RM Revisjon Midt-Norge

Digital sikkerhet

Trøndelag fylkeskommune

Forvaltningsrevisjon

2026

FR1369

FORORD

Revisjon Midt-Norge SA har gjennomført denne forvaltningsrevisjonen på oppdrag fra Trøndelag fylkeskommunes kontrollutvalg i perioden mars 2026 til oktober 2026.

Vi vil takke alle som har bidratt med informasjon i prosjektet.

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

Mo i Rana, 30.10.2026

Cathrine Berg-Mortensen
Oppdragsansvarlig revisor

Hanne Marit U. Bjerkan og Merete M. Montero
Prosjektmedarbeidere

SAMMENDRAG

Revisjon Midt-Norge SA har gjennomført en forvaltningsrevisjon av digital sikkerhet i Trøndelag fylkeskommune. Revisjonen har undersøkt om fylkeskommunen har et forsvarlig arbeid med digital sikkerhet, innenfor utvalgte områder knyttet til informasjonssikkerhet og personvern.

Revisor konkluderer med at Trøndelag fylkeskommune i hovedsak har etablert og gjennomført et forsvarlig arbeid med digital sikkerhet innenfor de områdene revisjonen har undersøkt. Fylkeskommunen har etablert sentrale rammer for styring og internkontroll, men det er forbedringsbehov knyttet til å styrke den systematiske gjennomføringen og oppfølgingen av sikkerhetsarbeidet.

Fylkeskommunen har dokumenterte mål og strategier, en etablert ansvarsfordeling og rutiner for sentrale deler av informasjonssikkerhetsarbeidet. Det er også etablert ordninger for avvikshåndtering, opplæring, tilgangsstyring og behandling av personopplysninger. Revisjonens vurderinger viser at disse ordningene i hovedsak ivaretar de undersøkte kravene.

Samtidig viser revisjonen variasjoner i kjennskap til og bruk av rutiner, mangler ved dokumentasjonen av internkontrollen og behov for mer systematisk bruk av avvik og sikkerhetshendelser i forbedringsarbeidet. Det er også identifisert svakheter ved oppfølgingen av enkelte tilganger og kontroll av tilgangslogger. Innen personvern er det forbedringsbehov knyttet til å videreutvikle den samlede oversikten over behandlinger av personopplysninger og tydeliggjøre enkelte rutiner.

Revisors anbefaler at fylkeskommunen:

1. Styrker arbeidet med å sikre at rutiner og prosedyrer for informasjonssikkerhet er kjent og tas i bruk i relevante deler av organisasjonen
2. Sikrer mer fullstendig og oppdatert dokumentasjon av internkontrollen for informasjonssikkerhet, herunder oversikten over informasjonssystemer og behandling av personopplysninger
3. Styrker den systematiske bruken av avvik, sikkerhetshendelser og risiko som grunnlag for læring og forbedring av internkontrollen
4. Etablerer en mer systematisk og risikobasert oppfølging av tilganger, herunder kontroll av tilgangslogger der dette er nødvendig.

INNHOLDSFORTEGNELSE

Forord 3

Sammendrag 4

Innholdsfortegnelse 5

1 Innledning 7
1.1 Bestilling 7
1.2 Problemstillinger 7
1.3 Avgrensning 8
1.4 Metode 9
1.5 Uttalelse om rapport 12
1.6 Informasjonssikkerhet og personvern 12

2 Styringssystemer og rutiner 16
2.1 Delproblemstilling 16
2.2 Revisjonskriterier 16
2.3 Funn 16
2.3.1 Mål og strategier for informasjonssikkerhet 17
2.3.2 Roller, ansvar og myndighet 18
2.3.3 Rutiner og prosedyrer 19
2.3.4 Kjennskap til og bruk av rutiner 21
2.3.5 Dokumentasjon av internkontrollen 22
2.4 Vurdering 24

3 Avvik og forbedringsarbeid 27
3.1 Delproblemstilling 27
3.2 Revisjonskriterier 27
3.3 Funn 27
3.3.1 Avdekking, registrering, klassifisering og oppfølging 27
3.3.2 Registrering og oppfølging i praksis 28
3.3.3 Håndtering og dokumentasjon av brudd på personopplysningssikkerheten 30
3.3.4 Bruk av avvik, sikkerhetshendelser og risiko i forbedringsarbeidet 31
3.4 Vurdering 32

4 Kompetanse og opplæring 34
4.1 Delproblemstilling 34
4.2 Revisjonskriterier 34
4.3 Funn 34
4.3.1 Opplæring om sikker bruk og behandling av personopplysninger 35
4.3.2 Informasjon og opplæring ved behandling av elevdata, pasientdata og personaldata 38
4.3.3 Dokumentasjon av opplærings- og informasjonstiltak 40
4.4 Vurdering 41

5 Tilgangsstyring 43
5.1 Delproblemstilling 43
5.2 Revisjonskriterier 43
5.3 Funn 43
5.3.1 Rutiner og ansvar for tilgangsstyring 44
5.3.2 Tildeling, endring og avslutning av tilganger ut fra tjenstlig behov 45
5.3.3 Logging og oppfølging av tilganger 48
5.4 Vurdering 50

6 Etterlevelse av utvalgte personvernkrav 52
6.1 Delproblemstilling 52
6.2 Revisjonskriterier 52
6.3 Funn 52
6.3.1 Oversikt over behandlinger og behandlingsprotokoller 53
6.3.2 Informasjon til de registrerte 55
6.3.3 Databehandleravtaler 58
6.4 Vurdering 59

7 Konklusjon og anbefalinger 61
7.1 Konklusjon 61
7.2 Anbefalinger 61

Kilder 62

Vedlegg 1 – Utledning av revisjonskriterier 65

Vedlegg 2 – Uttalelse 73

1 INNLEDNING

1.1 Bestilling

Kontrollutvalget i Trøndelag fylkeskommune har bestilt en forvaltningsrevisjon med tema Informasjonssikkerhet, drift og utvikling. Bestillingen er gjort med bakgrunn i Plan for forvaltningsrevisjon. Kontrollutvalget vedtok revisors prosjektplan i sak 02/26.

1.2 Problemstillinger

Følgende problemstilling vil bli besvart i rapporten:

Har fylkeskommunen etablert og gjennomført et forsvarlig arbeid med digital sikkerhet?

Delproblemstillinger:

Styringssystemer og rutiner: Har fylkeskommunen etablert rutiner og prosesser for å sikre informasjonssikkerhet, og i hvilken grad er disse gjort kjent og tatt i bruk i organisasjonen?

Avvik og forbedringsarbeid: Har fylkeskommunen etablert rutiner for håndtering av avvik og sikkerhetshendelser innen informasjonssikkerhet, og hvordan brukes avvik i arbeidet med å forbedre internkontrollen?

Kompetanse og opplæring: Har fylkeskommunen etablert og fulgt opp tiltak for å gi ansatte nødvendig informasjon, opplæring og kompetanseutvikling innen informasjonssikkerhet?

Tilgangsstyring: Har fylkeskommunen rutiner og ordninger for tilgangsstyring som ivaretar tjenstlig behov og nødvendig logging og oppfølging?

Etterlevelse av personvernregelverket i tjenesteområdene: Etterlever fylkeskommunen utvalgte krav i personvernregelverket ved behandling av pasientdata, elevdata og personaldata?

Delproblemstillingene konkretiserer hvilke områder av fylkeskommunens arbeid med digital sikkerhet som undersøkes. De gir ikke en uttømmende oversikt over alle krav eller forhold som kan være relevante. Funnene vurderes opp mot revisjonskriteriene innenfor hvert område. Det gis ikke egne konklusjoner på delproblemstillingene. Revisors vurderinger på revisjonskriteriene under delproblemstillingene inngår samlet som grunnlag for revisjonens konklusjon på den overordnede problemstillingen.

1.3 Avgrensning

Rapporten undersøker utvalgte organisatoriske og styringsmessige forhold ved fylkeskommunens arbeid med digital sikkerhet. Digital sikkerhet inngår i arbeidet med informasjonssikkerhet, som omfatter beskyttelse av informasjon i alle former. Begrepet informasjonssikkerhet brukes i rapporten ved omtale av fylkeskommunens styringssystemer og rutiner som skal ivareta sikkerheten ved behandling av informasjon, herunder i digitale systemer.

Revisjonen omfatter styringssystemer og rutiner, avvik og forbedringsarbeid, kompetanse og opplæring samt tilgangsstyring. Undersøkelsen bygger på skriftlig dokumentasjon og verifiserte intervjuopplysninger. Beskrivelsene av hvordan rutiner og ordninger praktiseres, bygger i hovedsak på intervjuopplysninger. Revisjonen har ikke gjennomført en systematisk kontroll av etterlevelsen gjennom observasjon eller gjennomgang av enkeltsaker.

For kompetanse og opplæring undersøkes fylkeskommunens tiltak og oppfølging for å gi ansatte nødvendig informasjon og opplæring, samt dokumentasjon av gjennomførte tiltak. Revisjonen kartlegger ikke den enkelte ansattes faktiske kompetanse.

Revisjonen omfatter ikke testing av tekniske sikkerhetstiltak eller vurderinger av den tekniske utformingen av fylkeskommunens IKT-infrastruktur og sikkerhetsløsninger. Det er blant annet ikke gjennomført penetrasjonstesting, sårbarhetsskanning eller testing av tekniske sikkerhetsmekanismer. Tilgangsstyring er undersøkt gjennom rutiner, ansvarsfordeling og beskrivelser av tildeling, endring og avslutning av tilganger. Den enkelte brukers faktiske tilganger er ikke kontrollert.

Logging av tilgang til og aktivitet i fylkeskommunens informasjonssystemer er undersøkt som del av fylkeskommunens organisatoriske og systematiske sikkerhetsarbeid. Undersøkelsen omfatter rutiner for logging og opplysninger om fylkeskommunens bruk av stikkprøver, systematisk kontroll og hendelsesbasert gjennomgang av logger. Revisjonen har ikke gjennomgått selve loggene eller testet funksjonaliteten i løsningene for logging og overvåkning.

Innen tannhelse, personal og elevområdet undersøkes utvalgte krav til behandlingsprotokoller, informasjon til de registrerte og databehandleravtaler. Omtalen av behandlingsprotokoller bygger på gjennomgåtte rammer og maler samt intervjuopplysninger om registrering, ansvar og oppdatering. Undersøkelsen av informasjon til de registrerte omfatter innholdet i og tilgjengeligheten av utvalgte personvernerklæringer. Det er ikke undersøkt om den enkelte registrerte har lest informasjonen. Tre databehandleravtaler fra skole, tannhelse og personal er gjennomgått med tilhørende bilag.

Revisjonen omfatter ikke en fullstendig vurdering av fylkeskommunens etterlevelse av personvernregelverket eller øvrig regelverk om informasjonssikkerhet. Andre personvernkrav, herunder krav til vurderinger av personvernkonsekvenser, er ikke vurdert særskilt. Revisjonen omfatter heller ikke virksomheten til den eksterne tjenesteleverandøren innen tannhelse og elevområdet eller kontroll av leverandørenes etterlevelse av databehandleravtalene. Fylkeskommunens oppfølging av leverandørene er ikke undersøkt.

Revisjonen har ikke som formål å kontrollere alle behandlinger, systemer eller enkeltsaker innen de undersøkte tjenesteområdene. Dokumentasjon, utvalgte avtaler og opplysninger om systemer er benyttet for å belyse fylkeskommunens ordninger og beskrevne praksis på de undersøkte områdene.

1.4 Metode

Forvaltningsrevisjonen er gjennomført i henhold til NKRFs standard for forvaltningsrevisjon, RSK 001. Revisor har vurdert egen uavhengighet overfor Trøndelag fylkeskommune, jf. kommuneloven § 24-4 og forskrift om kontrollutvalg og revisjon kapittel 3.

Revisjonen bygger på dokumentgjennomgang, oppstartsmøte, intervjuer og supplerende informasjon innhentet underveis i gjennomføringen.

Oppstartsmøte og Intervjuer

Det ble gjennomført oppstartsmøte med Direktør for organisasjon og økonomi og informasjonssikkerhetskoordinator fra fylkeskommunen. Oppstartsmøte ble brukt til å informere om prosjektet, avklare praktiske forhold ved gjennomføringen og få innledende oversikt over relevante kontaktpunkter og informasjonsbehov.

I tillegg til oppstartsmøte ble det gjennomført 14 intervjuer. Alle er verifisert av informantene. Aktuelle informanter ble valgt ut med hjelp av kontaktperson (informasjonssikkerhetskoordinator) fra fylkeskommunen.

Det ble gjennomført intervju med følgende ansatte:

- Seksjonsleder organisasjon
- Fylkestannlege
- Leder kvalitet og internkontroll
- Seksjonsleder eksamen og støttetjenester
- Seksjonsleder jus og anskaffelser
- Seniorrådgiver digitalisering

- Informasjonssikkerhetskoordinator
- Sikkerhets- og beredskapsleder
- Direktør organisasjon og økonomi
- Seksjonsleder arkiv
- Personvernombud
- Seksjonsleder IKT
- Seksjonsleder kommunikasjon
- IKT sikkerhetskoordinator

Intervjuene omfatter sentrale funksjoner og utvalgte tjenesteområder med ansvar eller oppgaver innen informasjonssikkerhet, personvern og internkontroll. De er brukt til å belyse hvordan styringssystemer, rutiner og ansvarsforhold forstås og praktiseres, og til å innhente erfaringer med avvikshåndtering, opplæring, tilgangsstyring og personvernarbeid. Omtalen i rapporten er på rolle- og funksjonsnivå.

Det er også innhentet supplerende dokumentasjon gjennom intervjuene og underveis i gjennomføringen.

Dokumentgjennomgang

Revisor har gjennomgått skriftlig dokumentasjon om fylkeskommunens arbeid med informasjonssikkerhet og personvern. Dokumentasjonen omfatter styrende dokumenter, strategier, retningslinjer, rolle- og ansvarsbeskrivelser og system- og prosessbeskrivelser. Videre er dokumentasjon om risikostyring, avvik og sikkerhetshendelser, kompetanse og opplæring samt tilgangsstyring og logging gjennomgått. Fylkeskommunens årsrapport for 2025 inngår også i datagrunnlaget.

På personvernområdet omfatter gjennomgangen dokumentasjon om system- og behandlingsoversikter, rutiner for behandling av elevdata, pasientdata og personaldata, samt maler og arbeidsdokumenter for behandlingsprotokoller og vurderinger av personvernkonsekvenser. Omtalen av protokoller i tjenesteområdene bygger også på verifiserte intervjuopplysninger om registrering, ansvar og oppdatering.

Revisor har gjennomgått utvalgte publiserte personvernerklæringer som gjelder elever, tannhelsepasienter og ansatte. Gjennomgangen omfatter erklæringenes innhold og tilgjengelighet på fylkeskommunens nettsider. I tillegg er tre databehandleravtaler fra skole, tannhelse og personal gjennomgått med tilhørende bilag. Avtalene er undersøkt med hensyn til hvilke behandlinger, opplysningstyper og grupper av registrerte de gjelder, og hvordan leverandørens behandling av personopplysninger er regulert.

Dokumentasjonen er brukt til å beskrive formelle systemer, rutiner, ansvarsforhold og dokumenterte prosesser. Skriftlige beskrivelser er sammenholdt med verifiserte intervjuopplysninger for å belyse hvordan ordningene forstås og praktiseres.

Prosjektplanen åpnet for stikkprøver som en supplerende datakilde. I gjennomføringen er det gjennomgått utvalgt dokumentasjon, blant annet de tre databehandleravtalene. Revisor vurderte at gjennomgang av konkrete elev-, pasient- eller personalsaker ikke var nødvendig for å belyse prosjektets formål og kunne innebære innsyn i sensitive personopplysninger. Det ble derfor ikke gjennomført stikkprøver i enkeltsaker.

I fylkeskommunens styrende dokumenter og i intervjuer benyttes ulike benevnelser om funksjonen informasjonssikkerhetskoordinator. Revisor har lagt til grunn at benevnelsene viser til samme funksjon. Ved gjengivelse av opplysninger brukes benevnelsen informasjonssikkerhetskoordinator.

Vurdering av metode

Dokumentgjennomgangen og intervjuene belyser de undersøkte områdene fra ulike kilder. Dokumentene viser formelle krav, ansvar og ordninger, mens intervjuene gir informasjon om forståelse og beskrevet praksis. Sammenligning av opplysninger fra dokumenter og intervjuer gir grunnlag for å vurdere om beskrivelsene er sammenfallende eller viser forskjeller. Verifiseringen bidrar til å sikre at intervjuopplysningene er riktig gjengitt, men er ikke en selvstendig kontroll av at den beskrevne praksisen gjennomføres.

Kontaktpersonens kjennskap til organisasjonen har bidratt til å identifisere informanter med relevant ansvar, kunnskap og erfaring. Samtidig kan utvelgelsen ha påvirket hvilke perspektiver som er representert, og relevante erfaringer eller synspunkter kan ha blitt utelatt. Utvalget omfatter i hovedsak ledere og nøkkelpersoner, og gir ikke grunnlag for å beskrive alle ansattes erfaringer eller praksis i alle enheter.

Undersøkelsen gir et grunnlag for vurderinger av fylkeskommunens dokumenterte ordninger og beskrevne praksis innenfor de valgte områdene. Gjennomgangen av personvernerklæringer og databehandleravtaler gir også informasjon om innholdet i disse dokumentene. Det er ikke gjennomført stikkprøver i enkeltsaker, og den beskrevne praksisen er ikke systematisk kontrollert gjennom observasjon eller testing. Vurderingene er derfor avgrenset til den dokumentasjonen og praksisen datagrunnlaget belyser, og til revisjonens avgrensning som er beskrevet ovenfor.

1.5 Uttalelse om rapport

Rapporten ble sendt på høring til fylkesdirektør 15.10.26 med høringsfrist 29.10.26.

Det ble gjennomført et høringsmøte med informasjonssikkerhetskoordinator 29.10.26. På bakgrunn av opplysninger og presiseringer som kom frem i møtet, har revisor gjort noen få språklige justeringer i rapporten.

Revisor mottok høringsuttalelse fra fylkesdirektør 29.10.26. Høringsuttalelsen er vedlagt i vedlegg 2.

Endringene har ikke hatt betydning for revisors vurderinger og konklusjon.

1.6 Informasjonssikkerhet og personvern

Trøndelag fylkeskommune er en politisk styrt organisasjon med fylkestinget som øverste besluttende organ. Fylkesdirektøren er fylkeskommunens øverste administrative leder og har hovedansvaret for den daglige driften. Den administrative ledelsen består av fylkesdirektøren og direktører med ansvar for ulike fagområder.

Fylkeskommunen har oppgaver innen blant annet utdanning og kompetanse, tannhelse, veg, samferdsel, næring, plan og kulturmiljø, kultur, folkehelse, klima og miljø, eiendomsforvaltning samt administrasjon og støttetjenester.

Fylkeskommunens oppgaver utføres dermed gjennom en organisasjon med virksomheter innen flere tjenesteområder og på ulike steder i fylket. Flere av tjenesteområdene omfatter behandling av informasjon om blant annet elever, pasienter og ansatte. Digitale systemer inngår samtidig i både tjenesteproduksjonen og den interne administrasjonen.

Informasjon er en viktig del av oppgaveløsningen i offentlig sektor. I noen tjenester er behandling av informasjon selve kjernen i arbeidet, mens den i andre tjenester er nødvendig støtte for at oppgavene skal kunne utføres. Digitale systemer og nettverk er samtidig blitt viktige for de fleste oppgaver og tjenester i offentlig forvaltning. God informasjonssikkerhet har derfor betydning for virksomhetenes evne til å utføre oppgaver og levere tjenester[1].

Informasjonssikkerhet kan enkelt forklares som å passe på at informasjon ikke blir kjent for personer som ikke skal ha den, ikke blir endret ved en feil eller av uvedkommende, og er tilgjengelig når den trengs. I fagspråket kalles dette **konfidensialitet, integritet og**

[1] https://www.digdir.no/informasjonssikkerhet/felles-sikkerhet-i-forvaltningen/5957

tilgjengelighet. Informasjonssikkerhet gjelder informasjon i alle former og systemene som brukes til å behandle den[2].

I praksis kan dette handle om helt vanlige arbeidssituasjoner. En ansatt kan ha tilgang til opplysninger eller systemer som vedkommende ikke trenger for å gjøre jobben sin. Opplysninger kan bli slettet eller endret ved en feil, eller nødvendig informasjon kan være utilgjengelig for dem som skal bruke den. Datatilsynet peker på behovet for å beskytte personopplysninger mot blant annet uautorisert tilgang, utilsiktet tap og endringer, og for at opplysningene skal være tilgjengelige for autoriserte personer når det er nødvendig. Nasjonal sikkerhetsmyndighet (NSM) viser tilsvarende til at brukere ikke bør ha mer tilgang enn de trenger for å utføre arbeidet sitt[3][4].

Digital sikkerhet er en viktig del av informasjonssikkerheten. Digitaliseringsdirektoratet bruker begrepet digital sikkerhet når det i hovedsak handler om å sikre digitale elementer som IKT-systemer og nettverk. Informasjonssikkerhet er bredere fordi informasjon også kan komme på avveie eller bli behandlet feil uten at digitale systemer er involvert. Et eksempel fra Digitaliseringsdirektoratet er at en ansatt kan bryte taushetsplikten muntlig. Et slikt brudd gjelder informasjonssikkerhet, selv om det ikke har skjedd gjennom et digitalt system. (Digitaliseringsdirektoratet, *Felles sikkerhet i forvaltningen*)

Arbeidet med digital sikkerhet handler derfor om mer enn å beskytte seg mot dataangrep. NSMs grunnprinsipper for IKT-sikkerhet omfatter både tekniske og organisatoriske tiltak, og NSM peker blant annet på betydningen av ledelsesinvolvering, sikkerhetskompetanse og etablerte styrings- og rapporteringslinjer. Digitaliseringsdirektoratet viser samtidig til at uønskede hendelser innen informasjonssikkerhet ikke nødvendigvis skyldes angrep, og at informasjonssikkerhet må styres som en del av virksomhetens øvrige styring og risikohåndtering. (Nasjonal sikkerhetsmyndighet, *Hva er NSMs grunnprinsipper for IKT-sikkerhet?* Digitaliseringsdirektoratet, *Felles sikkerhet i forvaltningen*)

Når informasjonssikkerheten svikter, kan konsekvensene være større enn at et datasystem ikke fungerer som det skal. Digitaliseringsdirektoratet viser til at brudd på

---

[2] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/iverksette-styringssystem-for-informasjonssikkerhet/

[3] https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/integritet-og-konfidensialitet/

[4] https://nsm.no/getfile.php/1313975-1717589722/NSM/Filer/Dokumenter/Veiledere/NSMs%20Grunnprinsipper%20for%20IKT-sikkerhet%20v2.1.pdf

informasjonssikkerheten kan påvirke virksomhetens leveranser, økonomi og evne til å utføre oppgaver og yte tjenester. Hendelser kan også få konsekvenser for innbyggere og ansatte, andre virksomheter og samfunnsfunksjoner. (Digitaliseringsdirektoratet, *Felles sikkerhet i forvaltningen*)

Personvern og informasjonssikkerhet henger nært sammen, men er ikke det samme. Når personopplysninger behandles, skal blant annet opplysningenes integritet, konfidensialitet og tilgjengelighet beskyttes. Personvern omfatter samtidig flere hensyn enn sikkerheten rundt opplysningene. Datatilsynet viser blant annet til krav om at behandling av personopplysninger skal være lovlig, ha et bestemt formål, begrenses til nødvendige opplysninger, være korrekt og ikke vare lenger enn nødvendig. Informasjonssikkerhet er dermed en viktig del av personvernet, men dekker ikke alle kravene som gjelder ved behandling av personopplysninger[5].

Arbeidet med informasjonssikkerhet inngår i fylkeskommunens internkontroll. Kommuneloven krever at internkontrollen skal være systematisk, og at fylkeskommunen blant annet skal ha nødvendige rutiner og prosedyrer, avdekke og følge opp avvik og risiko for avvik, dokumentere internkontrollen og ved behov forbedre tiltakene. eForvaltningsforskriften stiller i tillegg krav om mål og strategi for informasjonssikkerhet og om internkontroll på informasjonssikkerhetsområdet som er tilpasset risiko. (Kommuneloven § 25-1; eForvaltningsforskriften § 15).

Et styringssystem for informasjonssikkerhet skal sikre sammenheng mellom mål, ansvar, risikovurderinger, rutiner, sikkerhetstiltak og oppfølging. Det omfatter både dokumenterte rammer og aktivitetene som skal sikre at disse brukes og forbedres. Styringssystemet inngår dermed i virksomhetens internkontroll[6].

Et systematisk sikkerhetsarbeid innebærer også at virksomheten må kunne oppdage og håndtere hendelser og bruke erfaringene til å forbedre sikkerheten. NSM[7] beskriver identifisering og kartlegging, beskyttelse, oppdagelse og håndtering og gjenoppretting som sentrale deler av IKT-sikkerhetsarbeidet. Datatilsynet[8] beskriver internkontroll som en

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

[6] https://www.digdir.no/informasjonssikkerhet/styringsaktiviteter/3153

[7] https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/introduksjon/de-fire-kategoriene/

[8] https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/oppfolging-og-opplaring/

kontinuerlig prosess der virksomheten blant annet må håndtere avvik og kontrollere at rutiner og tiltak brukes og fungerer etter hensikten.

Revisjonen undersøker fylkeskommunens arbeid med digital sikkerhet, med vekt på organisatoriske og styringsmessige forhold. Dette omfatter hvordan fylkeskommunen arbeider med informasjonssikkerhet gjennom styringssystemer og rutiner, avvik og forbedringsarbeid, kompetanse og opplæring samt tilgangsstyring. Ettersom fylkeskommunens digitale systemer også benyttes til behandling av personopplysninger, omfatter revisjonen utvalgte personvernkrav innen tannhelse, personal og elevområdet.

2 STYRINGSSYSTEMER OG RUTINER

Dette kapitlet omhandler fylkeskommunens styringssystemer og rutiner.

2.1 Delproblemstilling

Det er utarbeidet følgende delproblemstilling for temaet styringssystemer og rutiner:

- Har fylkeskommunen etablert rutiner og prosesser for å sikre informasjonssikkerhet, og i hvilken grad er disse gjort kjent og tatt i bruk i organisasjonen?

2.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne delproblemstillingen:

- Fylkeskommunen skal ha dokumenterte mål og strategi for informasjonssikkerhet i digitale tjenester og systemer.
- Fylkeskommunen skal ha avklart og dokumentert roller, ansvar og myndighet for informasjonssikkerhet og personvern.
- Fylkeskommunen skal ha nødvendige rutiner og prosedyrer for informasjonssikkerhet.
- Fylkeskommunen skal sikre at rutiner og prosedyrer for informasjonssikkerhet er gjort kjent, tilgjengelige og tatt i bruk i relevante deler av organisasjonen.
- Fylkeskommunen skal dokumentere internkontrollen for informasjonssikkerhet i den formen og det omfanget som er nødvendig.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

2.3 Funn

Dette kapitlet beskriver fylkeskommunens styringssystem for informasjonssikkerhet slik det kommer til uttrykk i tilgjengelig dokumentasjon og intervjudata. Datagrunnlaget består av styrende dokumenter, strategier, rutiner, organiseringsdokumenter, system- og prosessbeskrivelser, maler og arbeidsdokumenter samt intervjuer med ledere og nøkkelpersoner innen informasjonssikkerhet, personvern, arkiv, internkontroll og systemforvaltning. Intervjudata brukes til å belyse hvordan styringsdokumentene forstås, gjøres kjent og brukes i fylkeskommunen.

Informantene beskriver styringssystemet som bestående av styrende, gjennomførende og kontrollerende dokumenter. Dokumentasjonen omfatter strategier og ansvarsbeskrivelser,

rutiner for blant annet risikostyring og systemforvaltning, samt rutiner for ledelsens gjennomgang og sikkerhetsrevisjon.

Dokumentet Organisering, roller og ansvar – Informasjonssikkerhet fastsetter at fylkesdirektøren skal sørge for at styrende dokumenter i internkontrollen inngår i fylkeskommunens virksomhetsstyring. Ansvar, myndighet og rapportering skal som hovedregel følge linjen. Informantene beskriver at informasjonssikkerhet og personvern inngår i rapportering og ledelsesoppfølging. Leder for kvalitet og internkontroll opplyser at informasjonssikkerhet er lagt inn som et eget punkt i styringsprosessen i kvalitetssystemet, og at internkontrollarbeidet bygger på ISO[9]-basert metodikk.

Fylkeskommunen opplyser i rapporteringen for 2025 at styringssystemet er videreutviklet, og at videreutvikling av internkontrollen og overgang til nytt overordnet kvalitetssystem er prioritert. Flere informanter opplyser at dokumentasjon og rutiner flyttes til EQS[10] som del av dette arbeidet.

2.3.1 Mål og strategier for informasjonssikkerhet

Trøndelag fylkeskommune (TRFK) omtaler informasjonssikkerhet og personvern i Digitaliseringsstrategi 2022–2026. Strategien beskriver at fylkeskommunen skal arbeide systematisk og dokumentert for å tilby sikre tjenester, og at informasjonssikkerhet skal ivareta konfidensialitet, integritet og tilgjengelighet.

Informasjonssikkerhetsstrategi datert 20.02.2023 er fylkeskommunens overordnede styringsdokument for internkontroll for informasjonssikkerhet og personvern. Strategien er godkjent av fylkesdirektøren. Dokumentet opplyser at strategien ble revidert i 2025, da åpenhet ble tatt inn som prinsipp. Strategien gjelder all informasjonsbehandling i fylkeskommunen, herunder informasjon i digitale tjenester og systemer og behandling utført av leverandører der fylkeskommunen er behandlingsansvarlig.

Strategien angir at informasjonsbehandlingen skal være i samsvar med gjeldende regelverk og beste praksis, ivareta personvernet, bidra til tillit og støtte virksomhetens mål. Den skal samtidig ivareta konfidensialitet, integritet og tilgjengelighet. Prinsippene for arbeidet omfatter

[9] ISO-standarder er internasjonale standarder. ISO/IEC 27001 beskriver krav til styringssystemer for informasjonssikkerhet

[10] EQS er et elektronisk kvalitetssikringssystem som blant annet brukes til å samle og forvalte rutiner og dokumentasjon

blant annet virksomhetsstyring, anerkjente standarder, klart definerte roller og ansvar, kompetanse, risikostyring, systematisk arbeid, læring, åpenhet og informasjonsdeling.

Strategien fastsetter at arbeidet skal vurderes årlig i fylkesdirektørens ledergruppe. Rutinen og informantenes opplysninger om denne gjennomgangen er beskrevet i punkt 2.3.5.

2.3.2 Roller, ansvar og myndighet

Dokumentet Organisering, roller og ansvar – Informasjonssikkerhet (20.03.2023) beskriver fylkeskommunens ansvarsfordeling. Fylkesdirektøren har det overordnede ansvaret for informasjonssikkerhet og personvern og skal blant annet sørge for tilstrekkelige ressurser, at personvernombud er oppnevnt, og at ledelsens årlige gjennomgang synliggjøres i styringshjulet.

Leder for seksjon organisasjon har delegert ansvar for informasjonssikkerhet på vegne av fylkesdirektøren. Koordinator informasjonssikkerhet er plassert i denne seksjonen og skal etablere og videreutvikle internkontrollen, lede informasjonssikkerhetsgruppen, støtte enhetene og legge til rette for ledelsens gjennomgang.

Personvernombudet er plassert i seksjon jus og anskaffelser og skal blant annet gi råd, kontrollere overholdelsen av personvernforordningen og bistå ved opplæring, avvik og vurderinger av personvernkonsekvenser.

Informasjonssikkerhetsgruppen er etter dokumentet en rådgivende og koordinerende funksjon. Den skal bistå organisasjonen, bidra til sikkerhetskultur og informere fylkesdirektørens ledergruppe om saker som krever håndtering. Gruppen består av koordinator informasjonssikkerhet, IKT-sikkerhetskoordinator og personvernombud. Informantene opplyser at gruppen har statusmøter annenhver uke og møtes oftere ved behov. Det opplyses også at informasjonssikkerhetsfunksjonen bevisst er plassert utenfor IKT.

Forvaltningsmodell for informasjonssystemer i TRFK (17.04.2023) definerer systemeier, systemansvarlig, systemforvalter og systemdrift. Systemeier har det overordnede ansvaret for systemforvaltningen, er dataeier og har ansvar for risiko knyttet til databehandlingen. Rollen er ifølge modellen typisk plassert hos en leder med ansvar for den tjenesten systemet inngår i. Systemansvarlig har delegert ansvar for prosessene i systemets livsfaser, mens systemforvalter bistår med teknisk forvaltning. Rollene skal avklares tidlig i planleggingsfasen og gjelde til avviklingsfasen er fullført.

Ansvarsdokumentet fastsetter at systemeiere skal følge opp internkontrollarbeidet i systemforvaltningen. Dette omfatter å påse at personvernregelverket overholdes, at

nødvendig dokumentasjon og rutiner er etablert, og at risikovurderinger gjennomføres. Forvaltningsmodellen plasserer ansvaret for leverandøravtaler hos systemeier og beskriver systemansvarlig som hovedkontakt mot leverandør.

Informantene beskriver et skille mellom overordnet ansvar for rammeverk og styring og gjennomføring i linjen. Hver direktør har ansvar innen eget område, og systemeiere skal følge opp systemer og avtaler med støtte fra sentrale fagmiljøer. I intervjuet om personvernombudsrollen beskrives rollen som avklart for informanten selv. Samtidig opplyses det at kjennskapen til rollen varierer i organisasjonen.

Seksjonsleder for eksamen og støttetjenester opplyser at støttetjenester har systemeierskap for felles applikasjoner, mens den enkelte skole har systemeieransvar for løsninger som tas i bruk utenfor den felles anskaffelsen. Dette omfatter ansvar for sikkerhetsvurderinger og eventuell vurdering av personvernkonsekvenser. Arkivseksjonen beskrives som systemeier for flere sentrale arkiv- og samhandlingsløsninger. Innen tannhelse opplyses det at systemeierskapet for journalsystemet ligger i tjenesten, men at dokumentasjonen av roller og ansvar knyttet til dette systemet ikke er fullt ut på plass.

Saksnotatet Informasjonssikkerhet og personvern (20.04.2026) beskriver et forslag om en arbeidsgruppe som skal tydeliggjøre oppgavene til personvernombudet, informasjonssikkerhetsgruppen og informasjonssikkerhetskoordinatoren. Notatet omtaler også behov for å avklare hva som skal gjøres sentralt, og hva som skal gjøres i linjen.

Seksjonsleder IKT opplyser at han har ansvar for drift, forvaltning og utvikling av IKT, samt teknisk sikkerhet. Han opplyser at ansvaret for teknisk sikkerhet ikke er særskilt beskrevet i en stillingsbeskrivelse. Han beskriver samtidig at grenseflatene mellom teknisk sikkerhet og informasjonssikkerhet ikke er fullt ut avklart, og at det oppstår tvilstilfeller om hvor ansvaret ligger. Han viser til at han har fått oppgaver som han vurderer hører til informasjonssikkerhetsområdet, og at de sentrale sikkerhetsfunksjonene samarbeider tett og i praksis arbeider på tvers av sine områder.

Seksjonsleder IKT peker også på at ikke alle ledere nødvendigvis har tilstrekkelig forståelse av sitt ansvar for tekniske løsninger og systemer. Han opplyser at det er etablert et prosjekt som skal undersøke hva ansvaret innebærer, om de ansvarlige har fått tilstrekkelig opplæring, og om ansvaret er tatt inn i organisasjonen.

2.3.3 Rutiner og prosedyrer

Fylkeskommunen har dokumenterte rutiner og retningslinjer for blant annet risikostyring, innføring av informasjonssystemer, systemforvaltning, klassifisering av informasjon, varsling

av avvik og sikkerhetshendelser, sikkerhetsrevisjon og ledelsens gjennomgang. Dokumentene beskriver ansvar, arbeidsprosesser og krav til dokumentasjon og oppfølging.

Den overordnede rutinen for risikostyring av informasjonssikkerhet beskriver at risikovurderinger skal gjennomføres systematisk og periodisk, samt ved etablering eller større endringer i tjenester, systemer, prosesser eller trusselbilde. Vurderinger kan også utløses av avvik, sikkerhetshendelser, sikkerhetsrevisjoner, egenkontroller eller ledelsens gjennomgang. Vurderingene skal identifisere uønskede hendelser, vurdere sannsynlighet og konsekvens og danne grunnlag for risikoreduserende tiltak.

Risikoeier er i rutinen angitt som linjeleder, systemeier eller operativt ansvarlig for tjenesten eller systemet. Risikoeier skal håndtere risiko og følge opp nødvendige tiltak. Tiltaksplaner skal angi ansvar og frister. For systemer med lav risiko er det etablert en rutine for forenklet risikovurdering, med kriterier for bruk og krav til dokumentasjon og vurdering av restrisiko.

Retningslinje – nytt informasjonssystem beskriver at risikovurderinger skal starte tidlig i planleggingsfasen og danne grunnlag for sikkerhetskrav, tekniske og organisatoriske tiltak og vurdering av behov for personvernkonsekvensvurdering (DPIA)[11]. Ved anskaffelse eller tjenesteutsetting skal det stilles krav til informasjonssikkerhet og personvern med utgangspunkt i risiko. Retningslinjen beskriver også at behandlingsgrunnlag, databehandlerforhold, systemeierskap og ansvar skal avklares. Digitaliseringsstrategien fastsetter at alle digitaliseringsprosjekter skal risikovurderes, og at personvernombudet skal kobles på for vurdering av personvernkonsekvenser når personopplysninger samles inn og behandles.

Retningslinje – Klassifisering av informasjon gir veiledning om klassifisering, lagring og deling, særlig av ustrukturert informasjon. Dokumentet angir at informasjon som hovedregel skal behandles i egnet fagsystem med tilgangsstyring. Rutinen for varsling av sikkerhetshendelser og avvik beskriver varsling og kobler hendelser til risikovurdering, kvalitetsarbeid og forbedring. Retningslinjene for sikkerhetsrevisjon beskriver en årlig kontrollprosess, primært i seksjon IKT.

Rapporteringen for 2025 beskriver økt etterspørsel etter rådgivning om risikovurderinger og større oppmerksomhet på risikobaserte vurderinger ved innføring og endring av systemer. Fylkeskommunen opplyser samtidig at det er identifisert behov for helhetlige risikovurderinger av den digitale infrastrukturen og tydeligere forankring av risikostyringen.

[11] DPIA (Data protection Impact Assessment) er en vurdering av personvernkonsekvenser ved behandling av personopplysninger

Informantene beskriver at risikovurderinger og DPIA brukes ved anskaffelse og innføring av systemer, behandling av personopplysninger og i prosjekter og arbeidsprosesser. Flere peker samtidig på behov for faglig støtte og variasjoner i hvor godt kravene er kjent, og hvordan relevante fagressurser involveres. Informasjonssikkerhetskoordinatoren opplyser at det ikke er etablert egne kontroller med særskilt ansvar for å etterprøve at alle risikovurderinger gjennomføres. Dette beskrives som særlig vanskelig å følge opp for skyløsninger.

Seksjonsleder IKT opplyser at anskaffelsesretningslinjen brukes i anskaffelsesarbeidet. Han beskriver samtidig at den kan være komplisert å bruke når skoler eller andre enheter ønsker å anskaffe systemer, apper eller mindre digitale løsninger. Han opplyser at alt som tas i bruk, i prinsippet skal risikovurderes, og at tidligere vurderinger gjenbrukes der det er mulig.

Seksjonsleder IKT opplyser videre at det er laget en forenklet risikovurderingsmatrise, og at systemeiere ikke alltid har tilstrekkelig kunnskap til å gjennomføre vurderingene alene. Mindre systemer beskrives som avhengige av støtte. Arbeidet beskrives som ressurskrevende, og etter hans vurdering er det ikke tilstrekkelige ressurser til å gjennomføre risikovurderinger på en god måte i alle tilfeller.

2.3.4 Kjennskap til og bruk av rutiner

Informasjonssikkerhetsstrategien fastsetter at ansatte skal ha tilstrekkelig kunnskap om informasjonssikkerhet og personvern og følge gjeldende lover og retningslinjer. Ansvarsdokumentet fastsetter at ledere med personalansvar skal sørge for nødvendig sikkerhetsforståelse og kunnskap hos ansatte. Ansatte har ansvar for å følge vedtatte rutiner og reglement.

IKT-reglement 2023 angir at alle med brukerkonto og tilgang til fylkeskommunens IKT-tjenester skal bekrefte digitalt at reglementet er lest og forstått. Bekreftelsen skal gjentas dersom reglementet endres.

Informantene beskriver at styrende dokumenter formidles gjennom intranett, Viva Engage, ledelseslinjen og møtefora, blant annet rektormøter. Seksjonene bruker også direkte kontakt, e-post, telefon, møter og besøk i enhetene. Det gjennomføres informasjon og opplæring gjennom blant annet nanolæring, phishingkampanjer og møter og samlinger for ledere og ansatte. Informasjonssikkerhetsgruppen har vært involvert i kvalitetssikring av informasjonsmateriell.

Flere informanter beskriver utfordringer med å nå hele organisasjonen. Dette knyttes til geografisk spredning, variasjon i sikkerhetskultur og at enkelte deler av virksomheten, særlig

skolene, i mindre grad bruker intranettet. Dagens løsninger gir oversikt over antall klikk på saker og rutiner, men ikke hvem som har lest innholdet.

Kunnskap om informasjonssikkerhet, personvern og rutiner beskrives som varierende. Enkelte rutiner er lite kjent og i varierende grad tatt i bruk. Det opplyses også at det ikke nødvendigvis er kjent om alle ansatte kjenner innholdet i rutinene. Enkelte informanter viser til at spørsmål om blant annet apper og filming av elever jevnlig kommer fra skoleområdet, og til et ønske om lik praksis mellom skolene.

Opplysningene om bruk av anskaffelsesrutiner, risikovurderinger og DPIA er beskrevet i punkt 2.3.3. Informantene beskriver samtidig at oppfølging av sikkerhetstiltak i hovedsak skjer gjennom linjeansvaret. Ledere og systemeiere forventes å følge opp tiltak innen egne områder. Det beskrives variasjoner mellom tjenesteområdene i modenhet og grad av systematikk, og enkelte informanter peker på behov for tydeligere ansvarslinjer og mer enhetlige arbeidsformer.

2.3.5 Dokumentasjon av internkontrollen

Rutinen for risikostyring fastsetter at risikovurderinger og tiltaksplaner skal journalføres i sak- og arkivsystemet. Retningslinjen for nye informasjonssystemer stiller dokumentasjonskrav til risikovurderinger, DPIA og andre vurderinger ved etablering eller endring av systemer. Forvaltningsmodellen fastsetter at dokumentasjon av systemforvaltning, behandlingsprotokoller og øvrig systemdokumentasjon skal etableres og vedlikeholdes gjennom systemets livsløp.

Retningslinje – nytt informasjonssystem beskriver at behandlingsprotokoll skal utarbeides før behandlingen starter, og at system, systemeier og systemansvarlig skal dokumenteres i Samsvar.[12] Fylkeskommunen har arbeidsdokumenter for behandlingsprotokoll og DPIA som skal støtte dokumentasjonen av behandlinger og vurderinger. Ansvarsdokumentet fastsetter at systemeier skal påse at blant annet behandlingsprotokoll og databehandleravtale er etablert.

Rutine for ledelsens gjennomgang av informasjonssikkerhet og personvern beskriver en årlig prosess i fylkesdirektørens ledergruppe. Gjennomgangen skal vurdere status opp mot strategiens mål og prinsipper, effekten av sikkerhetsarbeidet og behov for korrigerende tiltak. Den skal omfatte pågående aktiviteter, revisjon av styrende elementer, avvik og hendelser,

[12] Samsvar er en løsning fylkeskommunen bruker til å registrere og dokumentere informasjonssystemer og behandling av personopplysninger

forbedringstiltak og oppfølging. Koordinator informasjonssikkerhet skal rapportere om status for tiltak fra forrige gjennomgang. Referatet skal journalføres og dokumentere beslutninger, tiltak og begrunnelser. Tiltakslisten skal brukes ved neste gjennomgang, der effekten av tiltakene også skal vurderes. Ansvarsdokumentet fastsetter at dokumentet skal revideres årlig i forbindelse med ledelsens gjennomgang.

Retningslinjene for sikkerhetsrevisjon fastsetter at årlige revisjoner og tiltak skal dokumenteres og arkiveres. Kontrollpunktene skal revideres, og data og tiltak skal dokumenteres på Teams og arkiveres i 360.

Informantene opplyser at ledelsens gjennomgang gjennomføres årlig og brukes til å behandle status, utvikling, forbedringstiltak og prioriteringer. Flere beskriver at rapportering og oppfølging bidrar til å forme beslutninger og prioriteringer.

Flere informanter beskriver at Samsvar brukes til oversikt over systemer, systemeiere, leverandører, drift og behandlingsprotokoller. Leverandøravtaler opplyses å være lagret i andre systemer. Seksjonsleder IKT opplyser at fylkeskommunen har oversikt over systemeiere og en tjenestekatalog, men at arbeidet med katalogen fortsatt pågår.

Fylkeskommunens rapportering for 2025 beskriver arbeidet med systemoversikt som i en tidlig fase, med betydelig gjenstående arbeid før systemporteføljen er helhetlig dokumentert. Informantene beskriver også at det arbeides med å etablere fullstendige oversikter over systemer og behandlinger. Dette krever bidrag fra systemeiere, og enkelte opplyser at det har vært krevende å få enhetene til å registrere og dokumentere alle systemer.

Fra skoleområdet opplyses det at behandlingsprotokoller og DPIA i hvert fall er etablert for de største systemene. Fra tannhelsetjenesten opplyses det at det finnes behandlingsprotokoller for journalsystemet og andre digitale fagsystemer. Arkivområdet beskriver samarbeid med informasjonssikkerhetsfunksjonen om behandlingsprotokoller for arkivsystemene.

Informantene beskriver at systemeiere og andre ansvarlige funksjoner skal registrere og vedlikeholde dokumentasjon med støtte fra sentrale fagressurser. Samtidig opplyses det at dokumentasjonen ikke er fullstendig på alle områder, at ansvar for ajourhold og oppdatering kan være uklart, og at dokumentasjonspraksis varierer mellom tjenesteområdene. Dokumentasjonen er fordelt mellom flere løsninger, og arbeidet med å samle den i et mer helhetlig kvalitetssystem pågår.

2.4 Vurdering

Fylkeskommunen har dokumenterte mål og strategi for informasjonssikkerhet i digitale tjenester og systemer.

Revisor vurderer at fylkeskommunen har dokumenterte mål og strategi for informasjonssikkerhet i digitale tjenester og systemer. Digitaliseringsstrategien omtaler informasjonssikkerhet og personvern, og informasjonssikkerhetsstrategien fastsetter mål og prinsipper for fylkeskommunens informasjonsbehandling. Strategien er godkjent av fylkesdirektøren og omfatter også digitale tjenester og systemer. Det er dessuten fastsatt at arbeidet skal vurderes årlig i fylkesdirektørens ledergruppe.

Revisor vurderer at revisjonskriteriet er **oppfylt.**

Fylkeskommunen har i hovedsak avklart og dokumentert roller, ansvar og myndighet for informasjonssikkerhet og personvern.

Revisor vurderer at fylkeskommunen har i hovedsak dokumentert en overordnet fordeling av roller, ansvar og myndighet for informasjonssikkerhet og personvern. Ansvarsdokumentet beskriver linjeansvaret og de sentrale funksjonene, mens forvaltningsmodellen beskriver ansvar og oppgaver knyttet til informasjonssystemene. Samlet gir dokumentene et grunnlag for å plassere ansvar både på overordnet nivå og i relevante tjenesteområder. Intervjuopplysningene understøtter beskrivelsen av linjeansvaret og systemeiernes ansvar.

Datagrunnlaget viser samtidig at det fortsatt er behov for enkelte avklaringer og presiseringer av roller og ansvar. Revisor vurderer at dette ikke endrer hovedbildet av en etablert og dokumentert ansvarsfordeling, men viser at arbeidet med å tydeliggjøre denne ikke er fullt ut avsluttet.

Revisor vurderer på denne bakgrunn at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen har nødvendige rutiner og prosedyrer for informasjonssikkerhet

Revisor vurderer at fylkeskommunen har nødvendige rutiner og prosedyrer for informasjonssikkerhet på de undersøkte områdene. Rutinene omfatter blant annet risikostyring, innføring og forvaltning av informasjonssystemer, klassifisering, avvikshåndtering, sikkerhetsrevisjon og ledelsens gjennomgang. De beskriver ansvar, arbeidsprosesser og krav til dokumentasjon og oppfølging.

Styringssystemet er under videreutvikling, og det er identifisert behov for å gjennomføre helhetlige risikovurderinger av den digitale infrastrukturen og forankre risikostyringen tydeligere. Disse forholdene, sammen med opplysninger om støttebehov, ressursutfordringer og kompliserte rutiner, gjelder i hovedsak gjennomføringen av sikkerhetsarbeidet. Det er ikke påvist konkrete mangler ved rutinenes innhold eller dekning på de undersøkte områdene.

Revisor vurderer at revisjonskriteriet **er oppfylt.**

Fylkeskommunen sikrer delvis at rutiner og prosedyrer for informasjonssikkerhet er gjort kjent, tilgjengelige og tatt i bruk i relevante deler av organisasjonen.

Revisor vurderer at fylkeskommunen har gjennomført flere tiltak for å gjøre rutiner og prosedyrer for informasjonssikkerhet kjent og tilgjengelige, blant annet gjennom interne informasjonskanaler, ledelseslinjen og opplæring. Intervjuopplysningene viser også at sentrale rutiner brukes på flere områder, blant annet ved anskaffelser og risikovurderinger.

Intervjuene viser samtidig at enkelte rutiner er lite kjent og i varierende grad tatt i bruk. Det beskrives utfordringer ved lokale anskaffelser, behov for støtte til risikovurderinger og variasjoner mellom tjenesteområdene i hvor systematisk rutinene følges. Dette viser at tiltakene for å formidle rutinene ikke fullt ut har sikret at de er kjent og brukes i relevante deler av organisasjonen.

Opplysningene om kjennskap og bruk bygger på intervjuer med ledere og nøkkelpersoner. Revisjonen har ikke gjennomført en systematisk kontroll av etterlevelsen gjennom observasjon eller gjennomgang av enkeltsaker. Datagrunnlaget gir derfor ikke grunnlag for å fastslå det samlede omfanget av manglende etterlevelse. Revisor vurderer likevel at de beskrevne svakhetene gir grunnlag for å konkludere med at fylkeskommunen ikke fullt ut har sikret kjennskap til og bruk av rutinene.

Revisor vurderer at revisjonskriteriet er **delvis oppfylt.**

Fylkeskommunen dokumenterer delvis internkontrollen for informasjonssikkerhet i den formen og det omfanget som er nødvendig.

Revisor vurderer at fylkeskommunen har etablert dokumentasjonskrav for sentrale deler av internkontrollen, blant annet risikovurderinger, systemforvaltning, behandlingsprotokoller, vurderinger av personvernkonsekvenser (DPIA) og ledelsens gjennomgang. Intervjuopplysningene viser at flere av disse aktivitetene dokumenteres, og at fylkeskommunen

arbeider med å samle dokumentasjon og rutiner i EQS. At dokumentasjonen er fordelt på flere løsninger, innebærer ikke i seg selv at dokumentasjonen av internkontrollen er mangelfull.

Rapporteringen og intervjuene viser samtidig at oversiktene over systemer og behandlinger av personopplysninger er ufullstendige. Det beskrives også uklarheter om ansvar for ajourhold og variasjoner i dokumentasjonspraksis mellom tjenesteområdene. Ufullstendige oversikter svekker grunnlaget for å identifisere risiko og følge opp sikkerhetsarbeidet. Uklarheter om ansvar for ajourhold svekker dessuten forutsetningene for å holde dokumentasjonen oppdatert.

Revisor vurderer derfor at fylkeskommunen ikke fullt ut dokumenterer internkontrollen i det omfanget som er nødvendig på de undersøkte områdene.

Revisor vurderer at revisjonskriteriet er **delvis oppfylt.**

3 AVVIK OG FORBEDRINGSARBEID

Dette kapitlet omhandler avvik og forbedringsarbeid.

3.1 Delproblemstilling

Det er utarbeidet følgende delproblemstilling for temaet avvik og forbedringsarbeid:

- Har fylkeskommunen etablert rutiner for håndtering av avvik og sikkerhetshendelser innen informasjonssikkerhet, og hvordan brukes avvik i arbeidet med å forbedre internkontrollen?

3.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne delproblemstillingen:

- Fylkeskommunen skal ha skriftlige rutiner for å avdekke, registrere, klassifisere, behandle og følge opp avvik og sikkerhetshendelser knyttet til informasjonssikkerhet.
- Fylkeskommunen skal ha rutiner som sikrer at brudd på personopplysningssikkerheten vurderes og dokumenteres.
- Fylkeskommunen skal bruke avvik, sikkerhetshendelser og risiko for avvik som grunnlag for forbedring av internkontrollen for informasjonssikkerhet.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

3.3 Funn

Dette kapitlet beskriver fylkeskommunens rutiner og praksis for avvik og sikkerhetshendelser innen informasjonssikkerhet og personvern. Datagrunnlaget består av rutiner for varsling, registrering og oppfølging av avvik, dokumenter om risikostyring og ledelsens gjennomgang, årsrapporten for 2025 og intervjuer med sentrale funksjoner og utvalgte tjenesteområder.

Revisjonen har ikke hatt en samlet avviksoversikt som grunnlag for undersøkelsen. Omtalen av registrering, behandling og oppfølging i praksis bygger på opplysninger i årsrapporten og intervjuene. Eksempler fra intervjuene belyser håndteringen av utvalgte hendelser.

3.3.1 Avdekking, registrering, klassifisering og oppfølging

Rutine – varsling av sikkerhetshendelse eller avvik gjelder for alle enheter i fylkeskommunen og er tilgjengelig på intranettet. Rutinen fastsetter at avvik og sikkerhetshendelser skal varsles, dokumenteres og følges opp som del av fylkeskommunens internkontroll. Alle med tilgang til

fylkeskommunens IKT-systemer har ansvar for å være oppmerksomme på mulige sikkerhetsbrudd og avvik, melde fra og bidra til god sikkerhetskultur.

Rutinen skiller mellom sikkerhetshendelser og avvik. En sikkerhetshendelse beskrives som uautorisert tilgang til informasjon, utilsiktet eller ulovlig endring av data, eller at data og systemer blir utilgjengelig over tid. Avvik innen informasjonssikkerhet og personvern beskrives som situasjoner der lovverk eller interne rutiner ikke etterleves. Eksemplene omfatter personopplysning sendt til feil mottaker, feilpublisering, feil i tilganger eller sikkerhetsmekanismer, manglende rutiner, rutiner som ikke følges, manglende risikovurdering og bruk av leverandør uten godkjent databehandleravtale.

Den ansatte som blir kjent med et mulig sikkerhetsbrudd eller avvik skal melde fra. Ved usikkerhet om situasjonen er en sikkerhetshendelse eller et avvik, åpner rutinen for å melde fra som om det er en sikkerhetshendelse og kontakte nærmeste leder. Nærmeste leder, IKT-hjelp og informasjonssikkerhetsgruppen er angitt som ressurser i vurderingen. Ved sikkerhetshendelser er IKT-hjelp første kontaktpunkt. Hendelser som truer informasjonssikkerhet, daglig drift eller tjenesteproduksjon skal varsles raskt dit.

IKT reglementet 2023 omtaler også brukeransvar for varsling. Reglementet gjelder alle med brukerkonto som gir tilgang til fylkeskommunens IKT-tjenester. Forhold som kan ha betydning for IKT-tjenestenes sikkerhet, skal varsles til seksjon IKT eller IKT ved skolen. Brudd på personvern skal varsles til nærmeste leder, kontaktlærer eller personvernombud.

Avvik og sikkerhetshendelser skal registreres i TQM[13]. Lenke til systemet er tilgjengelig på intranettet. Avviksarbeidet følger linjen, og leder for enheten hvor avviket meldes inn, er ansvarlig for oppfølgingen. Ved avvik innen informasjonssikkerhet og personvern sendes kopi til koordinator informasjonssikkerhet og personvernombudet. Tiltak kan tildeles saksbehandlere på andre fagområder, for eksempel IKT eller informasjonssikkerhet.

Registrering skal omfatte en beskrivelse av avviket eller hendelsen, tiltak for å håndtere forholdet og tiltak for å forbedre arbeidsprosessen. Rutinen stiller også krav til vurderinger ved personvernbrudd. Disse er nærmere omtalt i delkapittel 3.3.3.

3.3.2 Registrering og oppfølging i praksis

Flere informanter beskriver at avvik registreres i avvikssystemet og sendes til nærmeste leder. Lederen vurderer hvilke funksjoner som skal involveres i den videre behandlingen. Ved behov

[13] TQM er et elektronisk kvalitets- og avvikssystem som fylkeskommunen bruker til å registrere og følge opp avvik og sikkerhetshendelser

involveres informasjonssikkerhetskoordinator eller relevante IKT- fagmiljøer. Enkelte avvik, særlig innen IKT-sikkerhet behandles av relevante fagmiljøer. Vesentlige avvik kan løftes til overordnet nivå og håndteres etter etablerte rutiner for sikkerhetshendelser, herunder eventuell melding til statlige myndigheter. Informantene beskriver også at avvik inngår i den overordnede rapporteringen, blant annet gjennom tertialrapportering.

Fylkestannlegen opplyser at avvik knyttet til personvern håndteres gjennom det ordinære avvikssystemet. Avvikene sendes til fylkestannlegen, personvernombudet og informasjonssikkerhetskoordinator. Fylkestannlegen har ansvar for oppfølgingen, men kan delegere gjennomføringen av tiltak til teamleder for distriktet. Når tiltakene er gjennomført, lukker fylkestannlegen avviket, og personvernombudet og informasjonssikkerhetskoordinator mottar melding. Fylkestannlegen opplyser videre at han opplever at ansatte i større grad melder avvik som medfører hindringer eller ulemper for dem selv, enn avvik de selv har gjort.

Seksjonsleder IKT opplyser at han mottar avvik som gjelder tekniske forhold, men også enkelte avvik som gjelder informasjonssikkerhet, han beskriver at det kan være vanskelig å skille mellom teknisk sikkerhet og informasjonssikkerhet i avvikshåndteringen. Som eksempel viser han til et tilfelle der en ansatt hadde tilgang til flere opplysninger enn vedkommende hadde behov for. Dette ble oppdaget av en ansatt i IKT og meldt som avvik og videre rettet. Han opplyser videre at IKT også melder avvik dersom de oppdager anskaffelser eller systemer som ikke er håndtert i tråd med rutinene.

IKT-sikkerhetskoordinatoren opplyser at det meldes avvik når anskaffelser ikke er gjennomført i tråd med etablerte retningslinjer. Han viser også til at enkelte anskaffelser reiser spørsmål om sikkerhetsrisiko, og beskriver behov for prinsipielle avklaringer knyttet til slike anskaffelser.

I årsrapporten for 2025 beskriver fylkeskommunen en fortsatt økning i antall innmeldte avvik og forbedringsforslag, med om lag 40 flere innmeldinger enn i 2024. Opplysningene gjelder samlet antall avvik og forbedringsforslag. Fylkeskommunen opplyser også at en egen retningslinje for håndtering av avvik, sammen med opplæring, fokus og bevisstgjøring, har medført økning i antall innmeldte og behandlede saker i kategorien «brudd på informasjonssikkerhet/personvern». Det er registrert avvik og sikkerhetshendelser knyttet til blant annet tilgangsstyring, feil håndtering av informasjon og sosial manipulering. Fylkeskommunen beskriver utviklingen i avviksrapportering som en indikasjon på økt bevissthet i organisasjonen.

Når det gjelder avvik hos leverandører opplyser enkelte informanter at oppfølgingen skjer innenfor rammene av de aktuelle avtalene. Avtaleeier må da vurdere konsekvensene og behovet for tiltak og videre oppfølging.

3.3.3 Håndtering og dokumentasjon av brudd på personopplysningssikkerheten

Rutiner for håndtering og dokumentasjon av brudd på personopplysningssikkerheten

Fylkeskommunens rutine bruker begrepet «brudd på personvern» om både brudd på personopplysningssikkerheten og andre brudd på de registrertes rettigheter. Rutinen angir at situasjonen må omfatte personopplysninger. Personvernforordningens regler om melding til Datatilsynet etter artikkel 33 gjelder brudd på personopplysningssikkerheten.

Rutinen stiller et generelt krav om registrering av avvik og sikkerhetshendelser i TQM, uavhengig av om bruddet meldes til Datatilsynet. Registreringen skal inneholde en beskrivelse av avviket eller hendelsen, vurdering av meldeplikt og behov for å informere berørte personer, samt tiltak for å håndtere forholdet og forbedre arbeidsprosessen. Rutinen beskriver også hvilke konsekvenser for de registrerte som bør vurderes. Virkningene av bruddet er imidlertid ikke uttrykkelig angitt blant opplysningene som skal registreres.

Rutinen angir at konsekvensene for de registrerte skal vurderes. Eksemplene omfatter tap av kontroll over egne personopplysninger, forskjellsbehandling, identitetstyveri, økonomisk tap, omdømmeskade, tap av fortrolighet og taushetsbelagte opplysninger og andre betydelige økonomiske eller sosiale ulemper. Personvernombudet og koordinator for informasjonssikkerhet er angitt som ressurser i vurderingen av om det foreligger brudd på personvern.

Rutinen angir at den enkelte skal vurdere om bruddet er meldepliktig. Det kommer frem at brudd skal meldes til Datatilsynet innen 72 timer fra det blir oppdaget. Rutinen beskriver videre at *«et brudd er meldepliktig dersom det er sannsynlig at det medfører en risiko for fysiske personers rettigheter og friheter».* Dersom alle opplysningene ikke er kjent innen fristen, kan utfyllende informasjon ettersendes. Koordinator informasjonssikkerhet kan bistå med meldingen som skal arkiveres i sak- og arkivsystem.

Håndtering av brudd i praksis

Personvernombudet opplyser at hun mottar kopi dersom personvernavviket sendes gjennom avvikssystemet, og at hun blir orientert sammen med seniorrådgiver for informasjonssikkerhet. Leder for seksjonen der avviket er meldt skal behandle avviket- personvernombudet behandler ikke avviket selv, men gir råd ved behov. Hun beskriver at hun oftere involveres når leder er i tvil om behandlingen, for eksempel om avviket skal meldes til Datatilsynet.

Flere informanter opplyser at avvik som gjelder personvern og informasjonssikkerhet håndteres internt og meldes til Datatilsynet når det er aktuelt. Informanter opplyser også at avvik som berører mange personer, alltid meldes til Datatilsynet, og at de berørte varsles i tråd med etablerte rutiner.

3.3.4 Bruk av avvik, sikkerhetshendelser og risiko i forbedringsarbeidet

Rutine for læring og forbedring

Rutine – varsling av sikkerhetshendelser eller avvik kobler avvik og hendelser til læring og forbedring. Formålet er blant annet å redusere konsekvensene av sikkerhetshendelser, lukke sårbarheter for å forhindre fremtidige hendelser, bruke hendelser og avvik som grunnlag for risikovurdering og kvalitetsarbeid og etterleve krav til varsling, avvikshåndtering og internkontroll. Registrering i TQM skal omfatte både tiltak for å håndtere avviket eller hendelsen og tiltak for å forbedre arbeidsprosessen.

Dokumentet Risikostyring av informasjonssikkerhet beskriver avvik og hendelser som forhold som kan utløse behov for risikovurdering. Risikovurderinger kan også initieres av status eller hendelser identifisert ved sikkerhetsrevisjon, egenkontroll eller ledelsens gjennomgang.

Retningslinje for sikkerhetsrevisjon gjelder primært seksjon IKT og beskriver en årlig sikkerhetsrevisjon. Kontrollpunkter skal revideres, og data fra revisjonen skal dokumenteres på Teams og arkiveres i 360. Resultatet skal tas opp i eget møte etter revisjonen, der tiltak planlegges.

Bruk i forbedringsarbeidet i praksis

Informantene gir ulike beskrivelser av hvordan avvik brukes i forbedringsarbeidet. Flere viser til at avvik kan brukes som grunnlag for læring, kvalitetsarbeid og forbedring, men beskriver samtidig variasjoner mellom enheter når det gjelder registrering, dokumentasjon og oppfølging. Det opplyses at avvik ikke systematisk benyttes som grunnlag for rutineendringer, selv om hendelser kan føre til informasjonstiltak, opplæring og oppdatering av rutiner. Flere peker også på at avvik kan synliggjøre systemfeil, brukerfeil og uklarheter i rutiner, som igjen kan gi grunnlag for forbedringstiltak.

Fylkestannlegen forteller at tannhelsetjenesten har erfaring med å bruke avvik til å forbedre rutiner. Det som oppfattes som alvorlig, tas sentralt inn til fylkestannlegens kontor. Rådgiver utarbeider forslag til ny rutine, som behandles i ledergruppen, partsgruppen og deretter i arbeidsmiljøutvalget. Etter dette ferdigstilles rutinen av rådgiver og godkjennes av fylkestannlegen.

Informasjonssikkerhetskoordinator beskriver at man har et forbedringspotensial når det kommer til å bruke avvik i forbedringsarbeid. Hun viser til at avvik kan brukes mer systematisk til læring og kvalitetsarbeid. Det beskrives også at det er variasjoner mellom enheter.

Videre beskriver noen informanter utfordringer med å følge sammenhengen mellom årsaker, tiltak og resultater i dagens avvikssystem. Det opplyses at systemet i begrenset grad har støttet systematisk oppfølging av årsakssammenhenger og tiltak. Overgangen fra TQM til EQS omtales som et tiltak for å gi bedre systemstøtte til oppfølging og forbedring.

Enkelte informanter viser også til at erfaringer fra avvik hos leverandører kan brukes i forbedringsarbeidet, blant annet knyttet til kompetanse og oppfølging av leverandørforhold.

3.4 Vurdering

Fylkeskommunen har rutiner for å avdekke, registrere, klassifisere, behandle og følge opp avvik og sikkerhetshendelser knyttet til informasjonssikkerhet.

Revisor vurderer at fylkeskommunen har skriftlige rutiner som dekker avdekking, registrering, klassifisering, behandling og oppfølging av avvik og sikkerhetshendelser innen informasjonssikkerhet. Rutinene beskriver ansattes ansvar for å melde fra, skiller mellom avvik og sikkerhetshendelser og gir eksempler som støtter vurderingen av hvilken type forhold det gjelder. De beskriver også varslingskanaler, registrering i avvikssystemet og ansvar for videre behandling og oppfølging.

Revisor legger vekt på at rutinene omfatter både håndtering av hendelsen og tiltak for å forbedre arbeidsprosessen. Intervjuopplysningene understøtter at avvikssystemet brukes, og at ledere og relevante fagfunksjoner involveres i behandlingen.

Revisor vurderer at revisjonskriteriet er **oppfylt.**

Fylkeskommunen har i hovedsak rutiner som sikrer at brudd på personopplysningssikkerheten vurderes og dokumenteres.

Revisor vurderer at fylkeskommunen har rutiner som beskriver sentrale vurderinger ved brudd på personopplysningssikkerheten og stiller krav til registrering og dokumentasjon. Registreringskravet gjelder uavhengig av om bruddet meldes til Datatilsynet. Rutinen krever at hendelsen, vurderingen av meldeplikt, behovet for å informere berørte personer og tiltak dokumenteres. Den beskriver også hvilke konsekvenser for de registrerte som bør vurderes, og hvilke funksjoner som kan bistå.

Beskrivelsen av meldeplikten er imidlertid ikke tilstrekkelig presis. Kravet om melding uten ugrunnet opphold kommer ikke tydelig frem, og formuleringen om risiko kan gi inntrykk av en høyere terskel for melding enn det som følger av personvernforordningen artikkel 33. Uklarhetene kan medføre at meldepliktige brudd ikke meldes, eller at melding utsettes uten grunnlag. Revisor vurderer derfor at rutinen bør presiseres for å gi tydelig veiledning om meldeplikten.

Revisor vurderer at revisjonskriteriet er i **hovedsak oppfylt.**

Fylkeskommunen delvis bruker avvik, sikkerhetshendelser og risiko for avvik som grunnlag for forbedring av internkontrollen for informasjonssikkerhet

Revisor vurderer at fylkeskommunen har etablert rutiner som legger til rette for å bruke avvik, sikkerhetshendelser og risiko for avvik som grunnlag for forbedring av internkontrollen. Avviksrutinen omfatter forbedring av arbeidsprosesser, og dokumentene om risikostyring og sikkerhetsrevisjon beskriver hvordan hendelser og identifiserte risikoforhold kan følges opp gjennom risikovurderinger og tiltak.

Intervjuopplysningene viser at avvik brukes i forbedringsarbeidet, blant annet gjennom informasjonstiltak, opplæring og oppdatering av rutiner. Samtidig beskriver flere informanter variasjoner mellom enheter og behov for mer systematisk bruk av avvik til læring og forbedring. Det beskrives også utfordringer med å følge sammenhengen mellom årsaker, tiltak og resultater i avvikssystemet. Etter revisors vurdering svekker dette grunnlaget for systematisk læring og forebygging av nye avvik.

Vurderingen av praksis bygger på intervjuopplysninger og fylkeskommunens rapportering. Revisjonen har ikke gjennomgått en samlet avviksoversikt eller kontrollert behandlingen av et utvalg avvikssaker. Datagrunnlaget gir derfor begrenset innsikt i omfanget og effekten av forbedringsarbeidet. Opplysningene gir også mindre grunnlag for å vurdere hvordan risiko for avvik brukes i praksis. Revisor vurderer likevel at de beskrevne svakhetene gir grunnlag for å konkludere med at bruken av avvik i forbedringsarbeidet ikke er tilstrekkelig systematisk på de undersøkte områdene.

Revisor vurderer at revisjonskriteriet er **delvis oppfylt.**

4 KOMPETANSE OG OPPLÆRING

Dette kapitlet omhandler kompetanse og opplæring innen informasjonssikkerhet.

4.1 Delproblemstilling

Det er utarbeidet følgende delproblemstilling for temaet kompetanse og opplæring:

- Har fylkeskommunen etablert og fulgt opp tiltak for å gi ansatte nødvendig informasjon, opplæring og kompetanseutvikling innen informasjonssikkerhet?

4.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne delproblemstillingen:

- Fylkeskommunen skal sikre at ansatte og andre brukere som får tilgang til digitale systemer og personopplysninger, får nødvendig opplæring om sikker bruk, konfidensialitet, tilgangsstyring, avvikshåndtering og behandling av personopplysninger.
- Fylkeskommunen skal sikre at ansatte som behandler elevdata, pasientdata eller personaldata får nødvendig informasjon og opplæring om relevante krav i regelverk og interne rutiner.
- Fylkeskommunen skal dokumentere gjennomførte opplærings- og informasjonstiltak i det omfanget som er nødvendig for å kunne følge opp internkontrollen.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

4.3 Funn

Dette kapitlet beskriver fylkeskommunens tiltak for informasjon, opplæring og kompetanseutvikling innen informasjonssikkerhet og personvern. Fremstillingen bygger på styrende dokumenter, rolle- og ansvarsbeskrivelser, rutiner og retningslinjer, årsrapporten for 2025 og intervjuer med ledere og nøkkelpersoner i sentrale funksjoner og utvalgte tjenesteområder.

Først beskrives ansvar og generelle tiltak for opplæringen. Deretter omtales informasjon og opplæring for ansatte som behandler elevdata, pasientdata og personaldata. Til slutt beskrives opplysningene om dokumentasjon av gjennomførte tiltak.

4.3.1 Opplæring om sikker bruk og behandling av personopplysninger

Ansvar og rammer for opplæringen

Informasjonssikkerhetsstrategien fastsetter kompetanse som et prinsipp i fylkeskommunens arbeid med informasjonssikkerhet. Strategien angir at ansatte skal ha kunnskap om fylkeskommunens arbeid med informasjonssikkerhet og personvern, relevante lover og retningslinjer, og at de skal følge disse.

Fylkeskommunens overordnede ansvarsfordeling for informasjonssikkerhet og personvern er beskrevet i kapittel 2. Dokumentet organisering roller og ansvar – informasjonssikkerhet fastsetter at ledere med personalansvar skal sørge for at ansatte har nødvendig sikkerhetsforståelse og kunnskap. Informasjonssikkerhetskoordinator skal gi råd til enhetene, mens personvernombudet skal informere, gi råd og bistå i opplæringen.

Forvaltningsmodell for informasjonssystemer i TRFK legger brukerstøtte og opplæring inn i systemforvaltningen. Systemansvarlig skal planlegge brukerstøtte og opplæring ved planlegging og implementering av systemer, og ha ansvar for eller koordinere brukerstøtten i produksjonsfasen. Retningslinje – Nytt informasjonssystem krever at nødvendig kompetanse kartlegges og relevante ressurspersoner involveres tidlig ved innføring eller endring av systemer.

Enkelte informanter beskriver at ansvar for rammeverk og veiledning er samlet sentralt, mens utføringen ligger i linjen. Andre beskriver koordinerende roller som samarbeider med ressurser innen informasjonssikkerhet, personvern og IKT- sikkerhet, mens det faglige arbeidet utføres av de respektive fagmiljøene.

Krav og veiledning om sikker bruk

IKT-reglementet 2023 gjelder alle med brukerkonto og tilgang til fylkeskommunens IKT-tjenester. Brukerne må akseptere reglementet og gi digital bekreftelse på at de har lest og forstått det. Bekreftelsen skal gjentas dersom reglementet endres. Reglementet beskriver personlig ansvar for brukerkonto og passord, varsling av forhold som kan ha betydning for sikkerheten til seksjon IKT eller IKT ved skolen, og varsling om brudd på personvern til nærmeste leder, kontaktlærer eller personvernombud.

Retningslinje – Klassifisering av informasjon beskriver hvordan informasjon skal klassifiseres, lagres og deles. Dokumentet omfatter informasjonsklasser, bruk av etiketter i Microsoft 365 og prinsipper for tilgangsstyring og tjenstlige behov. Veilederen skal hjelpe ansatte til å ta riktige valg for lagring og deling av ustrukturert informasjon.

Retningslinje for bruk av kunstig intelligens setter minimumskrav til ansattes bruk av generativ KI: Ansatte skal ikke dele personopplysninger om ansatte, elever eller innbyggere, taushetsbelagt informasjon, gradert informasjon, informasjon unntatt offentlighet eller påloggingsinformasjon i slike løsninger. Ledere har ansvar for opplæring, for at ansatte har nødvendig kompetanse til å bruke generativ KI forsvarlig og effektivt, og for at retningslinjene er kjent blant ansatte.

Gjennomførte opplærings- og informasjonstiltak

I årsrapporten for 2025 beskriver fylkeskommunen målrettet opplæring, temamøter for nye ledere og tilbud om kurs til aktuelle seksjoner og skoler. Årsrapporten omtaler også jevnlige webinarer for å gjøre strategier og reglement kjent, samt fagnettverk der aktuelle temaer tas opp og relevante målgrupper får opplæring.

Flere informanter beskriver at fylkeskommunen gjennomfører opplærings- og informasjonstiltak både for hele organisasjonen og for bestemte målgrupper. Nanolæring[14] og phishingkampanjer[15] har vært gjennomført over flere år, blant annet med opplæring om risiko ved bruk av digitale tjenester og øvelser der ansatte mottar simulerte phishingforsøk. Informasjonssikkerhetskoordinator og seksjonsleder organisasjon opplyser at tiltakene er satt på pause i 2026 som følge av innføring av nytt kvalitetssystem og ERP-system, for å unngå opplæringstretthet. Seksjon organisasjon og seksjon IKT har samarbeidet om gjennomføringen, og informasjonssikkerhetsgruppen har gjennomgått materialet før utsending.

Informasjonssikkerhetskoordinator opplyser at fylkeskommunen gjennomfører årlige aktiviteter i forbindelse med sikkerhetsmåneden i oktober. Tiltakene omfatter blant annet fagartikler, beskrivelser av sikkerhetshendelser og digitale kurs, som formidles gjennom intranettet. Fylkesdirektøren bidrar til å synliggjøre kampanjen gjennom intranett og allmøter. Fylkestannlegen opplyser at sikkerhetsmåneden også omfatter e-læringskurs for ansatte.

Opplæring i informasjonssikkerhet og personvern inngår videre i introduksjonen av nye ledere. Informasjonssikkerhetskoordinator opplyser at HR organiserer tematimer for nye ledere, og at hun også bidrar med opplæring i seksjonsmøter og avdelingssamlinger. Seksjonsleder

[14] Nanolæring er korte, digitale opplæringsøkter som tar for seg et avgrenset tema om gangen.

[15] Phishing er digital svindel der noen forsøker å få mottakeren til å oppgi opplysninger, åpne skadelige lenker eller utføre handlinger gjennom falske meldinger.

organisasjon opplyser at nye seksjonsledere og rektorer har et eget opplæringsopplegg, mens noe informasjon inngår i det digitale opplæringsopplegget for øvrige nyansatte.

Seksjonsleder organisasjon og direktør for organisasjon og økonomi beskriver et gjennomført tretimers kurs for fylkesdirektørens ledergruppe. Kurset ble holdt av KINS (forening for kommunal informasjonssikkerhet)[16] og tok utgangspunkt i fylkeskommunens dokumentasjon og ISO-standard. Opplæringen omfattet styring og ledelse av informasjonssikkerhet, regelverk, styringssystem og NIS2[17]. Direktøren opplyser at deltakerne skulle formidle innholdet videre til sine avdelinger. Seksjonsleder organisasjon opplyser at det planlegges videre opplæring i organisasjonen.

Flere fagmiljøer beskriver også egne opplærings- og veiledningstiltak. Arkivseksjonen gir saksbehandlere veiledning om sikker lagring og deling av informasjon, blant annet i arkivsystemet, filområder og Teams. Personvernombudet opplyser at hun gir opplæring og holder foredrag om personvern etter forespørsel og ved behov.

Informasjonssikkerhet har også vært tema på samlinger for IKT-ansatte sentralt og ved skolene. IKT-sikkerhetskoordinatoren beskriver opplæring om personvernregelverket, sikkerhetsprodukter og tilgangsstyring, samt foredrag om sikkerhet knyttet til OT-utstyr[18]. Seksjonsleder IKT opplyser at sikkerhet tas opp i seksjonsmøter og samlinger, og at seksjonen gir støtte og veiledning til organisasjonen.

Gjennomføring, opplæringsbehov og formidling

Leder for kvalitet og internkontroll opplyser at opplæring og sikkerhetskultur er et eget punkt i kvalitetssystemet. Det finnes bevisstgjøringskampanjer og sikkerhetskurs for ansatte, men hun viser samtidig til lav respons på kursene. Hun vurderer at lederne må ha ansvar for at ansatte gjennomfører dem.

Seniorrådgiver digitalisering opplyser at få gjennomfører nanolæringen. Fylkestannlegen anslår at om lag 50 til 60 prosent gjennomfører e-læringskurset i sikkerhetsmåneden.

Informasjonssikkerhetskoordinator opplyser at ledere oppfordres til å snakke om kompetansebehov i medarbeidersamtaler. Hun beskriver en kontinuerlig vurdering av ansattes

[16] https://www.kins.no/om-oss/

[17] https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/

[18] OT (Operational Technology) er teknologi som brukes til å styre eller overvåke fysiske prosesser og utstyr)

opplæringsbehov. Seksjonsleder organisasjon opplyser at seksjonen gir opplæring og bistand i risikovurderinger, mens ansvaret ligger i linjen.

Seksjonsleder kommunikasjon opplyser at rutiner er tilgjengelige på intranettet, men at ansatte som omfattes av regelverket ikke alltid vet at rutinene finnes og derfor ikke nødvendigvis oppsøker dem. Seksjonsleder jus og anskaffelser beskriver også forbedringsbehov i den interne informasjonsflyten. Personvernombudet opplyser at det ikke er lett å finne personvernrutiner i organisasjonen. Informantene viser til nytt intranett og nye systemer som tiltak som skal gjøre informasjon lettere tilgjengelig.

Opplysninger om obligatorisk opplæring og videre tiltak

Informantene gir ulike beskrivelser av obligatorisk opplæring. Informasjonssikkerhetskoordinator opplyser at det ikke finnes obligatorisk opplæring for nyansatte utover kravet om å lese og forstå IKT-reglementet. Nærmeste leder har ansvar for at ansatte har nødvendig kompetanse til å utføre arbeidet. Seksjonsleder arkiv opplyser at det mangler obligatorisk opplæring i informasjonssikkerhet og personvern, også for nyansatte. Seniorrådgiver digitalisering opplyser at nyansatte ikke får særskilt opplæring på disse områdene.

Direktør for organisasjon og økonomi opplyser derimot at opplæring i informasjonssikkerhet er obligatorisk, og viser særlig til kurs for nye ledere. Hun beskriver også at det utvikles nye kompetansehevende kurs som skal prøves ut i egen avdeling før de tas i bruk i organisasjonen. Informasjonssikkerhetskoordinator opplyser at det arbeides med en kompetanseportal som skal omfatte både eksisterende og nyansatte. Seksjonsleder jus og anskaffelser opplyser at det finnes kurs alle ansatte plikter å gjennomføre, og at informasjonssikkerhet inngår i obligatorisk opplæring av nyansatte.

4.3.2 Informasjon og opplæring ved behandling av elevdata, pasientdata og personaldata

Ansvar og felles rammer

Dokumentet organisering roller og ansvar – informasjonssikkerhet beskriver at systemeier skal sørge for rutiner for informasjonssikkerhet og personvern i egne systemer. Ledere skal sørge for sikkerhetsforståelse og kunnskap hos ansatte. Ansvar for brukerstøtte og opplæring inngår også i forvaltningsmodellen for informasjonssikkerhet.

Personvernombudet opplyser at det er gitt opplæring eller informasjon i aktuelle seksjoner om elevdata og personaldata. Hun beskriver at enkelte ansatte kjenner behandlingen av

personopplysninger godt, fordi de har involvert personvernombudet eller fordi leder har gitt opplæring. Andre kommer mer sporadisk borti personvernspørsmål og kan etter hennes beskrivelse oppleve å få et stort ansvar uten tilsvarende kompetanse.

Elevdata

Seksjonsleder eksamen og støttetjenester forteller at ansatte i hans område har fått opplæring i flere omganger. Alle nyansatte får innføring, og ansatte som arbeider med systemer, får opplæring av ansatte med erfaring fra systemene. Ved behov deles informasjon og det gis internopplæring, blant annet når det kommer forslag til nye rutiner.

Han opplyser videre at avdelingen har en personverngruppe som arbeider på tvers av sentraladministrasjonen og tilbyr bistand til skolene, blant annet ved anskaffelser og utarbeidelse av interne rutiner. Seksjonslederen vurderer at flere skoler burde benytte seg av gruppen, og at behovet for opplæring er større enn skolene selv oppfatter.

Personvernombudet viser til spørsmål fra skoler om bruk av apper og filming av elever. Hun opplyser at IKT har laget en egen rutine for nye apper som skal tas i bruk. Hun beskriver også at lærere kan bli presentert for apper på seminarer uten at det alltid tenkes gjennom om løsningene kan brukes. Hun peker i denne sammenhengen på mangler i opplæringen av ansatte.

Retningslinje – strømming av arrangement gjelder avdeling kompetanse og har som hovedregel at arrangementer med elever ikke skal strømmes. Ved eventuell strømming beskriver dokumentet krav om vurdering etter personvernregelverket, utnevning av behandlingsansvarlig, risikovurdering, samtykke og informasjon ved inngangene. Risikovurderingen skal drøftes med personvernombudet før strømming.

Pasientdata

Fylkestannlegen opplyser at tannhelsetjenesten har et årshjul der taushetsplikt, personvern og sikker behandling av opplysninger skal gjennomgås minst en gang i året. Alle ansatte skal gjennomgå dette ved oppstart og signere taushetserklæring. Nærmeste leder skal gjennomgå hvordan den ansatte skal håndtere personopplysninger i sin stilling. Ansatte får også informasjon om praktisk håndtering, blant annet telefonbruk og bekreftelse av identitet.

Fylkestannlegen opplyser samtidig at tjenesten ikke har en god rutine for å fange opp behov for ytterligere veiledning eller opplæring. Behov kan bli synlig dersom det viser seg at noen har mangler, og det settes da inn tiltak.

Personaldata

Seksjonsleder organisasjon opplyser at seksjonen håndterer taushetsbelagt informasjon og personopplysninger i lønnssystemet og i personalsaker. Ansatte har fått opplæring i hva det innebærer og håndterer slike opplysninger. Informasjonssikkerhet er også tatt opp med tillitsvalgte og i lederforum.

Seksjonsleder viser til opplæring for nye seksjonsledere og rektorer, og til at noe informasjon inngår i et digitalt opplæringsopplegg for øvrige ansatte.

4.3.3 Dokumentasjon av opplærings- og informasjonstiltak

IKT-reglementet fastsetter at brukere skal gi digital bekreftelse på at de har lest og forstått reglementet. Bekreftelsen skal gjentas dersom reglementet endres.

De øvrige gjennomgåtte styrende dokumentene beskriver i hovedsak krav, ansvar og veiledning. Retningslinjer for bruk av kunstig intelligens plasserer ansvaret for opplæring og kjennskap hos lederne, men beskriver ikke registrering av gjennomført opplæring.

I årsrapporten for 2025 beskriver fylkeskommunen at arbeidet med å styrke informasjonssikkerhet og personvern har omfattet målrettet opplæring, temamøter for nye ledere og tilbud om kurs til aktuelle seksjoner og skoler. Årsrapporten omtaler også jevnlige webinarer for å gjøre strategier og reglement kjent, samt fagnettverk der aktuelle temaer tas opp og relevante målgrupper får opplæring.

Direktør for organisasjon og økonomi opplyser at digital opplæring dokumenteres. Hun er usikker på om eksterne kurs registreres, og opplyser at den ansatte i så fall selv må registrere deltakelsen. Leder for kvalitet og internkontroll opplyser at fylkeskommunen har oversikt over hvem som har gjennomført kurs, men ikke en samlet oversikt over ansattes kompetanse innen informasjonssikkerhet.

Leder for kvalitet og internkontroll og direktør for organisasjon og økonomi opplyser at intranettet viser antall klikk på saker og rutiner, men ikke hvem som faktisk har lest innholdet. Leder for kvalitet og internkontroll opplyser at det nye kvalitetssystemet kan sende ut leselister og innhente bekreftelse på at dokumenter er lest.

4.4 Vurdering

Fylkeskommunen sikrer i hovedsak at ansatte og andre brukere som får tilgang til digitale systemer og personopplysninger, får nødvendig opplæring om sikker bruk, konfidensialitet, tilgangsstyring, avvikshåndtering og behandling av personopplysninger

Revisor vurderer at fylkeskommunen har etablert relevante ordninger for informasjon og opplæring innen informasjonssikkerhet og personvern. Fylkeskommunen har gjennomført flere opplærings- og informasjonstiltak, både for ansatte generelt og for bestemte målgrupper. Opplæringen omfatter også tiltak tilpasset tjenesteområder, arbeidsoppgaver og informasjonssystemer. Den sektorvise opplæringen og veiledningen bidrar dermed til å dekke opplæringsbehov utover de felles tiltakene. Det er også etablert krav om at brukerne skal bekrefte at de har lest og forstått IKT-reglementet.

Flere informanter beskriver samtidig lav deltakelse i enkelte fellestiltak og varierende kjennskap til rutiner. Det beskrives også mangler i opplæringen på enkelte områder, særlig ved skolene. Etter revisors vurdering bør fylkeskommunen derfor styrke oppfølgingen av gjennomføring og formidling, slik at ansatte får nødvendig informasjon og opplæring gjennom felles tiltak eller tiltak i det enkelte tjenesteområdet.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen sikrer i hovedsak at ansatte som behandler elevdata, pasientdata eller personaldata får nødvendig informasjon og opplæring om relevante krav i regelverk og interne rutiner.

Revisor vurderer at fylkeskommunen har etablert relevante ordninger for informasjon og opplæring til ansatte som behandler elevdata, pasientdata og personaldata. Innen eksamen og støttetjenester beskrives opplæring ved oppstart, systemopplæring og løpende internopplæring. Tannhelsetjenesten har ordninger for gjennomgang av taushetsplikt, personvern og sikker behandling av opplysninger ved oppstart og årlig. Innen seksjon organisasjon opplyses det at ansatte har fått opplæring i håndtering av personopplysninger og taushetsbelagt informasjon.

Funnene viser samtidig svakheter i oppfølgingen av opplæringsbehov. På skoleområdet beskrives mangler i opplæringen, blant annet knyttet til bruk av apper og behandling av elevopplysninger. Tannhelsetjenesten mangler en god rutine for å fange opp behov for ytterligere veiledning og opplæring. Etter revisors vurdering gir dette risiko for at ansatte ikke får tilstrekkelig opplæring tilpasset oppgavene sine.

Samlet vurderer revisor at de beskrevne ordningene i hovedsak ivaretar behovet for informasjon og opplæring på de undersøkte områdene. Fylkeskommunen bør likevel styrke arbeidet med å identifisere og følge opp udekkede opplæringsbehov, særlig ved skolene og i tannhelsetjenesten.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen dokumenterer i hovedsak gjennomførte opplærings- og informasjonstiltak i det omfanget som er nødvendig for å kunne følge opp internkontrollen.

Revisor vurderer at fylkeskommunen i hovedsak dokumenterer gjennomførte opplærings- og informasjonstiltak i det omfanget som er nødvendig for å følge opp internkontrollen. Intervjuopplysningene viser at digital opplæring dokumenteres, og at fylkeskommunen har oversikter over hvem som har gjennomført kurs. Årsrapporten beskriver også gjennomførte tiltak på overordnet nivå. Dette gir et grunnlag for å følge opp gjennomføringen av opplæringen.

Revisjonen har ikke gjennomgått oversiktene over kursdeltakelse, og datagrunnlaget gir begrenset informasjon om dokumentasjonen av lokal opplæring og eksterne kurs. Vurderingen bygger derfor på intervjuopplysningene om registrering og oversikter, sammenholdt med dokumenterte krav og rapportering om gjennomførte tiltak.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

5 TILGANGSSTYRING

Dette kapitlet omhandler tilgangsstyring.

5.1 Delproblemstilling

Det er utarbeidet følgende delproblemstilling for temaet tilgangsstyring:

- Har fylkeskommunen rutiner og ordninger for tilgangsstyring som ivaretar tjenstlig behov og nødvendig logging og oppfølging?

5.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne delproblemstillingen:

- Fylkeskommunen skal ha rutiner for tilgangsstyring i digitale systemer som behandler eller gir tilgang til personopplysninger og annen beskyttelsesverdig informasjon.
- Fylkeskommunen skal sikre at tilganger tildeles på bakgrunn av tjenstlig behov.
- Fylkeskommunen skal ha rutiner for logging og oppfølging av tilgang der dette er nødvendig for å avdekke eller følge opp urettmessig tilgang, eller følger av særskilt regelverk.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

5.3 Funn

Dette kapitlet beskriver rutiner, ansvar og praksis for tilgangsstyring, samt logging og oppfølging av tilganger. Fremstillingen bygger på styrende dokumenter om systemforvaltning, klassifisering, autentisering og IKT-bruk, og intervjuer med sentrale funksjoner og utvalgte tjenesteområder. Opplysninger om praksis bygger på informantenes beskrivelser.

I kapitlet brukes enkelte begreper om pålogging og tilgangsstyring. Autentisering betyr å kontrollere brukerens identitet, mens tilgangsstyring gjelder hvilke systemer, opplysninger og funksjoner brukeren får tilgang til. Felles pålogging, også omtalt som SSO, gjør det mulig å bruke samme pålogging til flere tjenester. Flerfaktorautentisering, omtalt som MFA, innebærer at brukeren må bekrefte identiteten med mer enn en faktor. En administrator eller superbruker har utvidede rettigheter, men hvilke oppgaver og tilganger disse rollene omfatter, varierer mellom systemene.

5.3.1 Rutiner og ansvar for tilgangsstyring

Skriftlige rammer og rutiner

Fylkeskommunens overordnede roller og ansvar for informasjonssikkerhet er beskrevet i kapittel 2. For tilgangsstyring legger de styrende dokumentene ansvar til systemforvaltningen. Systemeier skal sørge for nødvendige rutiner for informasjonssikkerhet og personvern, mens systemansvarlig skal etablere rutiner for tilgangsstyring. Ved innføring eller endring av informasjonssystemer skal ansvarlige roller avklares og dokumenteres.

Mal og veileder forenklet ROS av informasjonssystem angir at systemet skal ha systemeier og systemansvarlig ved ansvarlig skole eller enhet. Systemeier skal vurdere sikkerheten i autentiseringsløsningene og behovet for sterk autentisering ut fra risiko og hvilke opplysninger systemet behandler.

IKT-reglementet 2023 fastsetter at brukerkontoer er personlige. Brukere skal ikke dele passord eller skaffe seg tilgang ved hjelp av en annen brukerkonto. Brukertilgangen til fylkeskommunens IKT- tjenester skal stenges når ansettelse eller elevstatus opphører. Brukerkontoen skal deaktiveres på sluttdato for ansatte eller i august for avgangselever. Reglementet beskriver også brukerens ansvar for å rydde i personlige data og overføre fylkeskommunens informasjon til riktig fagsystem eller nærmeste leder før kontoen stenges. E-post og personlige filområder skal slettes etter tre måneder.

Retningslinje for autentisering gjelder autentisering i fylkeskommunens infrastruktur og hos leverandører av tjenester og programvare. Dokumentet beskriver felles pålogging og bruk av Azure AD[19], samt krav om flerfaktorautentisering for alle ansatte. Kravene styres blant annet ut fra hvor brukeren logger på og brukerens risikonivå. Dokumentet omtaler også utprøving av autentisering som er mer motstandsdyktig mot phishing, for kontoer med tilgang til mer data enn normalt.

Ansvar i praksis

Seksjonsleder for IKT opplyser at systemeierne har administratorer og superbrukere for sine systemer. IKT har administratortilganger til sentrale systemer som er organisert under IKT. Han opplyser at lederne i seksjonen avgjør hvilke tilganger ansatte skal ha, fordi lederne skal ha oversikt over de tjenstlige behovene,

[19] Azure Active Directory (AD), nå Microsoft Entra ID, er Microsofts løsning for identitets- og tilgangsstyring.

Informasjonssikkerhetskoordinator opplyser at hun ikke har ansvar for tilgangsstyring. Hun beskriver at fylkeskommunen bruker opplysninger fra HR-systemet som grunnlag for automatisk opprettelse av tilganger i kjernesystemene.

Seksjonsleder organisasjon opplyser at systemeier, systemansvarlig, forvalter og superbrukere er beskrevne roller. Systemansvarlig kjenner systemet og tildeler roller. Seksjonsleder eksamen og støttetjenester opplyser at seksjonen er systemeier for felles applikasjoner i skolesektoren, og at systemadministrator ivaretar operativ tildeling og oppfølging av tilganger. Dersom en skole tar i bruk en løsning utenfor felles anskaffelser, skal skolen selv ivareta systemeieransvaret og nødvendige sikkerhetsvurderinger før løsningen tas i bruk.

Seksjonsleder arkiv opplyser at arkivseksjonen er systemeier for sak- og arkivsystemet Public 360 og har ansvar og eierskap for Acos Interact. Administratorene for sak- og arkivsystemet sitter i arkivseksjonen.

Fylkestannlegen opplyser at han er systemeier for journalsystemet Opus Dental. Tannhelsetjenesten har administrator og superbrukere som ivaretar praktisk administrering, herunder tilganger og brukerroller. Han opplyser samtidig at det ikke er godt nok dokumentert hvem som har hvilke roller og ansvar knyttet til systemet. Oppgavene er kjent internt, men han mener at ansvarsfordelingen må beskrives bedre. Tannhelsetjenesten samarbeider med IKT og har en kontaktperson der som bistår tjenesten.

5.3.2 Tildeling, endring og avslutning av tilganger ut fra tjenstlig behov

Automatisert tilgangsstyring og felles pålogging

Flere informanter beskriver at opplysninger om ansatte og roller i HR-systemet benyttes som grunnlag for automatisk opprettelse av tilganger i sentrale systemer. Enkelte tilganger tildeles automatisk ut fra rolle og bortfaller når rollen opphører, mens andre må tildeles og fjernes manuelt. For ERP-systemet beskrives det at ledere søker om tilganger, og at behovet vurderes før tilgang tildeles. Tjenesteområdene og seksjonen spiller inn behov for tilganger i delsystemer og løsninger de har ansvar for.

Seksjonsleder IKT opplyser at det tidligere systemlandskapet hadde mange spredte løsninger for brukere og tilganger. Med innføringen av nytt ERP-system skal mer samles på et sted. Målet er å knytte mest mulig av tilgangsstyringen til den sentrale løsningen, slik at brukere avsluttes i relevante systemer når arbeidsforhold eller tilganger opphører. Han viser samtidig til sårbarheter der systemer ikke er koblet til den sentrale løsningen og det må opprettes egne

brukere. Det arbeides med mer automatisering. Han opplyser også at det skal gjennomføres årlige gjennomganger av tilganger.

Seniorrådgiver digitalisering opplyser at kompetansesektoren bruker Feide, en nasjonal tjeneste for felles pålogging. Gjennom Feide kan de se hvilke tjenester som er aktivert. Fylkeskommunen har også en felles identitetsløsning som gir oversikt over brukertilganger. Han beskriver samtidig at det ikke finnes en samlet og fullstendig oversikt over alle løsninger, og at arbeidet med registrering i Samsvar fortsatt pågår. Han opplyser videre at han har administratorrettigheter i Feide og kan godkjenne nye tjenester. Han beskriver gruppebasert tilgangsstyring, for eksempel for elever eller ansatte ved en bestemt skole. Tilgangene er automatiserte, slik at en bruker som slutter ved én enhet og begynner ved en annen, mister tilgangene knyttet til den tidligere enheten.

Administratortilganger IKT

Seksjonsleder IKT opplyser at ansatte i IKT ikke har alle administratortilganger tilgjengelige hele tiden. Tilganger fordeles når det er behov. IKT-sikkerhetskoordinator beskriver en tilgangsstyringsmodell der ansatte får de administratortilgangene de trenger når de arbeider med det aktuelle området, for eksempel enheter, e-post eller Teams.

IKT-sikkerhetskoordinator opplyser at han godkjenner midlertidig utvidelse av tilganger innenfor sitt ansvarsområde. Den som har ansvar for en administratorrolle, skal vurdere kompetansen og forståelsen av ansvar hos den som får rollen. Han opplyser at dette er hovedpraksis, men at ordningen ikke fungerer fullt ut for alle roller. Han forvalter tilgangsstyringsmodellen sammen med to andre ansatte i IKT.

Bestilling, tildeling, endring og avslutning av tilganger i IKT-seksjonen skjer etter koordinatorens opplysninger manuelt. Ved nyansettelser vurderes tilganger ut fra arbeidsoppgaver og behov, og tilgangene justeres ved behov underveis. Tilganger avsluttes når ansatte slutter. Kontoer deaktiveres før de senere slettes automatisk.

IKT- sikkerhetskoordinatoren opplyser at enkelte manuelt opprettede tilganger for ansatte i IKT kan bli liggende igjen en periode mens de undersøker hvor det finnes spor og tilganger. Han presiserer at deaktiverte tilganger ikke er brukbare. Det ryddes fortløpende. Seksjonen har forsøkt å ha en revisjonsmåned i september for gjennomgang av faste kontrollpunkter, men kapasitet gjør dette krevende. Mye av oppfølgingen skjer derfor fortløpende.

Skoleområdet

Seksjonsleder eksamen og støttetjenester opplyser at ansatte skal ha tilgang til informasjon de har et fast tjenstlig behov for. Dersom behovet bare oppstår et fåtall ganger, skal opplysninger heller gjøres tilgjengelige ved behov. Han opplyser at fem ansatte har tilgang til alt i det skoleadministrative systemet fordi de utfører supportoppgaver. Det finnes også superbrukere på de store programmene som tilbys. Videre beskriver han at noen tilganger fjernes automatisk når arbeidsforhold avsluttes, mens andre må fjernes manuelt. Informasjon om ansatte som slutter, når ikke alltid frem til dem som administrerer tilganger. Slike forhold kan bli oppdaget når det bestilles tilganger til nyansatte.

Videre beskriver han at endringsbehov kan fanges opp gjennom tilbakemeldinger fra skolene eller ved at seksjonen selv ser behov for nye rutiner eller innstramminger. Han beskriver at rutiner internt i seksjonen følges godt, men at han ikke har mulighet til å kontrollere fullt ut hva som foregår på skolene.

Sak- og arkivsystem

Seksjonsleder arkiv opplyser at alt som arkiveres, vurderes med hensyn til tilgangsstyring. Prinsippet er tjenstlig behov og minst mulig tilgang. Tilgangsmodellen omfatter generelle brukergrupper, enhetsvise grupper, ledergrupper og egne grupper for sensitive personopplysninger. Det finnes også en løsning der bare den som registrerer en sak eller et dokument, har tilgang inntil andre eventuelt legges til.

Enkelte rettigheter har sluttdato. Arkivseksjonen mottar oversikter fra IKT ved endringer, omtalt som BAS-oversikter[20], for å kontrollere om tilganger i sak- og arkivsystemet må justeres. Seksjonsleder opplyser at endringer i arbeidsforhold også kan bli oppdaget på andre måter.

Tannhelsetjenesten

Fylkestannlegen opplyser at journalsystemet har et hierarki for tilganger og oversikt over hvem som har tilgang til hva. Administrator har ansvar for å tildele, endre og avslutte tilganger. Superbrukere kan gi tilganger og avslutte roller, men kan ikke endre egenskapene til tilgangene eller rollene.

Det finnes rutiner for tilgang til særskilte pasientjournaler. I hovedsak er det to til tre ansatte som har tilgang til å åpne slike journaler. Administrator har tilgang til alt til enhver tid.

[20] BAS-oversikter brukes her om oversikter fra IKT over brukere eller endringer i brukertilganger som benyttes ved kontroll av tilganger i sak- og arkivsystemet.

Fylkestannlegen beskriver at røntgensystemet har andre tilgangsmuligheter enn journalsystemet. Journalnummer, navn og bilder av tenner ligger tilgjengelig for ansatte i tannhelsetjenesten. Han opplyser at det ikke er mulig å sperre tilgangen i røntgensystemet, og at han ikke kjenner til alternativer per intervjutidspunktet.

Personaldata og andre lokalt forvaltede systemer

Seksjonsleder organisasjon opplyser at tilgangene til lønnssystemet er begrenset. Tilgang til sensitive personopplysninger er i hovedsak lagt til lønnsteamet. Seksjonen behandler også personopplysninger i personalsaker og sykefraværsoppfølging.

Seksjonsleder jus og anskaffelser opplyser at seksjonen har ansvar for tilgangsstyring i noen få systemer, anslagsvis to til tre. Seksjonen har superbrukere, og tilgangsbehov vurderes løpende. Han vurderer rutinene for å opprette og avslutte tilganger som gode.

Direktør for organisasjon og økonomi opplyser at det gjennomføres strenge vurderinger av hvem som skal ha hvilke tilganger, og at det er gjennomført risiko- og sårbarhetsanalyser knyttet til tilganger.

Seksjonsleder kommunikasjon opplyser at nettredaktøren har det operative ansvaret for å gi tilganger til fylkeskommunens nettsider. Han vurderer at for mange har tilgang, og opplyser at det arbeides med å redusere antallet redaktører. Dette må samtidig balanseres mot behovet for drift. Tilganger skal beskrives i seksjonens innholdsstrategi.

5.3.3 Logging og oppfølging av tilganger

Skriftlige krav og ansvar

Retningslinje – Klassifisering av informasjon stiller krav om sporing av tilgang til informasjon i klassene «Beskyttet» og «Strengt beskyttet». Forvaltningsmodell for informasjonssystemer i TRFK legger det overordnede ansvaret for informasjonssikkerhet og personvern til systemeier. Systemdrift har ansvar for teknisk sikkerhet, systemovervåkning og overvåkning og håndtering av sikkerhetshendelser. Overvåkningen skal tilpasses systemets kritikalitet.

Retningslinje – Nytt informasjonssystem krever at risikovurderinger avdekker behov for tekniske og organisatoriske sikkerhetstiltak, og at sikkerhetskrav inngår i kravspesifikasjoner og anskaffelser. Vurderingene skal også omfatte behandling av personopplysninger som oppstår gjennom tilgangsstyring og bruk av tjenester.

Logging og oppfølging i IKT

IKT-sikkerhetskoordinator opplyser at gjennomgang av logger og stikkprøver i hovedsak skjer på bakgrunn av hendelser. Hendelser kan avdekke tilganger som ikke skal være der, og disse forholdene følges opp. Han beskriver at sikkerhetsarbeidet også avdekker andre forhold som krever tiltak.

Koordinatoren opplyser at passord på avveie utløser alarmer og automatisk blokkering. Slike forhold fremgår av logger som analyseres og følges opp. Han opplyser samtidig at de ikke har overvåkning rettet mot innsiderisiko. Arbeidet med klassifisering av informasjon kan etter hans beskrivelse gi muligheter for alarmer om for eksempel omfattende nedlasting eller utsending av informasjon. Dette omtales som muligheter i det videre arbeidet.

Seksjonsleder IKT opplyser at sikkerhetsansvarlige har tilgang til logger, blant annet brannmurlogger. Han beskriver store loggmengder og behov for verktøy som kan bidra til å finne relevante forhold. Han opplyser også at det ikke gjennomføres særskilt kontroll av IKT-seksjonen på dette området.

Logging i sak- og arkivsystemet

Seksjonsleder arkiv opplyser at bruk av administratorrollen i sak- og arkivsystemet loggføres. Hun anslår at om lag fire personer har administratorrolle, og opplyser at to personer gjør endringer i administrasjonsdelen.

Seksjonsleder organisasjon opplyser at all aktivitet i lønnssystemet loggføres. Hun beskriver at loggene kan gjøre det mulig å oppdage bruk uten tjenstlig behov.

Flere informanter opplyser at det ikke gjennomføres rutinemessige stikkprøver eller systematisk kontroll av logger i systemene de har ansvar for. Disse opplysningene beskriver oppfølgingen i de aktuelle systemene, mens IKT-sikkerhetskoordinatoren beskriver hendelsesbasert gjennomgang og oppfølging av tekniske alarmer.

Kontroll av journaloppslag i tannhelsetjenesten

Fylkestannlegen opplyser at oppslag i pasientjournaler loggføres. Det tas stikkprøver i loggene av og til, men det finnes ikke en rutine for hvor ofte kontrollene skal gjennomføres. Han beskriver også at det er vanskelig å vite hvem kontrollene skal rettes mot.

Kontrollene gjennomføres av fylkestannlegen eller administrator, og bare disse har tilgang til kontrollfunksjonen. Det er mulig å undersøke hvem som har gjort oppslag i en pasients journal uten å åpne selve journalen. Fylkestannlegen viser som eksempel til at det kan undersøkes om det er gjort urettmessige oppslag i journalene til kjente personer. Han opplyser at det ikke

er oppdaget avvik gjennom slike kontroller, og vurderer at det ikke er grunn til å tro at ansatte misbruker tilgangene sine.

5.4 Vurdering

Fylkeskommunen har i hovedsak rutiner for tilgangsstyring i digitale systemer som behandler eller gir tilgang til personopplysninger og annen beskyttelsesverdig informasjon.

Revisor vurderer at fylkeskommunen har etablert skriftlige rammer og rutiner for tilgangsstyring. Dokumentene angir ansvar i systemforvaltningen, tjenstlig behov som prinsipp, krav til autentisering og avslutning av brukerkontoer. Beskrivelsene av praksis understøtter at ansvaret ivaretas gjennom ledere og ulike systemroller. Det er samtidig behov for å tydeliggjøre dokumentasjonen av den praktiske ansvarsfordelingen i deler av systemforvaltningen.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen sikrer i hovedsak at tilganger tildeles på bakgrunn av tjenstlig behov.

Revisor vurderer at fylkeskommunens ordninger og beskrevne praksis i hovedsak ivaretar tjenstlig behov ved tildeling av tilganger. Lederes behovsvurderinger, rolle- og gruppebasert tilgangsstyring og begrensning av administratortilganger bidrar til dette.

Det er samtidig svakheter i oppfølgingen av manuelt administrerte tilganger og i muligheten til å begrense tilgang i enkelte systemer. Revisor vurderer at disse forholdene viser behov for å styrke oppfølgingen av tilganger, slik at de fortsatt er i samsvar med tjenstlig behov ved endringer i arbeidsoppgaver eller avslutning av arbeidsforhold.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen har delvis rutiner for logging og oppfølging av tilgang der dette er nødvendig for å avdekke eller følge opp urettmessig tilgang, eller følger av særskilt regelverk.

Revisor vurderer at fylkeskommunen har etablert krav om sporing og ansvar for overvåkning. Logger brukes til å avdekke og følge opp sikkerhetshendelser og til å kontrollere tilganger.

Funnene viser samtidig at deler av oppfølgingen er lite systematisert. Etter revisors vurdering bør rutinene tydeliggjøre hvordan og når tilgangslogger skal kontrolleres, ut fra risikoen for urettmessig tilgang. Dette vil gi et mer systematisk grunnlag for oppfølging der slik kontroll er nødvendig.

Revisor vurderer at revisjonskriteriet er **delvis oppfylt.**

6 ETTERLEVELSE AV UTVALGTE PERSONVERNKRAV

Dette kapitlet omhandler etterlevelse av utvalgte personvernkrav innen elev-, pasient- og personalområdet.

6.1 Delproblemstilling

Det er utarbeidet følgende delproblemstilling for temaet etterlevelse av personvernregelverket i tjenesteområdene:

- Etterlever fylkeskommunen utvalgte krav i personvernregelverket ved behandling av pasientdata, elevdata og personaldata?

6.2 Revisjonskriterier

Følgende revisjonskriterier er utledet for denne delproblemstillingen:

- Fylkeskommunen skal ha oversikt over behandling av personopplysninger og dokumentere behandlingsaktivitetene i behandlingsprotokoller i samsvar med personvernregelverket.
- Fylkeskommunen skal gi de registrerte informasjon om hvordan personopplysningene deres behandles.
- Fylkeskommunen skal inngå databehandleravtale når eksterne leverandører behandler personopplysninger på fylkeskommunens vegne.

Utledningen av revisjonskriteriene finnes i vedlegg 1.

6.3 Funn

Dette kapitlet beskriver fylkeskommunens dokumentasjon av behandlinger, informasjon til de registrerte og databehandleravtaler ved behandling av elevdata, pasientdata og personaldata. Datagrunnlaget består av styrende dokumenter, arbeidsdokumenter og maler, publiserte personvernerklæringer, tre databehandleravtaler med bilag og intervjuer med sentrale funksjoner og de undersøkte tjenesteområdene.

Overordnet organisering og styring er omtalt i kapittel 2, opplæring i kapittel 4 og tilgangsstyring i kapittel 5. Her omtales disse forholdene bare der de belyser de tre revisjonskriteriene.

Fremstillingen skiller mellom behandlingsprotokoller, som er fylkeskommunens dokumentasjon av behandlingsaktivitetene, og personvernerklæringer, som informasjon til de registrerte. Opplysninger fra maler og retningslinjer omtales som krav og rammer. Informantenes beskrivelser av protokoller og praksis kommer frem som intervjuopplysninger.

6.3.1 Oversikt over behandlinger og behandlingsprotokoller

Arbeidsdokument – behandlingsprotokoll beskriver at fylkeskommunen som behandlingsansvarlig skal føre protokoll over behandlinger av personopplysninger som utføres under dens ansvar. Behandlingsprotokollene skal registreres i et eget system, og informasjonssikkerhetsgruppen skal bistå ved utarbeidelse og registrering.

Arbeidsdokumentet legger opp til at den enkelte behandlingen skal dokumenteres med blant annet formål, kategorier av de registrerte og personopplysninger, behandlingsgrunnlag, interne brukere, eksterne mottakere, systemer, lagring, sletting og behov for vurdering av personvernkonsekvenser. Elever, lærere, foresatte og andre ansatte inngår som kategorier av registrerte. Opplæringsloven og arbeidsmiljøloven er angitt som mulige lovgrunnlag for aktuelle behandlinger, og lønnsmedarbeidere og HR-personell som mulige interne brukere.

Dokumentet skiller mellom protokoll over behandlingsaktiviteter og oversikt over systemene som brukes i behandlingen. Systemene skal registreres som en del av dokumentasjonen av behandlingen, mens teknisk informasjon skal dokumenteres i en egen systemkatalog.

Retningslinje - Nytt informasjonssystem krever at det ved innføring eller endring av systemer som behandler personopplysninger, kartlegges hvilke opplysninger som behandles, hvem de registrerte er, hvem som er behandlingsansvarlig og hvem som er databehandler. Dokumentet Organisering, roller og ansvar – informasjonssikkerhet legger ansvar til systemeier for at nødvendig dokumentasjon, herunder behandlingsprotokoller, er etablert.

Flere informanter beskriver at ansvaret for behandlingsprotokoller i hovedsak ligger hos ledere og systemeiere, med bistand fra sentrale fagressurser. De beskriver samtidig at det er krevende å etablere fullstendig oversikt over behandlinger og systemer i en stor og geografisk spredt organisasjon.

Registrering og oppfølging i Samsvar

Fylkeskommunen bruker Samsvar til behandlingsprotokoller og oversikt over informasjonssystemer. Flere informanter opplyser at arbeidet med å utvikle en samlet oversikt fortsatt pågår, og at dokumentasjonen ikke er fullstendig på alle områder.

Seksjonsleder arkiv opplyser at arkivseksjonen utarbeider behandlingsprotokoller for arkivsystemene i samarbeid med informasjonssikkerhetskoordinator. Dokumentasjonen for arkivområdet er etablert i Samsvar, men seksjonslederen beskriver uklarheter om ansvaret for å holde protokollene oppdatert.

Behandlingsprotokoll for elevdata

Seksjonsleder eksamen og støttetjenester opplyser at seksjonen har systemeierskap for felles applikasjoner i skolesektoren. Disse omfatter blant annet skoleadministrativt system, system for oppfølging av lærlinger, inntakssystem og læringsplattformer.

Seksjonsleder eksamen og støttetjenester opplyser at det foreligger oppdaterte behandlingsprotokoller for systemene han er systemeier for. Han presiserer at dokumentasjonen i alle fall er på plass for de store systemene. Seksjonslederen har ansvar for oppdatering av protokollene, mens systemansvarlige og systemadministratorer utfører det praktiske arbeidet ved behov.

Behandlingsprotokoller for pasientdata

Fylkestannlegen opplyser at tannhelsetjenesten behandler pasientdata og helseopplysninger, i tillegg til opplysninger om ansatte. Tjenesten bruker Opus Dental som journalsystem.

Han opplyser at tannhelsetjenesten har behandlingsprotokoller for Opus. Protokollene ble utarbeidet i forbindelse med sammenslåingen av fylkene og gjelder etter hans opplysninger alle digitale fagsystemer i tannhelsetjenesten, blant annet tidligere journalsystem og røntgenprogramvare. Fylkestannlegen har ansvar for protokollene, og de er lagret hos IKT.

Opplysninger om personalbehandlinger og kvalitetssystem

Seksjonsleder organisasjon opplyser at seksjonen har eierfunksjon for blant annet lønnsmodul, rekrutteringssystem og HR-system. Hun beskriver at systemene ligger i Samsvar, og at forvaltningsmodellen angir roller som systemeier, systemansvarlig, forvalter og superbruker. Seksjonen behandler personopplysninger og taushetsbelagt informasjon i lønnssystemet, personalsaker og sykefraværsoppfølging.

Leder for kvalitet og internkontroll opplyser at det er utarbeidet behandlingsprotokoll i Samsvar for det nye kvalitetssystemet EQS. Denne opplysningen gjelder kvalitetssystemet, ikke dokumentasjon av lønns-, HR- og personalbehandlinger generelt.

6.3.2 Informasjon til de registrerte

Fylkeskommunen har informasjon om personvern og personvernerklæringer tilgjengelig på nettsidene. Erklæringene beskriver ulike behandlinger innen utdanning, tannhelse og behandlinger som omfatter ansatte. Nedenfor beskrives innholdet i de undersøkte erklæringene.

Informasjon om behandling av elevdata

Personvernerklæringene for elevadministrasjon, digitale læringsplattformer og læremidler samt individuell tilrettelegging og tilpasset opplæring omtaler flere sentrale behandlinger av elevdata. De beskriver blant annet formål, hvilke opplysninger som behandles, behandlingsgrunnlag, kilder, mottakere og lagring og sletting.

Erklæringen for elevadministrasjon angir at formålet er å tilby lovpålagte tjenester knyttet til videregående opplæring. Behandlingen omfatter blant annet inntak, undervisning og fagvalg, eksamen, vurdering, dokumentasjon, veiledning og klagebehandling. Opplysningene omfatter identifikasjons- og kontaktopplysninger, karakterer, vitnemål, fravær, foto, elevmappe og skole- og klasse- og fagtilhørighet. Opplysninger innhentes blant annet fra eleven, kommuner og Kontakt- og reservasjonsregisteret. Lånekassen, Utdanningsdirektoratet, Nasjonal vitnemålsdatabase og Feide er oppført som mottakere.

For digitale læringsplattformer, læringsressurser og pedagogiske programmer angir erklæringene at formålet er å støtte læring, undervisning og vurdering. Opplysningene omfatter blant annet navn, bruker-ID, e-postadresse, IP-adresse, skole- og klassetilhørighet, nettverks- og systemlogger og opplysninger om aktivitet og fremdrift som er nødvendig for tjenestens funksjonalitet. Fylkeskommunen beskriver dette som behandling av en begrenset mengde personopplysninger om elever og ansatte.

Erklæringen om individuell tilrettelegging og tilpasset opplæring angir at opplysninger behandles for å vurdere behov for tilrettelegging og utarbeide individuell opplæringsplan. I tillegg til identifikasjons- og kontaktopplysninger omfattes blant annet informasjon om hjemmeforhold, samtalehistorikk, henvisninger, kartleggingsresultater og pedagogiske rapporter. Opplysninger kan innhentes fra eleven, Folkeregisteret, fylkeskommunen og fastlege eller spesialisthelsetjenesten. BUP (barne- og ungdomspsykiatrisk poliklinikk), spesialisthelsetjenesten og fastlege er oppført som mulige mottakere.

For de omtalte behandlingene opplyser fylkeskommunen at personopplysninger ikke overføres til tredjeland[21], og at lagring skjer hos sky- eller tjenesteleverandører innenfor EU/EØS. For flere behandlinger oppgis det at opplysninger slettes når formålet er oppfylt, senest etter 90 dager, mens arkivpliktige opplysninger arkiveres i samsvar med arkivregelverket. Det opplyses også at det ikke benyttes automatiske avgjørelser.

Informasjon om behandling av pasientdata

Personvernerklæringen for tannhelsetjenesten angir at personopplysninger behandles for å yte tannhelsehjelp, føre pasientjournal og administrere tjenesten. Fylkeskommunen viser til helsepersonelloven, pasientjournalloven og tannhelsetjenesteloven, samt personvernforordningen artikkel 6 nr. 1 bokstav e og artikkel 9 nr. 2 bokstav h som behandlingsgrunnlag.

Tannhelsepasienter, ansatte og pårørende er oppgitt som kategorier av registrerte. Erklæringen angir identifikasjons- og kontaktopplysninger, opplysninger om pårørende, timeavtaler og elektronisk kommunikasjon. Den beskriver ikke nærmere hvilke helseopplysninger som behandles i forbindelse med tannhelsehjelpen og pasientjournalføringen.

Opplysninger kan ifølge erklæringen innhentes fra den registrerte, Folkeregisteret, fylkeskommunen, spesialisthelsetjenesten og henvisende instans. Mulige mottakere omfatter blant annet tilsynsmyndigheter, spesialisthelsetjenesten, Helsedirektoratet, NAV, politiet og barnevernet. For enkelte mottakere er utlevering knyttet til særskilte vilkår. Utlevering til politiet omtales som avhengig av samtykke, rettslig kjennelse eller hjemmel i lov, og utlevering til barnevernet knyttes til helsepersonells opplysningsplikt.

Fylkeskommunen opplyser at personopplysninger ikke overføres til tredjeland. Opplysninger lagres på lokal server eller datasenter og hos sky- eller tjenesteleverandører innenfor EU/EØS. De lagres så lenge det er nødvendig for formålet eller følger av særlover eller forskrifter, mens arkivpliktige opplysninger arkiveres etter arkivregelverket. Det opplyses at det ikke benyttes automatiske avgjørelser.

[21] Tredjeland er i denne sammenheng land utenfor EØS-området

Informasjon om behandling av personaldata

De undersøkte personvernerklæringene som omfatter ansatte, gjelder blant annet digitale kurs, avviksbehandling, tilgangsstyring og autentisering, sikkerhet i IKT-infrastrukturen, adgangskontroll, kameraovervåkning, arkiv og postjournal og bruk av bilder.

Erklæringen for digitale kurs og opplæring angir at opplysninger behandles for å gjennomføre digitale kurs. For ansatte kan dette omfatte navn, bruker-ID, e-postadresse, IP-adresse og aktivitetsdata. Opplysningene innhentes fra den registrerte og fylkeskommunen. Det opplyses at de ikke deles med eksterne mottakere og behandles og lagres innenfor EU/EØS.

Erklæringen for meldinger om avvik og forbedringer beskriver behandling av navn, IP-adresse, e-postadresse og saksopplysninger om involverte personer. Fylkeskommunen opplyser at sensitive personopplysninger normalt ikke registreres, men kan inngå dersom et avvik skyldes eller kan påvirke helse eller andre sensitive forhold. Opplysninger kan i enkelte tilfeller deles med tilsynsmyndigheter og bedriftshelsetjenesten.

Erklæringen om tilgangsstyring og autentisering angir at formålet er å sikre at bare autoriserte brukere får tilgang til applikasjoner og funksjoner de trenger i arbeidet. Opplysningene omfatter blant annet navn, bruker-ID, IP-adresse, kontaktopplysninger, system- og nettverkslogger og opplysninger om rolle og tilgangsnivå. Det opplyses at enkelte personopplysninger kan overføres utenfor EU/EØS når det foreligger gyldig overføringsgrunnlag.

Erklæringen om sikkerhet og tilgangsstyring i IKT-infrastrukturen beskriver behandling av bruker- og nettverksopplysninger, lokaliseringsinformasjon, brannmurlogger, informasjon om blokkerte domener og sikkerhetsskanning og analyse av dokumenter i Microsoft 365. Formålet er tekniske sikkerhetstiltak som tilgangskontroll, overvåkning, loggføring og analyse. Fylkeskommunen opplyser at automatiske analyser og hendelseshåndtering brukes for å oppdage og stanse mulige sikkerhetshendelser.

Erklæringen for adgangskontroll beskriver behandling av navn, stilling, organisatorisk tilhørighet og tidspunkt og lokasjon ved bruk av adgangskort. Formålet er å kontrollere adgang til fylkeskommunale bygg. Kameraovervåkning omtales i en egen erklæring som et tiltak for å forebygge skadeverk og ivareta sikkerheten i bygg og anlegg. Opptak skal slettes senest syv dager etter at formålet er oppfylt.

Erklæringen for arkiv og postjournal angir at opplysninger behandles for å dokumentere saksbehandling og korrespondanse. Dette kan omfatte identifikasjons- og kontaktopplysninger, saksopplysninger og annen relevant informasjon. Dokumenter kan

gjøres tilgjengelige gjennom innsyn etter offentlighetslovens regler, og opplysninger kan deles med offentlige myndigheter når det foreligger lovpålagt plikt.

Erklæringen for bruk av bilder og video i informasjon og profileringsmateriell angir samtykke som grunnlag for behandlingen. Opplysningene omfatter blant annet navn, kontaktopplysninger, bilde og dokumentasjon av samtykket. Lagringstiden knyttes til samtykket, som kan trekkes tilbake.

6.3.3 Databehandleravtaler

Retningslinje – Nytt informasjonssystem fastsetter at det skal avklares hvem som er databehandler dersom et system skal behandle personopplysninger. Når behandlingen helt eller delvis settes ut til ekstern leverandør eller samarbeidspartner, skal forholdet mellom behandlingsansvarlig og databehandler reguleres i en databehandleravtale. Avtalen skal være signert før behandlingen starter.

Retningslinjen krever at mal for databehandleravtale inngår i anskaffelsesprosessen, og at avtaleinnholdet kontrolleres mot lovverk og sikkerhetskrav før signering. Avtalen skal dokumenteres i Public 360 som del av anskaffelsen og i Samsvars modul for systemforvaltning.

Forvaltningsmodell for informasjonssystemer i TRFK har databehandleravtale som egen aktivitet før et system kan tas i bruk og beskriver tilsvarende krav til signering og dokumentasjon. Organisering roller og ansvar – Informasjonssikkerhet legger ansvar til systemeier for at nødvendig dokumentasjon, herunder databehandleravtale, er etablert.

Arbeidsdokument – DPIA legger opp til registrering av om databehandlere benyttes, om det er etablert avtale med alle databehandlere og lenke til avtalene for det enkelte systemet i Samsvar. Dette beskriver hvordan databehandleravtalene skal knyttes til dokumentasjonen av systemene.

Gjennomgåtte avtaler

Revisor har gjennomgått tre databehandleravtaler fra tjenesteområdene med tilhørende bilag. Avtalene angir hvilke tjenester og behandlinger de gjelder, hvilke typer personopplysninger som behandles og hvilke grupper av personer opplysningene gjelder. De beskriver hvordan leverandøren skal behandle opplysningene på vegne av fylkeskommunen.

Avtalene inneholder bestemmelser om konfidensialitet, informasjonssikkerhet, bruk av underdatabehandlere og bistand til fylkeskommunen ved ivaretakelse av plikter etter

personvernregelverket. De regulerer også håndtering av opplysninger ved avtalens opphør og fylkeskommunens mulighet til å få informasjon om og kontrollere leverandørens behandling.

Praksis ved anskaffelser og leverandørforhold

Flere informanter opplyser at behovet for databehandleravtaler vurderes ved anskaffelser, innføring av systemer og behandling av personopplysninger. Ansvar beskrives som lagt til systemeier eller avtaleeier i linjen, med råd og bistand fra sentrale støttefunksjoner ved behov.

Seksjonsleder eksamen og støttetjenester opplyser at det foreligger databehandleravtaler for systemene seksjonen har ansvar for, og at seksjonen varsles ved endringer. Han beskriver at tilbydere som ikke forholder seg til fylkeskommunens rutiner og databehandleravtaler, avvises.

Seksjonsleder jus og anskaffelser opplyser at databehandleravtaler er satt i system for de avtalene seksjonen har ansvar for. Seksjonen bruker DFØs[22] mal, og forslag til egne avtaler fra leverandører vurderes særskilt. Seksjonen har oversikt over egne avtaler i et kontraktsadministrasjonsverktøy, men har ikke et sentralt ansvar for oversikt over alle avtaler i fylkeskommunen.

Enkelte informanter beskriver at personvernkrav ikke alltid har vært tydelig nok integrert i anskaffelsesprosessene. De viser til utfordringer ved systemer og anskaffelser som gjennomføres utenfor etablerte prosesser eller støttefunksjoner, og behov for tydeligere forankring av krav og kompetanse hos ansvarlige ledere.

6.4 Vurdering

Fylkeskommunen har i hovedsak oversikt over behandlinger av personopplysninger og dokumenterer behandlingsaktivitetene i behandlingsprotokoller i samsvar med personvernregelverket.

Revisor vurderer at fylkeskommunen har etablert ordninger for å holde oversikt over og dokumentere behandling av personopplysninger. Arbeidsdokumentet beskriver hva som skal registreres, og intervjuopplysninger understøtter at behandlingsprotokoller brukes i tjenesteområdene, med ansvar for utarbeidelse og oppdatering.

Fylkeskommunen arbeider samtidig med å videreutvikle oversikten i Samsvar. Intervjuopplysningene viser at arbeidet med en samlet oversikt ikke er ferdigstilt, og at ansvaret

[22] Direktoratet for forvaltning og økonomistyring

for ajourhold er uklart på enkelte områder. Revisor vurderer at dette viser behov for å videreutvikle oversikten og tydeliggjøre ansvaret for oppdatering.

Vurderingen bygger på etablerte ordninger og beskrevet praksis, og omfatter ikke kontroll av behandlingsprotokollenes innhold og fullstendighet.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen gir i hovedsak de registrerte informasjon om hvordan personopplysningene deres behandles

Revisor vurderer at fylkeskommunen gjennom de undersøkte personvernerklæringene gir informasjon om sentrale behandlinger av elevdata, pasientdata og personaldata. Erklæringene er tilgjengelige på nettsiden, og beskriver blant annet formål, behandlingsgrunnlag, opplysninger, mottakere og lagring.

Informasjonen kan samtidig tydeliggjøres for enkelte behandlinger, slik at sentrale opplysningstyper og behandlingen av disse fremgår mer presist. Etter revisors vurdering vil dette gjøre det lettere for de registrerte å forstå hvordan opplysningene deres behandles.

Revisor vurderer at revisjonskriteriet i **hovedsak er oppfylt.**

Fylkeskommunen inngår databehandleravtale når eksterne leverandører behandler personopplysninger på fylkeskommunens vegne

Revisor vurderer at fylkeskommunen har etablert rutiner og ansvar for å inngå databehandleravtaler når eksterne leverandører behandler personopplysninger på fylkeskommunens vegne. Gjennomgangen av tre avtaler fra skole, tannhelse og personal, sammenholdt med intervjuopplysningene, underbygger at databehandleravtaler inngås i de undersøkte tjenesteområdene.

Enkelte informanter beskriver utfordringer ved anskaffelser utenfor etablerte prosesser og med integrering av personvernkrav i anskaffelsesarbeidet. Dette viser en sårbarhet som fylkeskommunen bør følge opp, men det er ikke påvist at nødvendige databehandleravtaler mangler.

Undersøkelsen omfatter et utvalg avtaler og gir ikke grunnlag for å fastslå at samtlige databehandlerforhold i fylkeskommunen er dekket av avtale.

På de undersøkte områdene vurderer revisor at revisjonskriteriet er **oppfylt.**

7 KONKLUSJON OG ANBEFALINGER

7.1 Konklusjon

Revisor konkluderer med at Trøndelag fylkeskommune i hovedsak har etablert og gjennomført et forsvarlig arbeid med digital sikkerhet innenfor de områdene revisjonen har undersøkt. Fylkeskommunen har etablert sentrale rammer for styring og internkontroll, men det er behov for å styrke den systematiske gjennomføringen og oppfølgingen av sikkerhetsarbeidet.

Fylkeskommunen har dokumenterte mål og strategier, en etablert ansvarsfordeling og rutiner for sentrale deler av informasjonssikkerhetsarbeidet. Det er også etablert ordninger for avvikshåndtering, opplæring, tilgangsstyring og behandling av personopplysninger. Revisjonens vurderinger viser at disse ordningene i hovedsak ivaretar de undersøkte kravene.

Samtidig viser revisjonen variasjoner i kjennskap til og bruk av rutiner, mangler ved dokumentasjonen av internkontrollen og behov for mer systematisk bruk av avvik og sikkerhetshendelser i forbedringsarbeidet. Det er også identifisert svakheter ved oppfølging av enkelte tilganger og kontroll av tilgangslogger. Innen personvern er det behov for å videreutvikle den samlede oversikten over behandlinger av personopplysninger og tydeliggjøre enkelte rutiner.

7.2 Anbefalinger

Revisor anbefaler at fylkeskommunen:

- Styrker arbeidet med å sikre at rutiner og prosedyrer for informasjonssikkerhet er kjent og tas i bruk i relevante deler av organisasjonen.
- Sikrer mer fullstendig og oppdatert dokumentasjon av internkontrollen for informasjonssikkerhet, herunder oversikten over informasjonssystemer og behandling av personopplysninger.
- Styrker den systematiske bruken av avvik, sikkerhetshendelser og risiko som grunnlag for læring og forbedring av internkontrollen.
- Etablerer en mer systematisk og risikobasert oppfølging av tilganger, herunder kontroll av tilgangslogger der dette er nødvendig.

KILDER

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften). (2004). https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

Forskrift om pasientjournal (pasientjournalforskriften). (2019). https://lovdata.no/dokument/LTI/forskrift/2019-03-01-168

Lov om behandling av personopplysninger (personopplysningsloven). (2018). https://lovdata.no/dokument/LTI/lov/2018-06-15-38

Lov om kommuner og fylkeskommuner (kommuneloven). (2018). https://lovdata.no/dokument/LTI/lov/2018-06-22-83

Personvernforordningen. (2016). Europaparlaments- og rådsforordning (EU) 2016/679. https://eur-lex.europa.eu/eli/reg/2016/679/oj

Kommunal- og moderniseringsdepartementet. (2018). Lov om kommuner og fylkeskommuner (kommuneloven) (Prop. 46 L (2017–2018)). https://www.regjeringen.no/no/dokumenter/prop.-46-l-20172018/id2593519/

Kommunal- og moderniseringsdepartementet. (2021). Veileder om kommunelovens internkontrollbestemmelser. https://www.regjeringen.no/no/dokumenter/internkontroll-i-kommunesektoren/id2876831/

Datatilsynet (2018). Etablere internkontroll. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

Datatilsynet. (2023.). Databehandleravtale**.** https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/hvordan-lage-en-databehandleravtale/

Datatilsynet. (2023). Innebygd personvern og personvern som standard. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern-og-personvern-som-standard/

Datatilsynet. (2018.). Protokoll over behandlingsaktiviteter**.** https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/protokoll-over-behandlingsaktiviteter/

Digitaliseringsdirektoratet. (2020). Overvåking og hendelseshåndtering. Del av veiledningen Internkontroll i praksis – informasjonssikkerhet.

https://www.digdir.no/informasjonssikkerhet/internkontroll-i-praksis-informasjonssikkerhet/2601

Digitaliseringsdirektoratet. (2021). Regelverkskrav og anbefalinger – internkontroll informasjonssikkerhet**.** https://www.digdir.no/informasjonssikkerhet/regelverkskrav-og-anbefalinger-internkontroll-informasjonssikkerhet/3229

Datatilsynet. (2019). Integritet og konfidensialitet**.** https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/integritet-og-konfidensialitet/

Datatilsynet. (2023). Personvernprinsippene**.** https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/

Digitaliseringsdirektoratet. (2022). Felles sikkerhet i forvaltningen. https://www.digdir.no/informasjonssikkerhet/felles-sikkerhet-i-forvaltningen/5957

Digitaliseringsdirektoratet. (u.å.). Styringsaktiviteter. https://www.digdir.no/informasjonssikkerhet/styringsaktiviteter/3153

Helsedirektoratet. (2025). Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), punkt 5.2 om tilgangsstyring. https://www.helsedirektoratet.no/normen/norm-for-informasjonssikkerhet-og-personvern-i-helse-og-omsorgssektoren

Nasjonal sikkerhetsmyndighet. (2024a). De fire kategoriene. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/introduksjon/de-fire-kategoriene/

Nasjonal sikkerhetsmyndighet. (2024). NSMs grunnprinsipper for IKT-sikkerhet. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/introduksjon/

Nasjonal sikkerhetsmyndighet. (2024c). Kartlegg brukere og behov for tilgang. https://nsm.no/regelverk-og-hjelp/rad-og-anbefalinger/identifisere-og-kartlegge/kartlegg-brukere-og-behov-for-tilgang/

Fylkeskommunens dokumenter

- **Trøndelag fylkeskommunes styrende dokumenter, strategier, rutiner og arbeidsdokumenter**
- **Trøndelag fylkeskommunens årsrapport for 2025. https://www.trondelagfylke.no/nyhetsarkiv/arsrapport-2025/**
- **Personvernerklæringer**

- **Databehandleravtaler**

VEDLEGG 1 – UTLEDNING AV REVISJONSKRITERIER

Ifølge forskrift om kontrollutvalg og revisjon (§ 15) skal det etableres revisjonskriterier for gjennomføring av forvaltningsrevisjon. Revisjonskriterier er de krav og forventninger som forvaltningsrevisjonsobjektet skal revideres/vurderes i forhold til. Disse kriteriene skal være begrunnet i, eller utledet av, autoritative kilder innenfor det reviderte området. Slike autoritative kilder kan være lov, forskrift, forarbeider, rettspraksis, politiske vedtak (mål og føringer), administrative retningslinjer, samt statlige føringer og praksis. I denne forvaltningsrevisjonen har vi benyttet oss av følgende kilder til revisjonskriterier:

- Kommuneloven
- eForvaltningsforskriften
- Personvernforordningen (GDPR)
- Pasientjournalforskiften
- Kommunal og moderniseringsdepartementet (2018). Prop. 46 L (2017–2018). Lov om kommuner og fylkeskommuner (kommuneloven)
- Kommunal- og moderniseringsdepartementet. (2021). Veileder om kommunelovens internkontrollbestemmelser.
- Datatilsynet (2018). Etablere internkontroll
- Datatilsynet. (2023.). Databehandleravtaler
- Datatilsynet. (2023). Innebygd personvern og personvern som standard.
- Datatilsynet. (2018.). Protokoll over behandlingsaktiviteter.
- Digitaliseringsdirektoratet. (2020). Overvåking og hendelseshåndtering. Del av veiledningen Internkontroll i praksis – informasjonssikkerhet.
- Digitaliseringsdirektoratet. (2021). Regelverkskrav og anbefalinger – internkontroll informasjonssikkerhet.
- Helsedirektoratet. (2025). Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren (Normen), punkt 5.2 om tilgangsstyring.
- Nasjonal sikkerhetsmyndighet. (2024). NSMs grunnprinsipper for IKT-sikkerhet.

Styringssystemer og rutiner

Kommuneloven § 25-1 stiller krav om at fylkeskommunens internkontroll skal være systematisk og tilpasses virksomhetens størrelse, egenart, aktiviteter og risikoforhold. Som del av internkontrollen skal kommunedirektøren blant annet ha nødvendige rutiner og prosedyrer og dokumentere internkontrollen i den formen og det omfanget som er nødvendig. Hva som er

nødvendig av rutiner, prosedyrer og dokumentasjon, må dermed vurderes ut fra virksomhetens aktiviteter og risikoforhold.

Det følger videre av forarbeidene til kommuneloven (Prop. 46 L (2017–2018)) at rutiner og prosedyrer må gjelde for virksomheten, gjøres kjent og være tilgjengelige. Kravet innebærer dermed ikke bare at nødvendige rutiner og prosedyrer skal være etablert, men også at de må gjøres kjent og tilgjengelige slik at de kan tas i bruk i virksomheten.

For informasjonssikkerhet følger det i tillegg av eForvaltningsforskriften § 15 at forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet. Målene og strategien skal danne grunnlaget for virksomhetens internkontroll på informasjonssikkerhetsområdet. Internkontrollen skal baseres på anerkjente standarder for styringssystem for informasjonssikkerhet, og omfang og innretning skal være tilpasset risiko.

Digitaliseringsdirektoratet beskriver sikkerhetsstrategien som virksomhetens sentrale valg og prioriteringer i sikkerhetsarbeidet. Retningslinjene for hvordan sikkerhetsarbeidet skal organiseres og gjennomføres må blant annet klargjøre roller, myndighet og ansvar. Tydelige roller og ansvar er nødvendig for at oppgaver knyttet til styring og kontroll med informasjonssikkerheten skal kunne gjennomføres og følges opp.

Ved behandling av personopplysninger gjelder i tillegg personvernforordningens krav til den behandlingsansvarliges ansvar. Etter artikkel 24 skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen skjer i samsvar med regelverket. Dette innebærer blant annet behov for en tydelig organisering av ansvar og oppgaver på personvernområdet.

Utledede revisjonskriterier:

- Fylkeskommunen skal ha dokumenterte mål og strategi for informasjonssikkerhet i digitale tjenester og systemer.
- Fylkeskommunen skal ha avklart og dokumentert roller, ansvar og myndighet for informasjonssikkerhet og personvern.
- Fylkeskommunen skal ha nødvendige rutiner og prosedyrer for informasjonssikkerhet.
- Fylkeskommunen skal sikre at rutiner og prosedyrer for informasjonssikkerhet er gjort kjent, tilgjengelige og tatt i bruk i relevante deler av organisasjonen.

- Fylkeskommunen skal dokumentere internkontrollen for informasjonssikkerhet i den formen og det omfanget som er nødvendig.

Avvik og forbedringsarbeid

Kommuneloven § 25-1 stiller krav om at fylkeskommunen skal avdekke og følge opp avvik og risiko for avvik. Departementets veileder om kommunelovens internkontrollbestemmelser presiserer at internkontrollen både skal avdekke og følge opp konkrete avvik som har skjedd, og risiko for at avvik kan skje. Avdekkede avvik skal følges opp eller korrigeres på en egnet måte. Oppfølgingen skal blant annet bidra til å rette opp eller redusere konsekvenser, forebygge nye avvik og gi grunnlag for læring og forbedring av virksomheten (Kommunal- og distriktsdepartementet, 2021, punkt 2.4.4).

For informasjonssikkerhet følger det av eForvaltningsforskriften § 15 at fylkeskommunen skal ha internkontroll på informasjonssikkerhetsområdet basert på anerkjente standarder for styringssystem for informasjonssikkerhet. Omfang og innretning på internkontrollen skal være tilpasset risiko. Digitaliseringsdirektoratets veiledning om internkontroll beskriver overvåking og hendelseshåndtering som en del av det systematiske informasjonssikkerhetsarbeidet. Virksomheten bør ha et system for rapportering og oppfølging av hendelser, avvik og informasjonssikkerhetsbrudd, der det framgår hva som skal rapporteres, hvordan rapportering skal skje og hvem som har ansvar for oppfølging (eForvaltningsforskriften § 15; Digitaliseringsdirektoratet, *Overvåking og hendelseshåndtering*).

Formålet med hendelses- og avvikshåndteringen er blant annet å redusere konsekvensene av hendelser, forebygge nye informasjonssikkerhetsbrudd og lære av tidligere erfaringer. Digitaliseringsdirektoratet viser til at oppfølgingen blant annet kan innebære korrigering eller forbedring av sikkerhetstiltak, kompetansetiltak og oppdatering av risikovurderinger. Informasjonen fra hendelses- og avvikshåndteringen bør systematisk brukes i virksomhetens videre arbeid med vurdering og håndtering av risiko (Digitaliseringsdirektoratet, *Overvåking og hendelseshåndtering*).

Ved brudd på personopplysningssikkerheten gjelder i tillegg personvernforordningen artikkel 33. Den behandlingsansvarlige skal vurdere hvilken risiko bruddet innebærer for fysiske personers rettigheter og friheter for å avgjøre om bruddet skal meldes til Datatilsynet. Uavhengig av om bruddet er meldepliktig, skal ethvert brudd på personopplysningssikkerheten dokumenteres. Dokumentasjonen skal omfatte de faktiske forholdene rundt bruddet, virkningene av det og hvilke tiltak som er truffet for å utbedre det (personvernforordningen artikkel 33 nr. 1 og 5).

Utledede revisjonskriterier:

- Fylkeskommunen skal ha skriftlige rutiner for å avdekke, registrere, klassifisere, behandle og følge opp avvik og sikkerhetshendelser knyttet til informasjonssikkerhet.
- Fylkeskommunen skal ha rutiner som sikrer at brudd på personopplysningssikkerheten vurderes og dokumenteres.
- Fylkeskommunen skal bruke avvik, sikkerhetshendelser og risiko for avvik som grunnlag for forbedring av internkontrollen for informasjonssikkerhet.

Kompetanse og opplæring

Kommuneloven § 25-1 inneholder ikke et selvstendig og detaljert krav om opplæring og kompetanseutvikling som eget internkontrollelement. Departementets veileder om kommunelovens internkontrollbestemmelser presiserer at bruk av kvalifisert personell, opplæring og kompetanseutvikling ikke er lovfestet som egne elementer i bestemmelsen. Samtidig skal fylkeskommunen ha en internkontroll som er egnet til å sikre etterlevelse av lover og forskrifter, og nødvendige rutiner og prosedyrer skal være kjent og tilgjengelige for dem som har behov for å kjenne dem (Kommunal- og distriktsdepartementet, 2021, punkt 2.4).

Ved behandling av personopplysninger følger det av personvernforordningen artikkel 29 at personer som handler under den behandlingsansvarliges eller databehandlerens myndighet og har tilgang til personopplysninger, bare skal behandle opplysningene etter instruks fra den behandlingsansvarlige, med mindre annet følger av rettslige krav. Dette innebærer at personer som gis tilgang til personopplysninger må få nødvendige instrukser for behandlingen.

Personvernforordningen artikkel 24 og 32 stiller videre krav om egnede tekniske og organisatoriske tiltak for å sikre og kunne påvise at behandlingen skjer i samsvar med regelverket. Datatilsynet viser i sin veiledning om internkontroll og informasjonssikkerhet til at ansatte og eventuelle tredjepartsbrukere bør få hensiktsmessig opplæring før de får tilgang til informasjon eller tjenester. Opplæringen bør blant annet omfatte krav til informasjonssikkerhet, juridisk ansvar, interne sikkerhetstiltak, sikker bruk av informasjonssystemer og rapportering av avvik. Opplæringen bør tilpasses ulike målgruppers behov, og brukerne bør holdes oppdatert på virksomhetens retningslinjer og rutiner (Datatilsynet, *Etablere internkontroll – oppfølging og opplæring*).

Personvernforordningen artikkel 39 angir i tillegg at personvernombudets oppgaver blant annet skal omfatte og informere og gi råd til ansatte som behandler personopplysninger og å

kontrollere etterlevelsen av regelverket og virksomhetens personvernretningslinjer, herunder holdningsskapende tiltak og opplæring av personell som er involvert i behandlingsaktivitetene.

Behovet for informasjon og opplæring vil variere med hvilke oppgaver den enkelte utfører og hvilke opplysninger vedkommende behandler. For ansatte som behandler elevdata, pasientdata eller personaldata innebærer dette at informasjon og opplæring må være tilpasset de kravene i regelverk og interne rutiner som er relevante for behandlingen de utfører.

Kommuneloven § 25-1 krever at internkontrollen dokumenteres i den formen og det omfanget som er nødvendig. Personvernforordningens krav til ansvarlighet innebærer samtidig at den behandlingsansvarlige skal kunne påvise at behandlingen skjer i samsvar med regelverket. Dette innebærer ikke et generelt krav om at hvert enkelt opplærings- eller informasjonstiltak skal dokumenteres, men fylkeskommunen må ha den dokumentasjonen som er nødvendig for å kunne følge opp om relevante tiltak er gjennomført som del av internkontrollen.

Utledede revisjonskriterier:

- Fylkeskommunen skal sikre at ansatte og andre brukere som får tilgang til digitale systemer og personopplysninger, får nødvendig opplæring om sikker bruk, konfidensialitet, tilgangsstyring, avvikshåndtering og behandling av personopplysninger.
- Fylkeskommunen skal sikre at ansatte som behandler elevdata, pasientdata eller personaldata får nødvendig informasjon og opplæring om relevante krav i regelverk og interne rutiner.
- Fylkeskommunen skal dokumentere gjennomførte opplærings- og informasjonstiltak i det omfanget som er nødvendig for å kunne følge opp internkontrollen.

Tilgangsstyring

Personvernforordningen artikkel 5 nr. 1 bokstav f fastsetter at personopplysninger skal behandles på en måte som sikrer tilstrekkelig sikkerhet, herunder vern mot uautorisert eller ulovlig behandling. Etter artikkel 32 skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å oppnå et sikkerhetsnivå som er egnet ut fra risikoen. Ved vurderingen skal det blant annet tas hensyn til risikoen for ikke-autorisert utlevering av eller tilgang til personopplysninger.

Tilgangsstyring er et sentralt tiltak for å ivareta disse kravene. Datatilsynet beskriver tilgangsstyring som regulering av hvem som skal ha hvilken type tilgang til personopplysninger, og legger til grunn at tilgang som standard skal være basert på tjenstlig behov ut fra en

nødvendighetsvurdering. Datatilsynet anbefaler at virksomheten etablerer rutiner for hvilke roller som skal ha tilgang til ulike typer personopplysninger og hvilke tilganger den enkelte har behov for i sitt arbeid, samt at tilgangsstyringen gjennomgås regelmessig (Datatilsynet, *Innebygd personvern og personvern som standard*).

For informasjonssikkerhet generelt følger det av eForvaltningsforskriften § 15 at fylkeskommunen skal ha internkontroll på informasjonssikkerhetsområdet basert på anerkjente standarder for styringssystem for informasjonssikkerhet, tilpasset virksomhetens risiko. Tilgangsstyring inngår som et sentralt sikkerhetstiltak for å beskytte informasjon og informasjonssystemer mot uautorisert tilgang. NSMs grunnprinsipper for IKT-sikkerhet fremhever blant annet behovet for oversikt over brukere, kontoer og tilgangsbehov og for at brukere ikke gis større rettigheter enn de trenger. Grunnprinsippene er anbefalinger og brukes her som støtte til forståelsen av risikobasert tilgangsstyring, ikke som selvstendig grunnlag for rettslige krav.

For behandling av pasientopplysninger gjelder særskilte krav. Etter pasientjournalforskriften § 13 skal behandling av journalopplysninger baseres på bestemte tildelte autorisasjoner. Autorisasjonene skal dokumenteres, være tidsbegrensede og vurderes på nytt når det skjer endringer i ansvarsområder eller ansettelsesforhold. Den dataansvarlige skal ha oversikt over hvem som har tilgang til hvilke typer opplysninger og kunne kontrollere i ettertid hvem som har benyttet seg av tilgangen.

Norm for informasjonssikkerhet og personvern i helse- og omsorgssektoren utdyper kravene til tilgangsstyring på helseområdet. Normen angir at virksomheten skal ha rutiner for autorisering, endring og avslutning av tilganger, og at bare autorisert personell med tjenstlig behov skal få tilgang til helse- og personopplysninger. Tilgangsstyringen omfatter også administrator- og systembrukere. For brukere med administratortilganger beskriver Normen særskilte tiltak, blant annet bruk av personlig separat administratorkonto og risikovurdering av behovet for administratorbrukere (Normen, punkt 5.2).

Tilgangsstyringen må også kunne kontrolleres. Datatilsynet viser til logging som et tiltak for å sikre sporbarhet og for å kunne kontrollere hvem som har behandlet personopplysninger. For pasientjournaler følger det særskilt av pasientjournalforskriften § 14 at tilgjengeliggjøring av journalopplysninger skal dokumenteres automatisk. Normen utdyper hvordan logger kan brukes i kontrollen med tilgangsstyringen, og beskriver risikobasert analyse og oppfølging av logger for å avdekke urettmessig tilgang.

Utledede revisjonskriterier:

- Fylkeskommunen skal ha rutiner for tilgangsstyring i digitale systemer som behandler eller gir tilgang til personopplysninger og annen beskyttelsesverdig informasjon.
- Fylkeskommunen skal sikre at tilganger tildeles på bakgrunn av tjenstlig behov.
- Fylkeskommunen skal ha rutiner for logging og oppfølging av tilgang der dette er nødvendig for å avdekke eller følge opp urettmessig tilgang, eller følger av særskilt regelverk.

Etterlevelse av personvernregelverket i tjenesteområdene

Personvernforordningen artikkel 30 stiller krav om at den behandlingsansvarlige skal føre protokoll over behandlingsaktiviteter som utføres under dennes ansvar. Protokollen skal blant annet inneholde informasjon om formålene med behandlingen, kategorier av registrerte og personopplysninger, kategorier av mottakere, eventuelle overføringer til tredjeland og, dersom det er mulig, planlagte slettefrister og en generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak. Datatilsynet viser til at protokollen skal gi virksomheten en samlet og dokumentert oversikt over behandlingen av personopplysninger (personvernforordningen artikkel 30; Datatilsynet, *Protokoll over behandlingsaktiviteter*).

Personvernforordningen artikkel 12–14 stiller krav til informasjon til de registrerte. Informasjonen skal gis på en kortfattet, åpen, forståelig og lett tilgjengelig måte og i et klart og enkelt språk. Hvilken informasjon som skal gis, avhenger blant annet av om opplysningene er samlet inn fra den registrerte eller fra andre. Informasjonen skal blant annet omfatte hvem som er behandlingsansvarlig, formålet med og det rettslige grunnlaget for behandlingen, eventuelle mottakere av opplysningene og informasjon om den registrertes rettigheter (personvernforordningen artikkel 12–14).

Når en ekstern leverandør behandler personopplysninger på vegne av fylkeskommunen, gjelder kravene til bruk av databehandler i personvernforordningen artikkel 28. Behandlingen skal reguleres i en avtale eller et annet rettslig dokument som er bindende for databehandleren. Avtalen skal blant annet regulere behandlingens art, formål og varighet, hvilke typer personopplysninger og kategorier av registrerte som omfattes, og den behandlingsansvarliges og databehandlerens rettigheter og plikter. Datatilsynet viser til at databehandleravtalen skal sette klare rammer for hvordan databehandleren kan behandle personopplysningene (personvernforordningen artikkel 28; Datatilsynet, *Hvordan lage en databehandleravtale?*).

Utledede revisjonskriterier:

- Fylkeskommunen skal ha oversikt over behandling av personopplysninger og dokumentere behandlingsaktivitetene i behandlingsprotokoller i samsvar med personvernregelverket.
- Fylkeskommunen skal gi de registrerte informasjon om hvordan personopplysningene deres behandles.
- Fylkeskommunen skal inngå databehandleravtale når eksterne leverandører behandler personopplysninger på fylkeskommunens vegne.

VEDLEGG 2 – UTTALELSE

Fylkesdirektørens uttalelse til rapport om digital sikkerhet

Fylkesdirektøren takker Revisjon Midt-Norge for en grundig gjennomgang av Trøndelag fylkeskommunes arbeid med digital sikkerhet. Rapporten gir nyttige innspill til det videre arbeidet med informasjonssikkerhet og personvern.

Fylkesdirektøren merker seg revisjonens konklusjon om at fylkeskommunen i hovedsak har etablert og gjennomført et forsvarlig arbeid med digital sikkerhet innenfor de undersøkte områdene. Det er positivt at revisjonen finner at sentrale rammer for styring og internkontroll er etablert. Samtidig viser rapporten behov for å styrke den systematiske gjennomføringen og oppfølgingen av sikkerhetsarbeidet.

Fylkeskommunen arbeider med å innføre et nytt overordnet kvalitetssystem. Dette skal gjøre styrende dokumenter lettere tilgjengelige, bedre kjent i organisasjonen, og styrke muligheten til å dokumentere at styringssystemet er gjort kjent. Dette gir et mer systematisk og etterprøvbart grunnlag for å følge opp at fylkeskommunens enheter har satt seg inn i gjeldende føringer, og for å avdekke behov for videre oppfølging.

Kvalitetssystemet skal også understøtte en mer systematisk oppfølging av avvik og sikkerhetshendelser, slik at erfaringer og identifiserte risikoforhold i større grad brukes som grunnlag for læring og forbedring.

Fylkesdirektøren registrerer revisjonens anbefaling om mer fullstendig og oppdatert dokumentasjon av internkontrollen, herunder oversikten over informasjonssystemer og behandlinger av personopplysninger. Dette vil bli fulgt opp i det videre internkontrollarbeidet. Det samme gjelder anbefalingen om en mer systematisk og risikobasert oppfølging av tilganger, herunder kontroll av tilgangslogger der dette er nødvendig.

Informasjonssikkerhet og personvern krever kontinuerlig oppfølging og utvikling. Fylkesdirektøren vil bruke revisjonens funn og anbefalinger i det videre arbeidet med å styrke internkontrollen og sikre at etablerte rammer og rutiner følges opp i praksis.

Postadresse: Fylkets hus
Postboks 2560
7735 Steinkjer

Bankkonto: 86017685300
IBAN: NO8486017685300
BIC/SWIFT: DABANO22

Telefon: 74 17 40 00
Epost: postmottak@trondelagfylke.no
Org.nr: 817 920 632

Trøndelag fylkeskommune
Seksjon Organisasjon

Fylkesdirektøren takker for et godt samarbeid gjennom revisjonsprosessen.

Med vennlig hilsen

Carl-Jakob Midttun
fylkesdirektør

Hilde Vikan
direktør organisasjon og økonomi