det i tillegg med at det er behov for periodiske øvelser og å ha dilemmatrening tilgjengelig på ansattportalen (Ullensaker kommune 2025f). Både for risikovurderingen på kommunenivå og for enhet innovasjon og digitalisering er det definert tiltak, ansvar og frist for gjennomføringen av tiltakene er satt.

I 2023 ble det gjennomført overordnet ROS (risikovurdering) for Ullensaker kommune. Ullensaker kommune har også deltatt i en regional ROS for kommunene i Gardemoenregionen. I den kommunale overordnede ROS-analysen ble bortfall av IKT-løsninger gjennomgått som scenario. I den regionale ROS-analysen ble bortfall av IKT og telefoni gjennomgått som scenario. Begge risikovurderingene ble gjennomført etter samme mal og inneholder blant annet en beskrivelse av eksisterende tiltak og hvordan tiltakene fungerer, vurderinger av hvordan den uønskede hendelsen vil påvirke kritiske samfunnsfunksjoner og -tjenester, samlede vurderinger av sårbarhet og konsekvenser og mulige sannsynlighetsreduserende og konsekvensreduserende tiltak.

Rådgiver informasjonssikkerhet og personvern informerer om at det er planlagt en risikovurdering om informasjonssikkerhet og personvern som skal gjennomføres for hele organisasjonen høsten 2025. Risikovurderingen skal være en fullstendig vurdering av alle avdelinger i kommunen. Rådgiver for informasjonssikkerhet og personvern forteller i intervju at enhet innovasjon og digitalisering har laget punktene i risikovurderingen i samarbeid med dokumentsenteret.

2.3 Revisjonens vurdering

Revisjonens vurdering er at kommunen har utarbeidet styrende dokumenter for informasjonssikkerhet. Flere av de styrende dokumentene fremstår imidlertid som utdaterte med hensyn dagens organisering av arbeidet med informasjonssikkerhet. Videre kommer det etter revisjonens syn ikke tydelig frem i sikkerhetsstrategien hva som er kommunens sikkerhetsmål.

Revisjonens vurdering er at de styrende dokumentene ikke gjenspeiler dagens rolle- og ansvarsfordeling knyttet til informasjonssikkerhet. Det går for eksempel ikke frem fra de styrende dokumentene hvem som har det overordnede ansvaret for å holde oversikt over de digitale systemene som er i bruk i kommunen. Hver enhet skal ha oversikt over systemene de selv anskaffer. Enhet innovasjon og digitalisering har, etter det revisjonen har fått opplyst, oversikt over de digitale systemene de selv administrerer, men kun i noen grad systemene som anskaffes og brukes i de ulike tjenesteområdene. En konsekvens av at styrende dokumenter ikke gjenspeiler dagens organisering og praksis kan være at roller og ansvar blir uklare i situasjoner hvor ansatte slutter i kommunen. Rollen fagansvarlig digitale tjenester er nevnt i flere av kommunens styrende dokumenter for informasjonssikkerhet og i kommunens plan for hendelseshåndtering. På undersøkelsestidspunktet var det imidlertid ingen som hadde denne rollen. Kommunen opplyser om at oppgavene knyttet til rollen har vært delegert til øvrige ansatte i enhet innovasjon og digitalisering

(e-post til revisjonen 5.1.2026). Det fremgår imidlertid ikke av dokumentasjonen revisjonen har mottatt hvem som har hatt hovedansvaret for håndteringen av kritiske og alvorlige IKT-sikkerhetshendelser. Kommunen har en retningslinje for systemforvaltning som sist var oppdatert i 2021, men revisjonen har ikke fått klarhet i hvorvidt denne retningslinjen viser et oppdatert bilde over systemforvaltningen i kommunen i dag.

Ullensaker kommune gjennomfører ikke ledelsens gjennomgang av informasjonssikkerhet i strategisk ledergruppe. Når internkontrollen med informasjonssikkerhet ikke er systematisert gjennom jevnlige gjennomganger i kommunens øverste ledelse, gir dette etter revisjonens vurdering risiko for at kontrollen med informasjonssikkerhet skjer ad hoc og at arbeidet med informasjonssikkerhet i kommunen ikke er tilstrekkelig forankret i kommunens øverste ledelse.

Revisjonens vurdering er at kommunen har et system for gjennomføring av risikovurderinger, etablering av tiltak og aksept av risikonivå.

3 DATAINNBRUDD – TJENESTER TIL HJEMMEBOENDE

3.1 Problemstilling og revisjonskriterier

For å undersøke hvordan kommunen arbeider for å fange opp og hindre forsøk på datainnbrudd i tjenester til hjemmeboende har revisjonen i all hovedsak tatt utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet. I denne sammenheng er det sentralt at kommunen har etablert sikkerhetsovervåkning, har kontroll på identiteter og tilganger, gjennomfører inntrengingstester og om det er etablert planverk for hendelseshåndtering. Å overvåke kommunens IT-systemer er viktig for å oppdage og reagere på sikkerhetstrusler tidlig. Kontroll på identiteter og tilganger er viktig for å hindre at angripere kommer seg inn i kommunens IT-systemer ved å ta over brukerkontoene til ansatte og andre brukere av kommunens systemer. NSMs grunnprinsipper trekker videre frem gjennomføring av jevnlige inntrengingstester som et viktig tiltak for å teste egen forsvarsevne, avdekke sårbarheter og mangler og vurdere egen beredskap. Når hendelsen først har inntruffet er det avgjørende at kommunen har en plan for hendelseshåndtering for å begrense skaden og gjenopprette normaltilstanden.

I tillegg har revisjonen lagt til grunn i undersøkelsen at tiltak knyttet til opplæring av ansatte er nødvendig for å sikre god informasjonssikkerhet.

Problemstillingen i denne undersøkelsen er rettet mot systemer knyttet til hjemmebaserte tjenester, men mange av tiltakene som anbefales for å fange opp og hindre forsøk på datainnbrudd gjennomføres sentralt i kommunen. I beskrivelsene i kapittel 3.2 under vil vi derfor vise til generelle systemer og rutiner der dette er aktuelt, og beskrive data for hjemmetjenesten spesielt, der dette passer.

For problemstilling 2 utledes følgende krav og forventninger til kommunen:

Problemstilling 2	Krav og forventninger til kommunen
I hvilken grad har kommunen satt inn tilstrekkelige tiltak for å fange opp og hindre forsøk på datainnbrudd på kommunens systemer knyttet til hjemmebaserte tjenester, samt etablert planverk for å håndtere denne typen hendelser?	Kommunen skal ha → ha etablert sikkerhetsovervåkning → kontroll på identiteter og tilganger → gjennomført inntrengingstester jevnlig, og minst en gang i året → etablert et planverk for hendelseshåndtering og som revideres jevnlig → tiltak som sikrer at ansatte får opplæring i informasjonssikkerhet

3.2 Tiltak for å fange opp og hindre datainnbrudd

3.2.1 Sikkerhetsovervåkning

Kommunen har engasjert en ekstern leverandør som overvåker systemene til enhver tid; Security Operations Center (SOC). Leverandøren leser loggene og overvåker cybersikkerhet i kommunens systemer, og varsler avdeling for digitale tjenester dersom det oppdages unormal aktivitet. Leverandøren kan også sette inn tiltak, som å bytte passord, hvis det oppdages unormal aktivitet fra en bruker (intervju med seniorrådgiver digitale tjenester).

Seniorrådgiver forteller i intervju at avdeling for digitale tjenester, i tillegg til overvåkningen til SOC, har egen overvåkning av systemene som avdelingen drifter. Dersom en applikasjon/system slutter å virke, får avdelingen et varsel. Avdelingen har en døgnbemannet vakttelefon, slik at SOC, ansatte og andre som kan oppdage hendelser alltid kan få tak i noen i avdelingen (intervju med seniorrådgiver digitale tjenester).

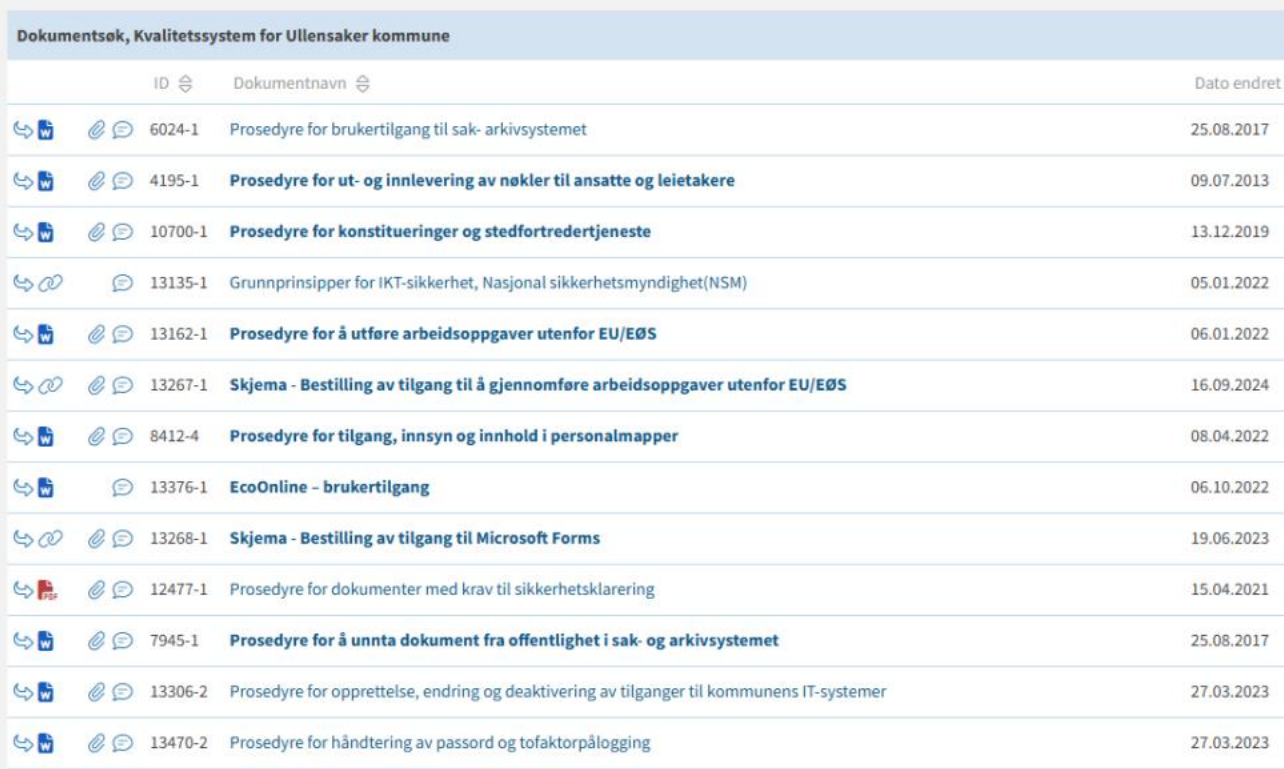
Det henvises til SOC (leverandør av overvåkningstjenester) i kommunens planverk for hendelseshåndtering. Planverket inneholder blant annet en sjekkliste som skal brukes ved IKT-sikkerhetshendelser. Denne sjekklisten inneholder en liste som skal gjennomgås av ressurser fra avdeling for digitale tjenester sammen med SOC. Blant punktene som skal gjennomgås er å sjekke egen overvåkning, kartlegging av hvilke tjenester som kan være kompromittert og ulike tiltak for å begrense konsekvensene av en IT-sikkerhetshendelse (Ullensaker kommune udatert e).

3.2.2 Kontroll på identiteter og tilganger

Ett av NSMs prinsipper knyttet til kartleggingen av brukere og behov for tilganger er prinsippet om å ha kontroll på identiteter og tilganger. Dette er viktig fordi manglende kontroll på tilganger øker risikoen for dataangrep. Prinsippet innebærer blant annet å etablere retningslinjer for tilgangskontroll (NSM 2024).

Ullensaker kommune har ulike prosedyrer som omhandler styring av identiteter og tilganger i kvalitetssystemet. Blant annet har kommunen en prosedyre for brukertilgang til saks- og arkivsystem (Ullensaker kommune 2017). Den skal sikre at ansatte gis tilgang til sak-/arkivsystemet ut ifra de tjenstlige behovene de har til enhver tid, inkludert at tilganger deaktiveres når behovet opphører. Prosedyren ble sist endret i august 2017, og ifølge prosedyren er det en enhet som ikke eksisterer lengre som har ansvaret for at prosedyren holdes ved like og følges opp. Videre har kommunen en prosedyre for når ansatte slutter i kommunen (Ullensaker kommune 2023). Ifølge prosedyren skal brukeren deaktiveres automatisk dagen etter siste arbeidsdag. Prosedyren er sist endret i desember 2023. Figuren under viser prosedyrer knyttet til tilgangsstyring i kvalitetssystemet.

Figur 4 Prosedyrer for tilgangsstyring i kvalitetssystemet



Dokumentsøk, Kvalitetssystem for Ullensaker kommune

ID	Dokumentnavn	Dato endret
6024-1	Prosedyre for brukertilgang til sak- arkivsystemet	25.08.2017
4195-1	**Prosedyre for ut- og innlevering av nøkler til ansatte og leietakere**	09.07.2013
10700-1	**Prosedyre for konstitueringer og stedfortredertjeneste**	13.12.2019
13135-1	Grunnprinsipper for IKT-sikkerhet, Nasjonal sikkerhetsmyndighet(NSM)	05.01.2022
13162-1	**Prosedyre for å utføre arbeidsoppgaver utenfor EU/EØS**	06.01.2022
13267-1	**Skjema - Bestilling av tilgang til å gjennomføre arbeidsoppgaver utenfor EU/EØS**	16.09.2024
8412-4	**Prosedyre for tilgang, innsyn og innhold i personalmapper**	08.04.2022
13376-1	**EcoOnline – brukertilgang**	06.10.2022
13268-1	**Skjema - Bestilling av tilgang til Microsoft Forms**	19.06.2023
12477-1	Prosedyre for dokumenter med krav til sikkerhetsklarering	15.04.2021
7945-1	**Prosedyre for å unnta dokument fra offentlighet i sak- og arkivsystemet**	25.08.2017
13306-2	Prosedyre for opprettelse, endring og deaktivering av tilganger til kommunens IT-systemer	27.03.2023
13470-2	Prosedyre for håndtering av passord og tofaktorpålogging	27.03.2023

Kilde: Skjermutklipp fra TQM

Seniorrådgiver i avdeling digitale tjenester forteller i intervju at tilgangsstyringen av ansattes tilganger er helautomatisert og følger HR-systemet. Når noen ansettes, blir de tildelt en avdeling med tilhørende tilganger til IKT-systemene knyttet til den aktuelle avdelingen. Når noen slutter i avdelingen slettes tilgangene automatisk. Når det skal opprettes nye avdelinger i kommunen, legger avdeling digitale tjenester inn de systemene avdelingen skal ha tilganger til.

Seniorrådgiver forteller videre at tjenesteområdene i tillegg har egne superbrukere, som administrerer tilgangsstyringen dersom det er behov for andre tilganger enn den automatiserte tilgangsstyringen.

Ifølge enhetsleder for tjenester til hjemmeboende er tilgangsstyringen til de ulike IT-systemene som benyttes i enheten forhåndsbestemt etter hvilken profesjon den enkelte ansatte har. Kun sykepleiere har for eksempel tilgang til kjernejournal. Hun forteller videre at tverrfaglig kartleggingsteam og mestringsteam har utvidete tilganger.

Seniorrådgiver i avdeling digitale tjenester forteller i intervju at kommunen har soneinndeling i IKT-systemene, noe som sørger for god sikkerhet. For eksempel er vanlig ansatte og elever delt inn i ulike soner, så informasjonen er skjult for de ulike rollene. Helsesystemer er helt segmentert fra resten av systemene. Ifølge seniorrådgiver gjør dette at det vil være svært vanskelig å få utvidede tilganger innenfor kommunens systemer uten å involvere avdeling digitale tjenester.

3.2.3 Inntrengingstester

Ett av NSMs grunnprinsipper for IKT-sikkerhet er at det gjennomføres inntrengingstester jevnlig, og minst en gang i året, for å identifisere sårbarheter (NSM 2024).

Seniorrådgiver i digitale tjenester forteller i intervju at det ikke blitt gjennomført inntrengingstester i de to årene han har hatt denne stillingen. Kommunedirektør forteller i intervju at forrige inntrengningstest ble gjennomført i etterkant av dataangrepet mot Østre Toten kommune i 2021. I kommunens veileder for risikovurdering av informasjonssikkerhet og personvern av IT-systemer er hvorvidt det gjennomføres inntrengingstester et punkt som bør vurderes i en risikovurdering (Ullensaker kommune 2023e). Ut over dette har ikke revisjonen har mottatt rutiner, prosedyrer eller annen dokumentasjon som omtaler gjennomføring av inntrengingstester i Ullensaker kommunes IT-systemer.

3.2.4 Planverk for hendelseshåndtering

Ullensaker kommune har en prosedyre for håndtering av IKT-sikkerhetshendelser. Prosedyren beskriver mulige IT-sikkerhetshendelser, fordeler roller og ansvar ved slike hendelser, og konkretiserer hva de forskjellige rollene skal foreta seg. Ved alvorlige og kritiske hendelser er det ifølge prosedyren enhet innovasjon og digitalisering ved stillingen fagansvarlig digitale tjenester som har hovedansvaret (Ullensaker kommune 2023c). Som nevnt i kapittel 2.2.3 har ikke denne stillingen vært besatt under revisjonens datainnhenting, men revisjonen har som nevnt fått opplyst i intervju at det fra oktober 2025 er ansatt en avdelingsleder ved avdeling digitale tjenester som skal dekke det som tidligere lå til denne stillingen (intervju med seniorrådgiver digitale tjenester).

Ifølge kommunens prosedyre for håndtering av IKT-sikkerhetshendelser, skal relevante kommunaldirektører/enhetsledere/systemeiere informeres ved mindre alvorlige hendelser. Ved kritiske hendelser, samt ved alvorlige hendelser, skal kommunaldirektører/enhetsledere/systemeiere bistå ved behov (Ullensaker kommune 2023c). I prosedyren er det definert hva som er kritiske, alvorlige og mindre alvorlige hendelser.

Prosedyren for håndtering av IKT-sikkerhetshendelser viser til flere dokumenter som skal brukes i hendelseshåndteringen. Disse er kontaktliste, liste over stedfortredere, sjekkliste ved IT-sikkerhetshendelser, mal for hendelseslogg og katastrofeplan. Sjekklisten inneholder en rekke tiltak som kan iverksettes ved en hendelse. Det skal krysses av når aktiviteten er vurdert (Ullensaker kommune udatert e).

Rådgiver forteller at hvis SOC ringer, får brukerstøtte telefonen. Brukerstøtte kontakter enhetsleder eller tredjelinje[2]. Deretter iverksettes kommunens prosedyre for håndtering av IKT-sikkerhetshendelser. Hvis det er etter arbeidstid, og kommunens IT-vakt blir kontaktet om hendelsen, så vil IT-vakten melde fra om dette til enhetsleder.

Enhetsleder for tjenester til hjemmeboende forteller i intervju at enheten forholder seg til prosedyrene som ligger i kvalitetssystemet og at prosedyrene ligger til grunn for alt enheten driver med. Ved brudd på informasjonssikkerhet og personvern benytter de seg av ansattportalen for å finne ut hvem man

[2] Avdeling digitale tjenester er organisert etter førstelinje (brukerstøtte), andrelinje (tekniske oppgaver) og tredjelinje (utvikling av nye tjenester, samt håndterer større tekniske oppgavene) (intervju med seniorrådgiver ved digitale tjenester).

skal ta kontakt med. Enhetsleder viser også til prosedyrene i kvalitetssystemet som inneholder beskrivelser av fremgangsmåten for å melde inn uønskede hendelser.

3.2.5 Opplæring i informasjonssikkerhet

Opplæring av ansatte er et sentralt tiltak for å sikre god informasjonssikkerhet i kommunen (KS 2022). Rådgiver informasjonssikkerhet og personvern forteller i intervju at det gjennomføres kurs og presentasjoner om informasjonssikkerhet og personvern for ansatte og at kommunen har informasjonskampanjer for å bevisstgjøre ansatte om temaet.

Ullensaker kommune har et introduksjonsprogram for nyansatte som inneholder en sjekkliste med aktiviteter som skal gjennomføres. Ifølge sjekklisten skal nyansatte på dag to i stillingen gjennomføre digital opplæring om informasjonssikkerhet og personvern, samt lese kommunens reglement for informasjonssikkerhet og personvern (Ullensaker kommune 2024a). En velkomst-e-post med lenke til opplæringsvideoer for informasjonssikkerhet og personvern er også automatisk satt opp til alle nyansettelser i organisasjonen (e-post til revisjonen 11.12.2025).

Rådgiver for informasjonssikkerhet og personvern forteller i intervju at det digitale kurset om informasjonssikkerhet og personvern er et tiltak som gjelder for hele kommunen og er tilgjengelig for alle ansatte gjennom ansattportalen. Kurset er obligatorisk å gjennomføre for alle nyansatte i kommunen. For de som startet å jobbe i kommunen før kurset ble innført er det ikke obligatorisk å gjennomføre, men alle ansatte oppfordres til å gjennomføre kurset. Rådgiver forteller videre at det digitale kurset blir vist som bakgrunnsbilde på alle ansattes PC-er under den årlige sikkerhetsmåneden (oktober).

Rådgiver informasjonssikkerhet og personvern og personvernombudet bruker Teams-området for alle ansatte til å informere om personvern. Revisjonen har fått vist informasjonskampanjer om informasjonssikkerhet som er publisert i denne kanalen. Blant annet er det informert om hvordan man oppdager falske e-poster, rutiner for hvilke it-systemer som skal brukes til hva og deling av podcaster fra Norsk senter for informasjonssikring om informasjonssikkerhet.

Rådgiver informasjonssikkerhet og personvern holder stadig kurs og presentasjoner, scenariodiskusjoner og samarbeidsmøter med de ulike tjenestene. Dette gjøres ut fra av observert behov, som risikoreduserende tiltak etter risikovurdering og etter dialog med lederne eller ansatte og etter ønske fra rådgiveren selv (e-post til revisjonen 11.12.2025).

Et annet opplæringstiltak som gjennomføres i kommunen er ifølge rådgiver for informasjonssikkerhet jevnlige phishing-tester[3] som sendes ut per e-post til alle ansatte. Disse e-postene tester hvor mange ansatte som blir lurt av en falsk e-post. Eksempelvis ble det sendt ut en e-post like før jul, og som hevdet at ansatte ikke fikk halvert skatt på lønnsinntekten i desember med mindre de svarte på e-posten i løpet av to dager. Ansatte som svarte på e-posten, fikk beskjed om at dette var en øvelse og fikk tilbud om digital opplæring. Rådgiver for informasjon og personvern forteller i intervju at det etter nevnte phishing-test ble gjennomført to nye øvelser hvor resultatene var bedre (altså, at færre

[3] Phishing er svindelforsøk der hackere utgir seg for å være en legitim kilde for å lure til seg sensitiv informasjon.

ble lurt av phishing-e-posten). Hun forteller videre at kommunen har blitt utsatt for reelle phishing-angrep og at hun da har informert om dette på kommunens felles Teams-kanal for alle ansatte.

Enhet hjemmebaserte tjenester har informasjonssikkerhet som tema i sitt opplegg for nyansatte. Enheten har blant annet et eget introduksjonshefte for nyansatte. Heftet informerer blant annet om taushetserklæring, to-faktorautentisering og lagringsrutiner for dokumentasjon.

Enhetsleder for tjenester til hjemmeboende forteller i intervju at informasjonssikkerhet er et tema som ofte kommer opp i hverdagen. Enheten er blant annet opptatt av taushetsplikt og det snakkes løpende om det for eksempel knyttet til hva som regnes som «snoking» og hvem som skal ha tilgang til IT-systemene som brukes i enheten. Enhetsleder oppfatter at ansatte har lav terskel for å si fra ved hendelser knyttet til informasjonssikkerhet og personvern.

Enhetsleder for tjenester til hjemmeboende forteller i intervju at ansatte i enheten har blitt flinke til å melde fra om avvik og at det har vært en markant økning av rapporteringer i hele helsesektoren. Hun tror likevel at det underrapporteres. Enhetsleder forteller videre at de fleste avvikene som rapporteres handler om legemidler og at hun ikke kan huske at det har vært avvik knyttet til informasjonssikkerhet de siste årene. Hun tror dette skyldes at det meste i dag er lagt til rette for god informasjonssikkerhet. Hun viser til hendelsen hvor en ansatt mistet papirer med sensitive personopplysninger i 2022 og forteller at dette er en hendelse enheten lærte mye av.

3.3 Revisjonens vurdering

Å overvåke kommunens IT-systemer er viktig for å oppdage og reagere på sikkerhetstrusler tidlig. Ullensaker kommune har etter revisjonens vurdering etablert en sikkerhetsovervåkning. Kommunen har engasjert en ekstern leverandør (SOC) for overvåkning av IT-systemene. Denne leverandøren leser logger og overvåker cybersikkerhet i kommunens systemer og varsler kommunen dersom de oppdages unormal aktivitet. I tillegg har avdeling digitale tjenester en egen overvåkning av systemene som driftes av avdelingen, samt en døgnåpen vakttelefon hvor avdelingen alltid kan nås.

Kontroll på identiteter og tilganger er viktig blant annet for å hindre at angripere kommer seg inn i kommunens IT-systemer ved å ta over brukerkontoene til ansatte og andre brukere av kommunens systemer. Revisjonens mener at kommunen har etablert systemer som kan bidra til å sikre kontroll på identiteter og tilganger. Kommunen har prosedyrer for tilgangsstyring knyttet til de ulike IT-systemene som benyttes i kommunen og har etablert en helautomatisk tilgangsstyring som følger kommunens HR-system. I tillegg har enheter og avdelinger utvalgte brukere med utvidede tilganger som ved behov kan gi tilganger som ikke er regulert gjennom den automatiske tilgangsstyringen.

Det er ikke gjennomført inntrengingstest i Ullensaker kommune siden 2021. Det er derfor etter revisjonens syn risiko for at kommunen ikke oppdager svakheter og mangler i kommunens IT-systemer og derfor er sårbar for dataangrep. Å gjennomføre inntrengingstester jevnlig er slik revisjonen oppfatter det et viktig tiltak for å teste egen forsvarsevne, avdekke sårbarheter og mangler og vurdere egen beredskap.

Revisjonens vurdering er at Ullensaker kommune har et planverk for hendelseshåndtering som fordeler roller og ansvar og inneholder konkrete tiltak og aktiviteter ved en IT-sikkerhetshendelse. Rollen som hovedansvarlig ved en sikkerhetshendelse er imidlertid lagt til en stilling som ikke var

besatt i kommunen på revisjonens undersøkelsestidspunkt. Planverket burde etter revisjonens vurdering ha vært revidert, slik at det er tilfredsstillende oppdatert.

Revisjonens vurdering er at kommunen har etablert tiltak for opplæring av ansatte om informasjonssikkerhet. Kommunen har et digitalt kurs om informasjonssikkerhet som er obligatorisk for alle nyansatte. Kommunen har ikke stilt krav om gjennomføring for ansatte som jobbet i kommunen før kurset ble innført, men oppfordrer alle ansatte til å gjennomføre kurset. Videre har kommunen praksis for deling av informasjon om informasjonssikkerhet på kommunens ansattsider, blant annet gjennom en Teams-kanal som er felles for alle ansatte i kommunen. Det gjennomføres også jevnlige phishing-tester som sendes ut til alle ansatte i kommunen.

4 PERSONOPPLYSNINGER

4.1 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, og det brukes mange ulike digitale læremidler i undervisningen. Det innebærer at det behandles flere personopplysninger i skolene enn før. Personopplysningene som samles inn om elever, kan gi et omfattende og detaljert bilde av den enkelte elevs faglige og sosiale atferd gjennom årene. Barns rett til personvern er i dag prisgitt at kommunene foretar de nødvendige vurderingene av digitale læremidler som brukes i skolen og at de tar beslutninger som ikke bryter med personvernreglementet. Kommunene må blant annet sørge for å ha kontroll på ansvarsforholdene 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 3 utledes følgende krav til kommunen:

Problemstilling 3	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 for å gjennomføre og dokumentere vurderinger av personvernkonsekvenser (DPIA) → rutiner og praksis som sikrer at kommunen har databehandleravtaler med alle eksterne leverandører som behandler personopplysninger

4.2 Sikring av personopplysninger

4.2.1 Personvernombud

Kommunen skal ifølge personvernforordningen utpeke et personvernombud. Oppgavene til personvernombudet er å gi råd om vern av personopplysninger og vurderinger av personvernkonsekvenser. Personvernombudet skal også samarbeide med tilsynsmyndigheten, iverksette holdningsskapende tiltak og lære opp personalet som behandlinger personopplysninger. Personvernombudet skal rapportere direkte til det øverste ledelsesnivået (personvernforordningen § 37 - 39).

Ullensaker kommune har utpekt et personvernombud som jobber i en 20 prosent stilling for kommunen. Vedkommende er personvernombud for flere kommuner i regionen.

Personvernombudets arbeidsoppgaver er beskrevet i kommunens strategi for informasjonssikkerhet (Ullensaker kommune 2021d). Oppsummert skal ombudet ifølge strategien:

- Informere og gi råd til kommunen og de ansatte som behandler personopplysninger om forpliktelsene de har etter personvernforordningen og øvrig personvernlovgivning.
- Kontrollere at kommunens praksis er i tråd med personvernlovgivningen og interne prosedyrer knyttet til personvern.
- På anmodning gi råd om personvernkonsekvensvurderinger (DPIA) og kontrollere gjennomføringen av disse.
- Samarbeide med datatilsynet og andre tilsynsmyndigheter.
- Informere de registrerte om alle spørsmål om behandling av personopplysningene deres og rettighetene deres.
- Gi opplæring til de ansatte og utføre holdningsskapende arbeid.
- Være en uavhengig ressursperson.

Personvernombudet forteller i intervju at arbeidsoppgavene hennes er lovfestet. De går ut på å gi råd til kommunen, samt være en støtte og kontaktpunkt for innbyggere og Datatilsynet. Hun forteller videre at risiko- og sårbarhetsanalyser, DPIA, behandlingsprotokoller er en stor del av hennes arbeidshverdag. Hun har en egen telefon hvor hun mottar hendelser fra innbyggerne. Videre forteller hun at arbeidet hennes består av blant annet bevisstgjøring av ansatte, besøk hos skoler og barnehager og opplæring av kvalitetskoordinatorer[4]. Hun har også sendt ut en personlig melding til alle innbyggerne i Ullensaker om personvern. Personvernombudet forteller at hun ikke har hatt kontakt med ledelsen i Ullensaker kommune siden hun startet i stillingen våren 2024.

Rådgiver for informasjonssikkerhet og personvern i Ullensaker kommune forteller i intervju at hun har et fast møtepunkt i uken med personvernombudet. Ut over dette tar hun kontakt med ombudet ved behov.

[4] Kommunen har utpekt en kvalitetskoordinator for hvert område i kvalitetssystemet TQM. Kvalitetskoordinatorene er en støtteressurs når de ansatte skal bruke kvalitetssystemet. Koordinatorene har tilgang til avviksmeldinger og følger opp at avvikene er håndtert riktig. Kvalitetskoordinatorene gjennomgår kurs i informasjonssikkerhet og personvern (intervju med rådgiver informasjonssikkerhet og personvern).

4.2.2 Behandlingsprotokollen

Kommunen skal ha en protokoll over hvilke personopplysninger kommunen behandler.

Ullensaker kommune har en behandlingsprotokoll som rådgiver for informasjonssikkerhet og personvern administrerer. Revisjonen har mottatt skjermutklipp av delene av protokollen som er gjeldende for digitale læremidler i skolen.

Ifølge rådgiver informasjonssikkerhet og personvern skal det opprettes en ny innføring i protokollen for hvert system eller prosess hvor personopplysninger behandles. I tillegg skal endringer i eksisterende systemer/prosesser legges inn. Enheten som eier systemet/prosessen, har ansvaret for å legge den inn i behandlingsprotokollen og involverer rådgiver for bistand til registreringen. Enheten fyller deretter ut protokollen selv eller sammen med rådgiveren (intervju med rådgiver informasjonssikkerhet og personvern).

I kommunens ansattportal ligger det informasjon om behandlingsprotokollen, og det står at den skal holdes løpende oppdatert. I portalen står det også at det automatisk sendes ut en påminnelse om protokollen til enhetslederne en gang i året. Ifølge rådgiver for informasjonssikkerhet og personvern er enhetslederne ansvarlige for å formidle informasjonen til sine ansatte om at alt skal inn i behandlingsprotokollen.

De digitale læremidlene i Ullensaker kommune har en samlet registrering i protokollen. Revisjonen har sett på om innføringen inneholder informasjonen som den skal ifølge personvernforordningens artikkel 30. Gjennomgangen vår viser at:

- Innføringen ikke inneholder navnet og kontaktopplysningene til de behandlingsansvarlige eller personvernombudet. Behandlingsprotokollen har ikke noe felt hvor disse opplysningene skal skrives inn.
- Innføringen inneholder en beskrivelse av formålet med behandlingen, som er «Pålogging på ulike godkjente digitale læringsressurser som brukes i undervisningen, som en del av en variert undervisning og som sørger for økt digital kompetanse, og tilpasset opplæring.»
- I feltet for «kategorier av personer som det samles inn opplysninger om (de registrerte)», står det «elever» og «ansatte». Innføringen inneholder også en liste med kategorier av personopplysninger som registreres, blant annet fullt navn og skoletilhørighet.
- Innføringen mangler informasjon om kategoriene av mottakere som personopplysninger er blitt eller vil bli utlevert til. Innføringen har et felt for «eksterne kommunen deler personopplysninger med», men feltet står tomt.
- Når det gjelder overføringer av personopplysninger til tredjestat eller en internasjonale organisasjon, har behandlingsprotokollen et felt for «overføring til tredjeland». Her henvises det til en oversikt på ansattportalen over godkjente digitale læringsressurser. I denne oversikten står det om data behandles i EU/EØS, USA eller andre tredjeland for hver enkelt læringsressurs.
- Planlagte tidsfrister for sletting av de forskjellige kategoriene av opplysninger er ikke beskrevet – protokollen har et felt for «sletterutiner» - her står det at det er egne sletterutiner for de ulike ressursene.
- Behandlingsprotokollen har ikke et felt for en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltakene, og det er ikke noen informasjon i innføringen om dette.

Kommunen informerer i e-post til revisjonen 5.1.2026 at de mener at krav til navn og kontaktopplysninger til de behandlingsansvarlige jf. personvernforordningen artikkel 30 er dekket ved at kommunens selv er behandlingsansvarlig, og at kommunens kontaktopplysninger er tilgjengelig gjennom innbyggerportalen og ansattportalen.

Personvernombudet forteller i intervju at så vidt hun kjenner til har kommunen gode rutiner på å sende ut påminnelser til ledere om å se gjennom og oppdatere behandlingsprotokollen.

Rådgiver for informasjonssikkerhet og personvern forteller i intervju at hun ikke er fornøyd med måten protokollen er lagt opp og at hun har etterspurt et nytt system. Rådgiver savner blant annet muligheten til å få varsler når det gjøres endringer i protokollen.

4.2.3 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.

Ifølge Ullensaker kommunens strategi for informasjonssikkerhet skal kommunen gjennomføre en skriftlig risikovurdering før enhver behandling av personopplysninger. Denne risikovurderingen er en avgrenset risikovurdering som skal avgjøre om det skal gjennomføres en personvernkonsekvensvurdering (DPIA). Dersom det er sannsynlig at behandlingen vil føre til høy risiko for fysiske personers rettigheter og friheter, skal en DPIA gjennomføres (Ullensaker kommune 2021). Kommunen har en mal for gjennomføring av DPIA som er forelagt revisjonen. I intervju forteller rådgiver for informasjonssikkerhet og personvern at hvis det handler det om KI eller overvåkning, gjennomføres det alltid DPIA.

Det er ikke oppgitt i strategien hvem i kommunen som skal gjennomføre DPIA (Ullensaker kommune 2021). Det vises til at rådgiver for IT-sikkerhet og personvern skal gi rådgivning og bistand, og at personvernombudet skal involveres. I intervju forteller rådgiver for informasjonssikkerhet og personvern at dersom andre har stått for gjennomføringen av DPIA, blir vurderingen gjennomgått av rådgiver for informasjonssikkerhet og personvern, som blant annet undersøker om lovverket er fulgt (intervju med rådgiver informasjonssikkerhet og personvern).

Revisjonen har mottatt kommunens mal for DPIA. Malen inneholder en lovlighetsvurdering og en initialvurdering som skal gjøres ved all ny behandling av personopplysninger, uavhengig av om man skal gjøre en full vurdering av personvernkonsekvenser. I veiledningsteksten i malen står det videre at personvernombudet skal kontrollere initialvurderingen. Etter malen skal initialvurderingen ende i en konklusjon om hvorvidt det skal gjennomføres en full vurdering av personvernkonsekvenser (DPIA). Malen inneholder deretter en rekke spørsmål som skal besvares i en DPIA, i tillegg til en veiledningstekst med eksempler. Spørsmålene inkluderer en beskrivelse av de planlagte behandlingsaktivitetene, formålet med behandlingen, vurderinger av nødvendighet av behandlingen, vurdering av risiko for de registrertes rettigheter og friheter og planlagte tiltak for å håndtere risiko.

Videre inneholder malen felt for uttalelser fra registrerte og personvernombudet, samt behandlingsansvarliges konklusjon, om restrisiko aksepteres og felt for signering.

Revisjonen har bedt kommunen om dokumentasjon på risikovurderinger, og eventuelle gjennomførte DPIA, for et utvalg på ti digitale læremidler. Revisjonens gjennomgang viser at kommunen har gjennomført en risikovurdering av alle de ti læremidlene. For åtte av de ti læremidlene hadde kommunen kommet frem til at det var lav risiko, og dermed ikke nødvendig å gjennomføre en DPIA.

For det niende læremidlet er det gjennomført en DPIA som revisjonen har gjennomgått. DPIA er fylt ut i 2021 i en excel-mal og inneholder initialvurdering, en systematisk beskrivelse av behandlingen av personopplysninger og vurdering av nødvendighet og proporsjonalitet. DPIA inneholder personvernombudets vurdering og vurderinger gjort av de registrerte, men revisjonen kan ikke se at den inneholder konklusjon eller ledelsens vurdering og signatur (punkter i malen som skal fylles ut). DPIA fremstår derfor som påbegynt, men ikke ferdigstilt. Rådgiver informasjonssikkerhet og personvern informerer i e-post til revisjonen 11.9.2025 om at den aktuelle DPIAen er gjennomført etter en tidligere mal.

For det tiende læremidlet er det påbegynt en risikovurdering i 2024, som ikke er ferdigstilt. I analysen oppgis det at kommunen mangler en avklaring av ansvarsforhold, og at en grundigere ROS vil gjennomføres når dette er avklart. Både det niende og det tiende læremiddelet er imidlertid oppført som godkjent på oversikten over digitale læringsressurser som kommunen har sendt til revisjonen.

4.2.4 Databehandleravtaler

Ifølge personvernforordningen skal behandlinger av personopplysninger utført av en databehandler være underlagt en bindende avtale mellom databehandleren og den behandlingsansvarlige. Den behandlingsansvarlige kan være en kommune og databehandleren en leverandør av et IT-system. 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.

Ifølge Ullensaker kommunes strategi for informasjonssikkerhet og personvern, skal kommunen ha rutiner og praksis som sikrer at kommunen har databehandleravtaler med alle eksterne leverandører som behandler personopplysninger (Ullensaker kommune 2021).

Kommunen har en mal for databehandleravtaler som sist ble godkjent i juni 2024. Malen inneholder blant annet informasjon om databehandleravtalens hensikt og formål, databehandlers plikter, krav ved bruk av underleverandører, behandlingsansvarliges rettigheter og plikter, krav til sikkerhet og jevnlige sikkerhetsrevisjoner og til slutt avtalens varighet. Ifølge malen kan leverandøren kun behandle personopplysninger med sikker lagring i land i EU/EØS, med mindre overføring av data til land utenfor EU/EØS er risikovurdert og har skriftlig godkjenning av kommunen (Ullensaker kommune 2024b).

Kommunen har videre en sjekkliste for vurdering av databehandleravtaler. Sjekklisten inneholder en liste på 41 punkter med krav til/beskrivelser av innhold i avtalen. En gjennomgang av sjekklisten og malen for databehandleravtaler viser at disse samsvarer med kravene i personvernforordningen. Blant annet inneholder både malen og sjekklisten beskrivelser av hvilke personopplysninger som

behandles, kategorier av personer det samles inn opplysninger om, databehandlers og behandlingsansvarliges plikter og rettigheter og informasjon om underleverandører.

Både i intervju med seniorrådgiver ved avdeling digitale tjenester og med digitaliseringsrådgiver skole kommer det frem at kommunen har et etterslep når det gjelder signering av databehandleravtaler og at det mangler en oversikt over kommunens avtaler med leverandører av IT-tjenester. Digitaliseringsrådgiver viser til at dokumenter knyttet til ROS, DPIA og databehandleravtaler ligger i ulike systemer. Hun mener dette gjør at det blir vanskelig å holde oversikt og videre gjør arbeidet med å gjennomføre aktivitetene som skal sikre personvernet utfordrende.

Revisjonen har bedt kommunen om databehandleravtaler for de ti utvalgte læremidlene. Rådgiver informasjonssikkerhet og personvern opplyser at databehandleravtaler dokumenteres for digitale læremidler der hvor leverandøren behandler personopplysninger på vegne av kommunen. Av de ti digitale læremidlene revisjonen har valgt ut som stikkprøver, er det fire læremidler hvor leverandør behandler personopplysninger på vegne av kommunen. Revisjonen har mottatt to databehandleravtaler. Ett av de digitale læremidlene er et Microsoft-produkt og faller under kommunens fellesavtale med Microsoft, som revisjonen også har mottatt. For det fjerde læremidlet har ikke revisjonen mottatt databehandleravtale.

De to ordinære databehandleravtalene revisjonen har mottatt er gjennomført etter andre maler enn den revisjonen har mottatt. Avtalene inneholder imidlertid informasjonen som kreves etter personvernforordningen, med unntak av at en av avtalene ikke inneholder informasjon om underleverandører. Avtalene inneholder blant annet beskrivelser av tjenesten, formålet med behandlingen av personopplysninger, hvilke kategorier av personer det behandles personopplysninger om, hvilke personopplysninger som behandles, avtalens varighet, samt databehandlers plikter til å ha tilstrekkelige sikkerhetstiltak og informasjon om bruk av underleverandører.

Databehandleravtalen kommunen har med Microsoft omfatter ett av de digitale læremidlene revisjonen har etterspurt dokumentasjon om. Avtalen er av overordnet karakter og inneholder ikke spesifikk informasjon om kategorier av registrerte eller hvilke personopplysninger som behandles i det aktuelle digitale læremidlet. Ifølge kommunen skiller Microsoft seg ut som en leverandør som ikke muliggjør signerte databehandleravtaler grunnet deres kundemengde. Rådgiver for informasjonssikkerhet og personvern har utfordret Microsoft på dette, men svaret hun har fått er at kommunen, ved å ta i bruk det aktuelle digitale læremidlet, samtykker til databehandleravtalen som Microsoft har med kommunen for alle sine programvarer (e-post til revisjonen 11.9.2025).

4.3 Revisjonens vurdering

Ullensaker kommune har utpekt et personvernombud. Personvernombudet rapporterer imidlertid ikke direkte til det høyeste ledelsesnivået hos den behandlingsansvarlige, slik personvernforordningen stiller krav om. Utover dette er det revisjonens vurdering at ombudets ansvar og oppgaver er i henhold til kravene i personvernforordningen.

Ullensaker kommune har en protokoll for personopplysninger som kommunen behandler. Etter revisjonens vurdering er ikke digitale læremidler tilstrekkelig dokumentert i protokollen. Kommunen har registrert digitale læremidler samlet under én innføring. Dette gir etter revisjonens syn begrenset

informasjon om hvilke personopplysninger som registreres for hvert av de digitale læremidlene. Protokollen inneholder ikke informasjon om hvorvidt kommunen deler personopplysninger med eksterne gjennom digitale læremidler.

Revisjonens vurdering er at kommunen har en mal for gjennomføring av vurderinger av personvernkonsekvenser (DPIA) som tilfredsstiller kravene i personvernforordningen. Det er imidlertid en svakhet at kommunen ikke har dokumentasjon som viser hvem som er ansvarlige for å gjennomføre DPIA. Det er gjennomført DPIA for ett av de ti digitale læremidlene revisjonen har gjennomgått. Denne DPIA-en mangler konklusjon og ledelsens vurdering og signatur, og fremstår derfor som påbegynt, men ikke ferdigstilt. For ett av de ti læremidlene er det påbegynt en risikovurdering i 2024 som ikke var ferdigstilt ved undersøkelsestidspunktet. Selv om dokumentasjonen tyder på at risikovurderinger og aksept av restrisiko ikke er gjort for disse to læremidlene er de likevel markert som godkjent. Revisjonen vurderer derfor at det er uklart hvorvidt kommunen har risikovurdert alle digitale læremidler som er i bruk. Da det kun er gjennomført DPIA for ett av de ti læremidlene revisjonen har gjennomgått, har ikke revisjonen grunnlag for å vurdere kommunens praksis knyttet til selve gjennomføringen av DPIA, ut over at den ene vurderingen revisjonen har gjennomgått fremstår som uferdig.

Revisjonens vurdering er at kommunen har mal og sjekkliste for databehandleravtaler som tilfredsstiller kravene i personvernforordningens artikkel 28. Det er imidlertid brukt en annen mal i de to databehandleravtalene revisjonen har gjennomgått. Avtalene er dekkende for kravene i personvernforordningen, med unntak av at én av avtalene ikke inneholder informasjon om underleverandører. En av de fire databehandleravtalene revisjonen har etterspurt er ikke oversendt. Videre viser undersøkelsen at kommunen mangler oversikt over databehandleravtaler og at det er et etterslep på signering av databehandleravtaler, noe som etter revisjonens syn er svært uheldig. 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.

5 KONKLUSJON OG ANBEFALINGER

Denne undersøkelsen har hatt som formål å avdekke eventuelle svakheter i informasjonssikkerheten og behandlingen av personopplysninger i Ullensaker kommune. Undersøkelsen viser at Ullensaker kommune har mye på plass på dette området. Samtidig viser undersøkelsen at det er flere svakheter som bør utbedres. De viktigste manglene gjelder tydelige rolle-, ansvars- og oppgavebeskrivelser, forankring av arbeidet med informasjonssikkerhet hos øverste ledelse og tilfredsstillende sikring av personopplysninger.

Det er revisjonens konklusjon at Ullensaker kommune har et styringssystem for informasjonssikkerhet, men at det er mangler knyttet til styrende dokumenter for informasjonssikkerhet, rolle- og ansvarsfordeling, samt ledelsens oppfølging av området.

Etter revisjonens syn er rolle- og ansvarsfordelingen uklar i noen av kommunens styrende dokumenter for informasjonssikkerhet og gjenspeiler ikke etter revisjonens syn dagens rolle- og ansvarsfordeling knyttet til informasjonssikkerhet i tilstrekkelig grad. Undersøkelsen viser at rolle- og ansvarsfordelingen er uklar på flere områder, for eksempel når det gjelder ansvarsfordelingen mellom enhet innovasjon og digitalisering og linjeorganisasjonen for øvrig, knyttet til systemforvaltning og informasjonssikkerhet. Videre ansvarliggjør kommunens plan for hendelseshåndtering en rolle som i en lengre tid ikke har vært besatt. Å sørge for en tydelig oppgave-, rolle og ansvarsfordeling vil bidra til å redusere sårbarhet ved bortfall av nøkkelpersonell.

Revisjonen konkluderer med at kommunen langt på vei har tilstrekkelige tiltak som fanger opp og hindrer forsøk på datainnbrudd. Kommunen har etablert et system for sikkehetsovervåkning samt prosedyrer og system for styring av identiteter og tilganger, men gjennomfører ikke jevnlige inntrengingstester som anbefalt. Kommunen har videre et planverk for hendelseshåndtering og tiltak for opplæring og bevisstgjøring av ansatte om informasjonssikkerhet. Samtidig er det en svakhet at hovedansvaret for alvorlige og kritiske hendelser er i kommunens prosedyre lagt til rollen fagansvarlig digitalisering, en rolle som nevnt over ikke var besatt under revisjonens datainnhenting.

Revisjonen konkluderer med at Ullensaker kommune i noen grad har sørget for at personopplysninger som lagres i kommunens IT-systemer på skoleområdet er sikret. Ullensaker kommune har utpekt et personvernombud i henhold til personvernforordningen. Ombudet rapporterer imidlertid ikke direkte til det øverste ledelsesnivået i kommunen, i henhold til personvernforordningen artikkel 38. Videre viser undersøkelsen at praksisen med å føre samtlige digitale læremidler samlet i kommunens behandlingsprotokoll, ikke gir tilstrekkelig informasjon om personopplysninger som kommunen behandler. Kommunen har heller ikke dokumentasjon som viser hvem som er ansvarlige for å gjennomføre DPIA. Digitale læremidler uten dokumentasjon på at risikovurderinger er fullført står som godkjent i kommunens oversikt over risikovurderinger. Når det gjelder databehandleravtaler viser undersøkelsen at kommunen ikke har oversikt over sine databehandleravtaler med leverandører som behandler personopplysninger på vegne av kommunen.

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

1. å oppdatere styrende dokumenter, slik at det gis en riktig beskrivelse av dagens styringssystem for informasjonssikkerhet
2. å tydeliggjøre og dokumentere oppgave-, rolle- og ansvarsfordelingen knyttet til informasjonssikkerhet
3. å gjennomføre ledelsens gjennomgang av informasjonssikkerhet årlig
4. at det gjennomføres jevnlige inntrengingstester
5. å etablere rutiner for direkte rapportering fra personvernombudet til kommuneledelsen
6. at behandlingsprotokollen tilfredsstiller kravene i personvernforordningen
7. tilstrekkelig dokumentasjon av risikovurderinger og vurderinger av personvernkonsekvenser for digitale læremidler som er i bruk i skolene
8. å skaffe oversikt over kommunens databehandleravtaler og sikre at databehandleravtaler som mangler kommer på plass

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).

Nasjonal sikkerhetsmyndighet (2024). NSMs grunnprinsipper for IKT-sikkerhet versjon 2.1, 2024.

Nasjonal sikkerhetsmyndighet (2017) Rammeverk for håndtering av IKT-sikkerhetshendelser. Versjon per 07.12.17.

Digitaliseringsdirektoratet (2025). Internkontroll i praksis – informasjonssikkerhet. Versjon 2.0. Hentet fra https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601 [22.10.2025]

Datatilsynet (2025). Virksomhetens plikter. Hentet fra https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/ [22.10.2025]

KS (2022) Kommunedirektørens verktøykasse for personvern og informasjonssikkerhet. Et tillegg til Kommunedirektørens internkontroll – Orden i eget hus.

Fra Ullensaker kommune

Ullensaker kommune (2021a). Prosedyre for dokumentstyring i kvalitetssystemet. Dokument-ID 13073-1.

Ullensaker kommune (2021b). Prosedyre for varsling av hendelser på kommunens IT-tjenester. Dokument-ID 13097-1. Sist godkjent 3.12.2021 av enhetsleder innovasjon og digitalisering.

Ullensaker kommune (2021c). Retningslinjer for internkontroll i Ullensaker kommune. Godkjent av kommunedirektørens strategiske ledergruppe 31.5.2021.

Ullensaker kommune (2021d). Strategi for informasjonssikkerhet og personvern i Ullensaker kommune. Godkjent av kommunedirektør i Strategisk ledergruppe (SLG) 6.12.2021.

Ullensaker kommune (2021e). Systemforvaltning IT – Retningslinjer for systemforvaltning i Ullensaker kommune.

Ullensaker kommune (2021f). Systemforvaltning IT – Styringsmodell Ullensaker kommune.

Ullensaker kommune (2022a). Internkontroll – beskrivelse av kommunens hovedoppgaver, mål og organisering iht. kommunelovens §25-1. Dokument-ID 13309-2. Godkjent av kommunedirektørens strategiske ledergruppe (SLG) 13.6.22.

Ullensaker kommune (2022b). Prosedyre for gjennomføring og oppfølging av risikovurderinger. Dokument-ID 13280-3. Godkjent av kommunedirektøren 19.8.2022.

Ullensaker kommune (2022c). Prosedyre for ledelsens gjennomgang av internkontrollsystemet. Dokument ID 13396-1. Godkjent av kommunedirektøren 28.10.2022.

Ullensaker kommune (2022d). Prosedyre for retting og sletting av personopplysninger. Dokument-ID 13184-1. Godkjent av kommunedirektøren 27.1.2022.

Ullensaker kommune (2022d). Årshjul for virksomhetsstyring og internkontroll i Ullensaker kommune. Godkjent av kommunedirektøren 19.10.2022.

Ullensaker kommune (2023a). Gardermoregionen regional risiko- og sårbarhetsanalyse.

Ullensaker kommune (2023b). Kommunal ROS.

Ullensaker kommune (2023c). Prosedyre for håndtering av IKT-sikkerhetshendelser. Dokument-ID 13190-4. Godkjent av enhetsleder innovasjon og digitalisering 31.3.2023.

Ullensaker kommune (2023d). Reglement for informasjonssikkerhet og personvern. Dokument-ID 13473-1. Godkjent av kommunedirektør 30.3.2023.

Ullensaker kommune (2023e). Veileder for risikovurdering av informasjonssikkerhet og personvern av IT-systemer. Dokument-ID 13406-4. Godkjent av rådgiver informasjonssikkerhet og personvern 17.3.2023.

Ullensaker kommune (2024a) Introduksjonsprogram for nyansatte i Ullensaker kommune siste versjon. Dokument-ID 12912-3. Godkjent 11.12.2024 av HR- og organisasjonsutviklingssjef.

Ullensaker kommune (2024b). Mal - databehandleravtale Ullensaker kommune. Sist godkjent av rådgiver informasjonssikkerhet og personvern 17.6.2024.

Ullensaker kommune (2025a). Kurs 5 og brukerveiledning: Risikovurderinger. Versjon 5.6.2025.

Ullensaker kommune (2025b). Prosedyre for hendelses- og avviksbehandling i kvalitetssystemet. Dokument-ID 13096-2. Godkjent av kommunedirektøren 10.6.2025.

Ullensaker kommune (2025c). Prosedyre for ledelsens gjennomgang av internkontrollsystemet.

Ullensaker kommune (2025d). Protokoll fra møte i SLG 24.11.2025.

Ullensaker kommune (2025e). Overordnet risikovurdering av helheten i internkontrollen med oppfølgingsplan – kommunenivå 2024. Godkjent av kommunedirektøren 3.2.2025.

Ullensaker kommune (2025f). Overordnet risikovurdering av helheten i internkontrollen med oppfølgingsplan – Innovasjon og digitalisering 2024. Godkjent av enhetsleder Innovasjon og digitalisering 24.1.2025.

Ullensaker kommune (udatert a). Mal - hendelseslogg.

Ullensaker kommune (udatert b). MAL for overordnet risikovurdering av helheten i internkontrollen.

Ullensaker kommune (udatert c). Mal – Personkonsekvensvurdering DPIA.

Ullensaker kommune (udatert d). Mal for risikovurderinger – kun for de som ikke kan gjennomføres i TQM.

Ullensaker kommune (udatert e). Sjekkliste ved IT-sikkerhetshendelser.

Ullensaker kommune (udatert f). Årshjul informasjonssikkerhet og personvern.

Ullensaker kommune (udatert g). Introduksjonshefte

Ullensaker kommune (udatert h). Oppgaver og ansvar fra Camilla.

Ullensaker kommune (udatert i). Stedfortredere. Skjermutklipp. Mottatt sammen med dokumenter knyttet til plan for hendelseshåndtering.

Andre kilder

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/ [17.10.2025]

Digdir (udatert). «Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål». Hentet fra Informasjonssikkerhet - en forutsetning for å nå virksomhetens mål | Digdir [22.10.2025]

NAOB (udatert). «Informasjonssikkerhet». Hentet fra: https://naob.no/ordbok/informasjonssikkerhet [22.10.2025]

NOU 2022:11. «Ditt personvern – vårt felles ansvar. Tid for en personvernpolitikk». Oslo: Statens forvaltningstjeneste.

Meld. St. 38 (2016-2017). «IKT-sikkerhet. Et felles ansvar». Justis- og beredskapsdepartementet.

Romerike blad (2024a). *Publiserte sensitive opplysninger om barnefamilie.* Hentet fra https://www.mittjessheim.no/publiserte-sensitive-opplysninger-om-barnefamilie-selvfolgelig-uheldig/s/5-111-244023 [17.10.2025]

Romerike blad (2024b). *Kommunen dømt til å betale 90.000 kroner i erstatning til elev: - Vil ikke anke dommen.* Hentet fra https://www.mittjessheim.no/kommunen-domt-til-a-betale-90-000-kroner-i-erstatning-til-elev-vil-ikke-anke-dommen/s/5-111-225225 [17.10.2025]

Romerike blad (2024c). *Hjemmesykepleier mistet liste med svært private opplysninger – brukerne ble ikke informert: - Menneskelig svikt.* Hentet fra https://www.mittjessheim.no/hjemmesykepleier-mistet-liste-med-svart-private-opplysninger-brukerne-ble-ikke-informert-menneskelig-svikt/s/5-111-187013 [17.10.2025]

VEDLEGG 1 KOMMUNEDIREKTØRS UTTALELSE

ULLENSAKER KOMMUNE Innovasjon og digitalisering

Romerike Revisjon Iks
Ringvegen 4
2050 Jessheim

Deres ref.:	Vår ref.:	Saksbehandler:	Dato:
	24/10086 - 6	May Britt Hamnes Grønningen	08.01.2026

Kommunedirektørens uttalelse til utkast av forvaltningsrapport IT sikkerhet og personvern

Ullensaker kommune har foretatt en grundig gjennomgang av utkastet til forvaltningsrevisjonsrapport. I denne prosessen har vi lagt særlig vekt på å kontrollere at faktagrunnlaget er korrekt og fullstendig, at revisjonskriteriene er anvendt på en relevant og riktig måte, samt at revisjonens konklusjoner fremstår som rimelige og tilstrekkelig dokumentert.

Med hjemmel i ovennevnte regelverk fremsettes følgende tilbakemelding:

Faktakorrigeringer
Informasjonssikkerhet er integrert i kommunens rammeverk for internkontroll, og det anses p.t. ikke som nødvendig å beskrive dette som et separat linjeansvar. Det følger av den helhetlige styring av kommunen.

Kommentarer til vurderinger og konklusjoner
Strategien for informasjonssikkerhet og personvern oppstiller etter vårt syn roller og ansvarsområder, og det er utarbeidet matriser som viser stedfortredere og oppgavefordeling. Vi noterer oss at revisjonen ber om at dette tydeliggjøres.

Selv om rollen som fagansvarlig har vært ubesatt i en periode, har oppgavene vært ivaretatt. Ny avdelingsleder er nå på plass, og enheten er fulltallig fra 1. januar 2026.

Tilleggsinformasjon
Ledelsens gjennomgang av informasjonssikkerhet og personvern er besluttet gjennom kommunedirektørens ledergruppe og følger årshjulet for internkontroll. Kommunen gjennomførte i 2024 en helhetlig risikovurdering av internkontrollen, der informasjonssikkerhet var et eget tema. I desember 2025 ble en egen risikovurdering av informasjonssikkerhet og personvern på organisatoriske forhold ferdigstilt. Denne er gjennomført i alle kommunens enheter. Arbeidet inngår som en del av kommunens kontinuerlige forbedringsprosess.

Når det gjelder opplæring og kompetanseheving, mottar alle nyansatte velkomst-e-post med lenke til opplæringsvideoer, og rådgiver for personvern og informasjonssikkerhet gjennomfører jevnlig kurs

Postadresse Postboks 470 2051 JESSHEIM
Besøksadresse Furusethgata 12 2050 JESSHEIM
Telefon +47 66 10 80 00
Kontonr. 1802.06.26948
Org.nr. 933 649 768
E-post postmottak@ullensaker.kommune.no
Internett www.ullensaker.kommune.no

og scenariodiskusjoner. Det er etablert rutiner for risikovurdering, tilgangsstyring og oppfølging av tiltak i dialog med tjenestene. Arbeidet med databehandleravtaler er innlemmet i anskaffelsesprosessen, og det vurderes ny løsning for behandlingsprotokoll, blant annet KS sin DigiOrden.

Personvernombudsordningen som er regulert gjennom vertskommunesamarbeid, gir personvernet rett til direkte dialog med kommunedirektør i tilfeller hvor det er aktualisert. I avtale om felles personvernombud punkt 2, 4. avsnitt er det regulert at ombudet faglig rapporterer til kommunedirektør i den kommune saken gjelder. Se vedlagt avtale.

Forberedelse til offentliggjøring
Flere relevante ressurser fra kommunen er påmeldt «Frokostseminar om personvern i kommunene» den 15. januar 2026, og ser frem til å høre forvaltningsrevisjonens funn og erfaringer som vil bli presentert der.

Administrasjonen starter planlegging av nødvendige tiltak dersom rapporten skulle avdekke avvik. Det er også igangsatt arbeid med kommunikasjonsstrategi for håndtering av rapporten når den blir offentlig.

Kommunedirektøren takker for samarbeidet og ser frem til den endelige rapporten. Ullensaker kommune står til disposisjon for ytterligere dialog dersom det er behov.

Med hilsen

Erling Sigmund Kristiansen
Kommunedirektør

May Britt Hamnes Grønningen
enhetsleder

Dokumentet er elektronisk godkjent og har derfor ingen signatur

Vedlegg
Interkommunal avtale om felles personvernombud

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:
  - 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)

Styringssystem 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 Ledelsessystemer[1] for informasjonssikkerhet (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 om informasjonssikkerhet 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 (Digitaliseringsdirektoratet, «Internkontroll i praksis»).

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). 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).

Oppgave-, rolle- og ansvarsfordeling for informasjonssikkerhet

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 sikkerhetstiltak og aksept av risikonivå

Hindre forsøk på datainnbrudd knyttet til tjenester til hjemmeboende

NSMs grunnprinsipper

For å undersøke hvordan kommunen arbeider for å fange opp og hindre forsøk på datainnbrudd i tjenester til hjemmeboende har revisjonen i all hovedsak tatt utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet versjon 2.1. NSM har definert 21 grunnprinsipper. Disse er fordelt inn i fire hovedkategorier:

1. Identifisere og kartlegge
2. Beskytte og opprettholde
3. Oppdage
4. Håndtere og gjenopprette

Noen av grunnprinsippene er omtalt i kapittel 1.2, da de kan knyttes til kommunens styringssystem for informasjonssikkerhet. For å tilpasse revisjonskriteriene til undersøkelsens omfang har revisjonen valgt ut noen av grunnprinsippene for gjennomgang.

Beskytte og opprettholde

Den andre hovedkategorien av NSMs grunnprinsipper handler om å beskytte og opprettholde IKT-systemene. Hovedprinsippet innebærer å ivareta en forsvarlig sikring av IKT-systemet og sørge for at systemet opprettholdes over tid og ved endringer. Prinsippene innenfor denne hovedkategorien av grunnprinsipper skal etablere en sikker tilstand for IKT-systemet i kommunen for å motstå eller begrense skaden fra dataangrep. Hvordan IKT-systemer anskaffes, planlegges, bygges og konfigureres slik at kommunen oppnår ønsket sikkerhet.

Et prinsipp knyttet til kartleggingen av brukere og behov for tilganger (prinsipp 1.3) er prinsippet om å ha kontroll på identiteter og tilganger (prinsipp 2.6). Dette er viktig fordi manglende tilgangskontroll

øker risikoen for dataangrep. Prinsippet innebærer blant annet å etablere retningslinjer for tilgangskontroll.

Et annet prinsipp er å etablere evnen til gjenoppretting av data (NSMs grunnprinsipp 2.9.). Dette er viktig for å minimere konsekvensene av et eventuelt dataangrep.

Oppdage

Den tredje hovedkategorien av NSMs grunnprinsipper handler om å oppdage og fjerne kjente sårbarheter og trusler og etablere sikkerhetsovervåkning.

Et av prinsippene innenfor denne hovedkategorien er å oppdage og fjerne kjente sårbarheter og trusler i kommunens IKT-systemer (prinsipp 3.1.). Dette innebærer blant annet å gjennomføre jevnlige sårbarhetskartlegginger i informasjonssystemet og å være oppdatert på nye og kommende sårbarheter.

Et annet prinsipp handler om å etablere sikkerhetsovervåkning (prinsipp 3.2.). Sikkerhetsovervåkning kan bidra til å oppdage sikkerhetshendelser tidlig, vurdere skadeomfang og hendelsens karakter og forstå hendelsesforløpet.

Et prinsipp knyttet til å oppdage og fjerne kjente sårbarheter og trusler er å gjennomføre inntrengingstester. Dette prinsippet innebærer blant annet en anbefaling om å gjennomføre jevnlige inntrengingstester for å identifisere sårbarheter. Det anbefales å gjennomføre inntrengingstester minst en gang i året.

Håndtere og gjenopprette

Den fjerde hovedkategorien av NSMs grunnprinsipper handler om å håndtere sikkerhetshendelser på en effektiv måte. Hensikten med prinsippene er at kommunen får på plass aktiviteter for å forberede seg på, vurdere, kontrollere og håndtere hendelser, samt gjenopprette normaltilstand. Prinsippene innebærer også å forberede sikkerheten basert på erfaringer fra hendelseshåndteringen.

Ett av prinsippene innenfor denne hovedkategorien er å forberede kommunen på håndtering av hendelser (prinsipp 4.1.). Dette prinsippet innebærer blant annet å etablere et planverk for hendelseshåndtering og å revidere dette planverket jevnlig. Prinsippet innebærer også å gjennomføre regelmessige øvelser på informasjonssikkerhetshendelser.

Et annet prinsipp innenfor håndtering og gjenoppretting er å evaluere og lære av hendelser (prinsipp 4.4.). Dette prinsippet er viktig for å sikre at kunnskap og erfaringer om sårbarheter som gjøres etter en hendelse fører til økt sikkerhet som kan hindre at liknende hendelser oppstår igjen. Prinsippet innebærer å identifisere erfaringer og lærepunkter, kartlegge og gjennomgå sikkerhetstiltak, vurdere effektiviteten av prosesser, prosedyrer, rapporteringsformater og organisatoriske strukturer og å kommunisere og dele erfaringene med relevante ansatte og andre interessenter. Sistnevnte kan innebære å bruke historier fra hendelseshåndtering i opplæring og bevisstgjøring av ansatte.

Opplæring i informasjonssikkerhet

I KS sin veileder *Kommunedirektørens verktøykasse for informasjonssikkerhet* påpekes det at god informasjonssikkerhet til syvende og sist avhenger av ferdighetene og kunnskapen til menneskene i organisasjonen. Det er ifølge veilederen viktig at alle ansatte bidrar til at teknologi brukes riktig,

prosesser følges, taushetsplikt ivaretas og avvik knyttet til sikkerhet og personvern registreres og følges opp. I veilederen understrekes viktigheten med tilstrekkelig opplæring i alle ledd i kommunen. I veilederen anbefales kommunedirektøren å ha et opplæringsprogram hvor alle ansatte bevisstgjøres på hvordan kommunen skal ivareta god informasjonssikkert og godt personvern, og hva dette betyr for den enkelte. Kunnskap er ferskvare og opplæringen bør tilpasses den enkeltes stilling.

Følgende revisjonskriterier legges til grunn for problemstilling 2:

Problemstilling 2	Krav og forventninger til kommunen
I hvilken grad har kommunen satt inn tilstrekkelige tiltak for å fange opp og hindre forsøk på datainnbrudd på kommunens systemer knyttet til hjemmebaserte tjenester, samt etablert planverk for å håndtere denne typen hendelser?	Kommunen skal ha → ha etablert sikkerhetsovervåkning → kontroll på identiteter og tilganger → gjennomført inntrengingstester jevnlig, og minst en gang i året → etablert et planverk for hendelseshåndtering og som revideres jevnlig → tiltak som sikrer at ansatte får opplæring i informasjonssikkerhet

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 Ullensaker 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.[2]

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

Databehandleravtaler

Personvernforordningen artikkel 28 stiller krav til kommunen knyttet til behandlinger av personopplysninger som skal gjøres av en databehandler på vegne av kommunen. Dersom en behandling av personopplysninger skal utføres på vegne av kommunen, skal kommunen bare bruke databehandlere som gir tilstrekkelige garantier for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen av personopplysningene oppfyller kravene i forordningen og vern av rettighetene til de som registreres.

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:

- En beskrivelse av selve behandlingen av personopplysninger, herunder:
  - hva databehandleren faktisk skal gjøre
  - hva som er formålet med behandlingen
  - hvor lenge avtalen skal vare
  - hva slags personopplysninger som er registrert
  - hvilke kategorier av personer personopplysningene gjelder
- Pliktene og rettighetene til den behandlingsansvarlige, herunder å regulere følgende:
  - 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 3	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 for å gjennomføre og dokumentere vurderinger av personvernkonsekvenser (DPIA) → rutiner og praksis som sikrer at kommunen har databehandleravtaler med eksterne leverandører som behandler personopplysninger