Vestfold og Telemark revisjon

Behandling av personopplysninger

Forvaltningsrevisjon | Telemark fylkeskommune

25: 4000 404

Innhold

Sammendrag 3

1. Innledning 5

1.1. Kontrollutvalgets bestilling 5
1.2. Problemstilling og revisjonskriterier 5
1.3. Avgrensning 6
1.4. Metode og kvalitetssikring 6
1.5. Fylkesdirektørens uttalelse 6

2. Behandling av personopplysninger 7

2.1. Organisering og rapportering 7
2.2. Personvernombud i Telemark fylkeskommune 23
2.3. Protokoll over behandlingsaktiviteter 25
2.4. Risikovurdering 29
2.5. Vurdering av personvernkonsekvenser (DPIA) 31
2.6. Avvikshåndtering 35
2.7. Ivaretakelse av registrertes rettigheter 41
2.8. Databehandleravtaler 47

3. Konklusjoner og anbefalinger 50

3.1. Konklusjoner 50
3.2. Anbefalinger 51

Litteratur og kildereferanser 52

Vedlegg 54

Vedlegg 1: Fylkesdirektørens uttalelse 54
Vedlegg 2: Revisjonskriterier 55
Vedlegg 3: Metode og kvalitetssikring 61

Sammendrag

Kommuner og fylkeskommuner er komplekse organisasjoner med et bredt spekter av oppgaver, og behandler store mengder informasjon om innbyggerne. Datatilsynet har sett mange brudd på personvernsikkerheten i denne sektoren, noe som har ført til store bøter. Etter en tilsynsaksjon i 2023 peker Datatilsynet på at det gjøres mye godt personvernarbeid til tross for begrensede ressurser, men at mange fortsatt mangler overordnede retningslinjer og rutiner/prosedyrer.

Denne rapporten er bestilt av kontrollutvalget i Telemark fylkeskommune, og handler om følgende problemstillinger:

1. **Har Telemark fylkeskommune etablert tiltak for å ivareta kravene i personopplysningsloven?**

2. **Hvordan blir personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern fulgt opp i praksis i fylkeskommunens virksomheter?**

Vi har undersøkt praksis innen tannhelsetjenesten og to videregående skoler. Data er samlet inn gjennom dokumentgjennomgang, intervjuer og spørreundersøkelse blant ansatte i tannhelsetjenesten og to videregående skoler.

Har Telemark fylkeskommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Etter fylkesdelingen har Telemark fylkeskommune etablert et nytt og omfattende styringssystem for informasjonssikkerhet og personvern, inkludert rutiner, prosedyrer og et dedikert organisasjonsnettverk med personvernombud og koordinatorer på sektornivå.

Det er innført et GRC-verktøy (Governance, Risk and Compliance) for systematisk protokollføring av behandlingsaktiviteter, risikovurderinger og oversikt over databehandlere.

Fylkeskommunen har med dette etablert tiltak for å ivareta kravene i personopplysningsloven.

Som fylkeskommunen selv påpeker, gjenstår det noe opplæring- og implementeringsarbeid, særlig i skolene. Flere tiltak er beskrevet i årshjul og planer.

Våre stikkprøver viser at protokollen over behandlingsaktiviteter, risikovurderinger og databehandleravtaler på revisjonstidspunktet ikke er fullstendig, og at det er et etterslep etter fylkesdelingen. Dette er fylkeskommunen kjent med, og har forut for og i løpet av revisjonen gjort flere tiltak for å fange opp nye behandlinger, sikre protokollføring og databehandleravtaler m.m.

Fylkeskommunens tiltak har så langt ikke sikret at DPIA alltid gjennomføres når det er høy risiko for fysiske personers rettigheter og friheter. Det er grunn til å tro at det nye verktøyet for protokoll (GRC-verktøyet) vil bidra til å ivareta dette på sikt, når protokollen blir fullstendig.

Informasjon om registrertes rettigheter gis hovedsakelig gjennom personvernerklæringer, men disse inneholder ikke alltid all relevant og lovpålagt informasjon.

Hvordan blir personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern fulgt opp i praksis i fylkeskommunens virksomheter?

Arbeidet med opplæring og implementering av styringssystemet er så vidt i gang høsten 2025. Vi ser derfor at personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern bare delvis er fulgt opp i praksis ved tannklinikkene og de to undersøkte videregående skolene.

Roller og ansvar for personvern er ennå ikke tilstrekkelig forankret i hele organisasjonen, spesielt innen skole, hvor det mangler tiltak for opplæring og bevisstgjøring.

Det er mangelfull praksis for gjennomføring av risikovurderinger, godkjenning og dokumentasjon av DPIA (vurdering av personvernkonsekvenser), avvikshåndtering og tiltak for å sikre at de registrerte får tilstrekkelig informasjon om sine rettigheter.

Det er viktig at implementeringsplanene gjennomføres, og at det arbeides kontinuerlig med å ivareta en god personvernskultur. Avvikshåndtering handler om å lære av feil, slik at risikoen i neste omgang blir mindre. Avviksstatistikk gir viktig informasjon for å sikre relevante og treffende tiltak, ut over den erfaringen det enkelte avvik gir. Derfor er det viktig å etablere god kultur for å melde avvik i hele organisasjonen, særlig når styringssystemet er nytt.

Anbefalinger

Vi anbefaler fylkeskommunen å

- fortsette arbeidet med å få en oppdatert og fullstendig protokoll og oppdaterte databehandleravtaler med alle databehandlere
- sikre at det gjøres regelmessige risikovurderinger og nødvendige DPIA i tråd med lovkrav og interne rutiner
- sørge for at personvernerklæringer gir lovpålagt informasjon og god oversikt over registrertes rettigheter, og at elever og andre mottar informasjon om sine rettigheter ved innsamling av personopplysninger
- gjennomføre planlagt opplæring/implementering, og vurdere særskilte tiltak for skolene
- sikre en god kultur for å melde og følge opp avvik

Skien, 27. november 2025

1. Innledning

1.1. Kontrollutvalgets bestilling

Forvaltningsrevisjonen er bestilt av kontrollutvalget i Telemark fylkeskommune i sak 20/25 Bakgrunnen for bestillingen er kontrollutvalgets vedtatte plan for forvaltningsrevisjon og eierskapskontroll for perioden 2024-2028.

Reglene om forvaltningsrevisjon står i kommuneloven § 23-2 første ledd bokstav c, jf. § 23-3 og § 24-2 og i forskrift om kontrollutvalg og revisjon.

1.2. Problemstilling og revisjonskriterier

Rapporten handler om følgende problemstillinger:

3. Har Telemark fylkeskommune etablert tiltak for å ivareta kravene i personopplysningsloven?

4. Hvordan blir personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern fulgt opp i praksis i fylkeskommunens virksomheter?

Vi har undersøkt praksis innen tannhelsetjenesten og to videregående skoler.

Revisjonskriteriene[1] er hentet fra personopplysningsloven, forskrift om elektronisk kommunikasjon med og i forvaltningen og fylkeskommunens egne rutiner. Kriteriene framgår under hvert kapittel nedenfor, og er nærmere omtalt i vedlegg 2.

Datatilsynets undersøkelser viser at etterlevelsen av personvernreglene oppleves lavere i kommuner og fylkeskommuner enn i andre sektorer. Årsaken til dette er sammensatt, blant annet at kommunene og fylkeskommunene er komplekse organisasjoner med et bredt spekter av oppgaver, og at de derfor behandler store mengder informasjon om innbyggerne. Datatilsynet har sett mange brudd på personvernsikkerheten i denne sektoren, noe som har ført til store bøter.[2] Etter en tilsynsaksjon i 2023 peker Datatilsynet på at det gjøres mye godt personvernarbeid til tross for begrensede ressurser, men at mange fortsatt mangler overordnede retningslinjer og rutiner/prosedyrer, og at det er behov for mer, bedre og samlet veiledning.[3]

[1] Det skal alltid etableres revisjonskriterier i forvaltningsrevisjon, jf. forskrift om kontrollutvalg og revisjon § 15. Revisjonskriterier er de regler og normer som gjelder innenfor det området vi skal undersøke. Revisjonskriteriene er grunnlaget for revisors analyser, vurderinger og konklusjoner.

[2] Personvernombud - undersøkelse 2020/21 | Datatilsynet
[3] Funn fra tilsyn i kommuner og fylkeskommuner | Datatilsynet

1.3. Avgrensning

Forvaltningsrevisjonen omfatter ikke fylkeskommunens behandling av personopplysninger om egne ansatte og politikere, eller fylkeskommunens rolle som databehandler for andre virksomheter.

Vi har ikke undersøkt om ordninger for registrering og oppbevaring av personopplysninger er i samsvar med regler om journalføring og arkivering.

1.4. Metode og kvalitetssikring

Denne forvaltningsrevisjonen er gjennomført av forvaltningsrevisor Sofie L. R. Berge, med Kirsti Torbjørnson som oppdragsansvarlig.

Vi har kartlagt rutiner på området og intervjuet ansatte som har oppgaver innenfor informasjons-sikkerhet og personvern sentralt i fylkeskommunen. Videre har vi undersøkt stikkprøver og gjennomført to spørreundersøkelser. Innenfor tannhelse har vi intervjuet seksjonsleder og personvernskoordinator for tannhelse, og sendt en spørreundersøkelse til alle tannklinikkene. Innenfor Utdanning har vi intervjuet ansatte i Team skoleutvikling som har oppgaver med personvern. Vi har plukket ut Nome og Porsgrunn videregående skoler. Her har vi intervjuet rektorene og deler av deres ledergruppe, og sendt en spørreundersøkelse til alle ansatte ved disse to skolene.

Det står mer om metode og tiltak for kvalitetssikring i vedlegg 3 til rapporten.

1.5. Fylkesdirektørens uttalelse

Rapporten er presentert i et møte med administrasjonen i fylkeskommunen og sendt til uttalelse 14.11.2025, jf. forskrift om kontrollutvalg og revisjon § 14. Fylkesdirektørens uttalelse ligger i vedlegg 1.

2. Behandling av personopplysninger

Har Telemark fylkeskommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Hvordan blir personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern fulgt opp i praksis i fylkeskommunens virksomheter?

2.1. Organisering og rapportering

Telemark fylkeskommune skal ha en organisasjon med klar plassering av ansvar og myndighet for behandlingen av personopplysninger, samt rutiner eller tiltak for rapportering.

Telemark fylkeskommune ble slått sammen med Vestfold fylkeskommune i 2018, med virkning fra 2020. Etter fire år i sameksistens, ble fylkeskommunene delt igjen med virkning fra 1.1.2024. Delingen førte til ny organisering og flere nye ledere. Over flere år er det dermed brukt mye ressurser på sammenslåing og deling og flere runder med omstillingsprosesser og reorganisering.

Ansvar og myndighet reguleres i et politisk og administrativt delegeringsreglement. I tillegg har fylkeskommunen etablert et helt nytt styringssystem for informasjonssikkerhet og personvern. Disse er nærmere beskrevet nedenfor.

Personopplysninger behandles i mange ulike systemer. Fylkeskommunen har tatt i bruk et GRC-verktøy[4] som skal bidra til å sikre oversikt og etterlevelse av personvernreglene.

2.1.1. Ansvar- og myndighetsfordeling – data

Delegeringsreglement

Telemark fylkeskommune har et reglement for delegering av myndighet fra fylkestinget, vedtatt 23.10.2024.

Fylkesdirektøren leder og organiserer administrasjonen og har fullmakter som gjelder drift av fylkeskommunen, med de unntak som framgår av lov, delegeringsreglementet eller andre vedtak i fylkestinget. Avgjørelser som gjelder drift og organisering vil i mange tilfeller være knyttet til bestemmelser i ulike særlover. I saker som ikke er delegert til andre organer og/eller ikke er av prinsipiell karakter, har fylkesdirektøren myndighet til å ta beslutninger.

[4] GRC står for Gorvernance, Risk and Compliance. Slike verktøy skal hjelpe organisasjonen med å styre, redusere risiko og sikre etterlevelse av gjeldende krav.

Fylkesdirektøren avgjør selv videre delegering i administrasjonen. Alle saker kan delegeres, med mindre det er spesielt uttalt at myndigheten ikke delegeres videre. Fylkesdirektøren selv utarbeider retningslinjer for videredelegering i administrasjonen og utøvelsen av slik delegert myndighet.

Administrativ delegering

Fylkeskommunen har et administrativt delegeringsreglement, vedtatt av fylkesdirektøren 11. august 2025. Det fremgår av dette reglementet at fylkesdirektør er behandlingsansvarlig etter personvernregelverket. Fylkesdirektøren har delegert utøvende behandlingsansvar til fylkessjefene. Fylkessjefene har generelt myndighet til å inngå databehandleravtaler og avtaler om felles behandlingsansvar på vegne av fylkeskommunen, innenfor sitt ansvarsområde. Fylkessjefene kan ikke delegere myndigheten til å inngå databehandleravtaler til andre enn seksjonsledere og rektorer.

Delegeringsreglementet kapittel 10 handler om delegering av myndighet etter særlov. På disse områdene er myndighet etter spesifikke bestemmelser i personopplysningsloven delegert til ulike roller, enten fylkessjefer, seksjonsledere/rektorer, teamledere/klinikkledere/avdelingsledere, personvernombudet, fylkesadvokaten og ansatte hos fylkesadvokaten. På særlovsområdene er det delegert til fylkessjefer, seksjonsledere/rektorer, teamledere/klinikkledere/avdelingsledere og personvernombudet å inngå databehandleravtaler.

Telemark fylkeskommune har et intranett som heter Innsida. Her deles informasjon og tjenester med ansatte. Innsida har en egen fane om informasjonssikkerhet og personvern, og her ligger også informasjon om roller og ansvar på området.

Styringssystem og -dokument for informasjonssikkerhet og personvern

Telemark fylkeskommune hadde ikke noe styringssystem for informasjonssikkerhet og personvern etter delingen i 2024. Det forelå heller ingen etablerte rutiner for risikovurderinger, eller malverk for risikovurdering, DPIAer eller databehandleravtaler.

Etter delingen har fylkeskommunen etablert et helt nytt styringssystem for informasjonssikkerhet og personvern. Et styringsdokument gir informasjon om roller og ansvar, og gjelder for alle ansatte, innleide konsulenter og leverandører som har tilgang til eller behandler fylkeskommunens informasjon, enten det er digitalt eller i fysisk form. Rolle- og ansvarsbeskrivelser ble godkjent av fylkesdirektørens ledergruppe første gang i mai 2024, og omtaler blant annet følgende:

Sikkerhetsorganisasjonen

Sikkerhetsorganisasjonen er ansvarlig for å utvikle, implementere, overvåke og forvalte styringssystemet for informasjonssikkerhet. Sikkerhetsorganisasjonen er

- fylkesdirektørens ledergruppe (en representant fra ledergruppen)
- seksjonsleder digitale tjenester
- teamleder teknologi og utvikling
- sikkerhetsrådgiver merkantil
- sikkerhetsrådgiver teknisk

- beredskapskoordinator[5]
- personvernombudet[6]

Sikkerhetsorganisasjonen skal etablere faste samarbeidsarenaer.

Fylkesdirektørens ledergruppe skal blant annet sikre at styringssystemet for informasjonssikkerhet er etablert, og at status gjennomgås årlig i ledelsens gjennomgang[7]. Ledergruppa skal også gjøre vurdering og beslutning av vurderinger av personvernkonsekvenser (DPIA) for sin respektive sektor.

Seksjonsleder for Digitale tjenester er fagansvarlig for informasjonssikkerhet, og skal kommunisere sikkerhetsrisikoer og sikkerhetstrusler til ledelsen og sørge for gjennomføring av beredskapsøvelser innen IT.

Teamleder teknologi og utvikling skal blant annet iverksette og følge opp tiltak som sikrer løpende teknisk drift av IT-løsningene, rådgi systemeiere og prosjektledere og sørge for at fylkeskommunens sikkerhetsarkitektur er definert og implementert i alle systemer og løsninger som omfattes av styringssystemet for informasjonssikkerhet. Teamleder teknologi og utvikling skal delta i endringsgjennomganger og forhandlinger om tjenestenivåavtale.

Sikkerhetsrådgiver merkantil skal overvåke fylkeskommunens informasjonssikkerhetsarbeid og rapportere dette videre til seksjonsleder digitale tjenester. Sikkerhetsrådgiver skal også sikre at fylkeskommunens styringssystem for informasjonssikkerhet er oppdatert, identifisere risikoområder, foreslå og gjennomføre sikringstiltak, bistå med faglig støtte på informasjonssikkerhetsområdet[8], sørge for at tiltakene i kompetanseplanen gjennomføres og holde beredskapsplan IT oppdatert.

Sikkerhetsrådgiver teknisk skal identifisere risikoområder og foreslå sikringstiltak, gjennomføre sikkerhetstiltak, utvikle, innføre og revidere sikkerhetspolicyer, bistå med faglig støtte og råd på informasjonssikkerhetsområdet, bistå i gjennomføring av risikovurderinger og databehandleravtaler ved anskaffelser og bidra i relevant opplæring.

Flere andre ansatte vil være involvert i informasjonssikkerhetsarbeidet, for eksempel i risikovurderinger og gjennomføring av sikkerhetstiltak.

[5] En beredskapskoordinator er en person som har ansvar for å planlegge, organisere og koordinere kommunens beredskapsarbeid.
[6] Personvernombudet er en del av sikkerhetsorganisasjonen, men med en rådgivende rolle.
[7] Det er en egen prosedyre for gjennomgangen som sier at styringssystemet for informasjonssikkerhet og personvern skal gjennomgås minst en gang i året i løpet av første kvartal, for å sikre at systemet er velegnet, tilstrekkelig og virkningsfullt. Dette vil bli gjort første gang i 2026.
[8] For eksempel gjennomføring av risikovurderinger og databehandleravtaler, også ved anskaffelser.

Personvernombud og personvernkoordinator
Personvernombudet skal

- informere og gi råd, kontrollere etterlevelsen av personvernregelverket, og på forespørsel delta i arbeid med DPIA. I tillegg være kontaktpunkt for Datatilsynet og de registrerte
- være uavhengig og skal ikke instrueres i sitt arbeid, og skal rapportere til øverste ledelsesnivå

Hver seksjon i fylkeskommunen har sin egen personvernkoordinator, noen seksjoner har flere, med følgende oppgaver:

- bidra til å sikre og dokumentere behandlingsaktivitetene i protokoll
- bidra til gjennomføring av risikovurdering (ROS) av informasjonssikkerheten- vurdere risiko og konsekvenser for behandling av personopplysninger
- bidra til å vurdere behov for og evt gjennomføring av personvernkonsekvensvurdering (Data Protection Impact Assessment - DPIA)
- bidra til at det settes i gang og gjennomføres nødvendige tiltak ved behandling av persondata (basert på risikovurdering nevnt over)
- bidra til at informasjonsplikten overfor den registrerte er oppfylt (personvernerklæringer)
- bidra ved henvendelser fra den registrerte knyttet til den registrertes rettigheter (innsyn, korrigering og sletting av personopplysninger ol)
- bidra ved implementering av overordnede rutiner knyttet til personvernregelverket i egen sektor (internkontroll)
- varsle personvernombudet når rutiner av betydning skal endres, eller nye it-systemer og sikkerhetstiltak skal utvikles/kjøpes inn

På tidspunktet for delingen var det få personvernkoordinatorer - de fleste koordinatorene som fylkeskommunen har i dag, er nye etter delingen.

Personvernombudet har etablert et nettverk for personvernkoordinatorene. I personvernombudets årsrapport rapporteres det om at nettverket i 2024 fikk grunnleggende opplæring og deltok i protokollarbeid, vi får opplyst at dette arbeidet har fortsatt i 2025.

Systemeier, prosesseier og systemanvarlig
Systemeier og prosesseier skal ha stillingsnivå fylkesdirektør, fylkessjef, virksomhetsleder, seksjonsleder eller teamleder.

Systemeier er den som har ansvar for et område på lavest mulig nivå iht. delegeringsreglementet. Følgende ansvar og oppgaver er plassert hos systemeier, jf. styringsdokumentet:

- sørge for at kravene til informasjonssikkerhet for systemet er definert, og sikre at disse kravene er innlemmet i systemet
- sørge for at kravene til informasjon som blir behandlet i systemet er definert, og sikre at disse kravene er innlemmet i systemet
- signere databehandleravtale

- påse at egen rolle, samt rollene systemansvarlig, og minst én prosesseier er avklart og dokumentert i protokoll og systemoversikt

Prosesseier skal sikre at behandlingen av personopplysninger som gjennomføres i prosessen skjer i samsvar med personvernregelverket. Prosesseier skal sørge for

- risikovurdering og vurdere behov for å vurdere personvernkonsekvenser (DPIA)
- at databehandleravtale kontrolleres og utpeke nødvendige ressurser til dette
- at databehandleravtalen kontrolleres evt justeres, dersom systemet finnes fra før, slik at det har korrekt informasjon om hva slags type data som behandles
- at prosessen dokumenteres i protokoll
- etablere og vedlikeholde policyer og prosedyrer for sine fagområder
- utpeke en systemansvarlig

Prosesseier er den som eier behandlingen som omhandler personopplysninger. Ett fagsystem kan ha flere prosesseiere, fordi et system gjerne brukes av flere deler av organisasjonen. En prosess kan også involvere flere fagsystemer, f.eks. tannhelsehjelp hvor seks ulike fagsystemer benyttes til ulike formål.

Systemansvarlig skal sørge for konfigurering, tilgangsstyring, at systemet er dokumentert i programvare/systemoversikt og gjennomføre risikovurderinger av systemet. Systemansvarlig skal ha inngående kjennskap til og daglig oppfølging av systemet.

Personvernombudet mener det fremdeles er behov for ytterligere opplæring av ledere for å bevisstgjøre og forankre disse ansvarsområdene. Når de siste styringsdokumentene på området er godkjent, er det planlagt opplæring av ledere i henhold til årshjulet[9].

Oversikt over programvare og systemeiere
Telemark fylkeskommune har oversikt over systemeiere og systemansvarlige i Programvareoversikten og GRC-verktøyet. Det arbeides med å oppdatere disse oversiktene, og det er mye etterslep etter fylkesdelingen. Med unntak av utdanning, er det i løpet av revisjonsperioden nesten ferdig ryddet i Programvareoversikten, med systemeiere og systemansvarlige på plass. Utdanning har betydelig mer programvare og tjenester enn de andre sektorene, og dermed er det mer krevende å kartlegge. Prosesseiere vil etter hvert bli dokumentert i GRC-verktøyet i forbindelse med protokollføring (se pkt. 2.3).

Ledere med personalansvar og ansatte
Ledere med personalansvar har også en rolle i informasjonssikkerhet og personvernsarbeidet. De skal sikre at de ansatte har grunnleggende forståelse for informasjonssikkerhet, er kjent med

[9] Fylkeskommunens årshjul for informasjonssikkerhet og personvern er beskrevet lenger ned i dette kapittelet.

gjeldende policyer og prosedyrer, har lest, forstått og skrevet under sikkerhetsinstruksen og at de vet hvordan de melder inn avvik/sikkerhetsbrudd.

Sikkerhetsinstruksen er en del av Telemark fylkeskommunes arbeid med informasjonssikkerhet og personvern. Innen 1. september 2025 skal alle ansatte ha signert instruksen. Status i oktober[10] er at det mangler signering fra i ca. 500 av ca.1800 ansatte. Fylkeskommunen vil sende ny påminnelse om å følge opp dette til ledere i starten av november. Etter hvert skal det også sendes ut et digitalt kurs der ansatte minnes på å signere og fremover skal instruksen være en del av arbeidsavtalen. Målet med instruksen er at ansatte skal ha oversikt over sitt ansvar ved behandling av informasjon i Telemark fylkeskommune[11]. Instruksen omhandler følgende tema:

- Informasjon: tilgang til informasjon og klassifisering av informasjon
- Digitale enheter og systemer: bruk av fylkeskommunens IT-utstyr, programvarer, tjenester på internett, e-post, brukernavn og passord, lagringsområder og flyttbare lagringsmedier.
- Fysisk sikkerhet: adgangskort, besøk i fylkeskommunens lokaler, fotografering og arbeidsplass
- Kompetanse
- Varslingsplikt
- Konsekvenser ved brudd på sikkerhetsinstruksen
- Arbeidsgivers rett til overvåkning og kontroll
- Arbeidsgivers rett til innsyn

Alle ansatte skal lese, signere og følge sikkerhetsinstruksen og annen opplæring, samt være oppmerksom på informasjonssikkerhetsrisikoer i sitt daglige arbeid, og melde fra ved mulige sikkerhetshendelser.

IT-tjenesteansvarlig og Servicedesk

IT-tjenesteansvarlig skal blant annet utarbeide og ajourholde driftsdokumentasjon[12], gjennomføre oppdateringer og vedlikehold av systemet, tekniske avklaringer i forhold til kravspesifikasjonen for programvare og maskinvare, sørge for at brukerne får tilgang, gjennomføre og bistå i risikovurderinger og teknisk drifte systemer. Teknisk drift innebærer blant annet oppgraderinger, sikkerhetskopiering og testing.

IT-tjenesteansvarlig skal også overvåke og administrere systemytelsen, sikkerheten og tilgjengeligheten, og iverksette tiltak for å løse eventuelle problemer eller avvik.

Servicedesk skal gi veiledning og brukerstøtte til ansatte, elever og eksterne, knyttet til informasjonssikkerhet, inkludert svare på spørsmål rundt tilganger og bruk av passord. De skal

[10] 16.10.25
[11] Sikkerhetsinstruksen er et ACOS-skjema som skal signeres digitalt. Dokumentet blir lagret i de ansattes personalmappe. Instruksen vil blir også lagt inn som en del av ansettelsesprosessen for nyansatte.
[12] Dokumentasjon av integrasjoner med andre IT-tjenester

også autentisere ansatte, elever og eksterne som ber om tilganger, passordbytte eller låse opp kontoer.

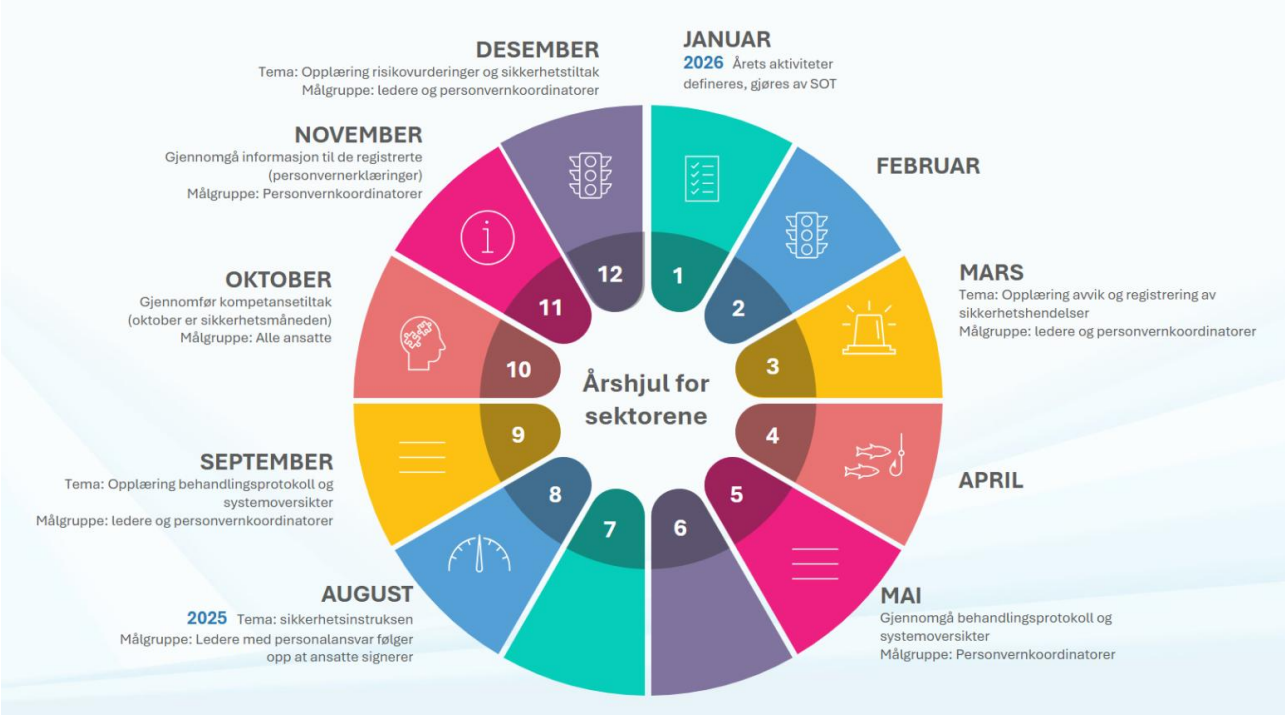
Styringsdokumenter og rutiner

Fylkeskommunen har en policy for kompetanseplan for informasjonssikkerhet og personvern fra juni 25. Denne tar utgangspunkt i kompetansekravene som kan utledes av personvernsforordningen, ISO 27001[13] og NIS2[14]. HR-leder skal samarbeide med seksjonsleder Digitale tjenester for å lage årlig kompetanseplan som fastsetter kompetansetiltak, når det skal gjennomføres og hvem som er ansvarlig. Styringsdokumentet er delt opp med forslag til temaer for ledere, for sikkerhetspersonell og personvernkoordinatorer og for ansatte. Eksempler på kompetansetiltak er opplæring av nyansatte, årlige oppdateringer, e-læring, medarbeidersamtaler og bevissthetstrening. En årlig kompetanseplan vil lages fra 2026, basert på risikovurderinger, avviksstatistikk, kartlegginger av trusselsituasjoner, revisjoner m.v.

Det følger videre at det skal etableres en metode for å måle at kompetansen faktisk blir høyere over tid, og at vurderinger av kompetansebehov og -resultater bør innlemmes i ledelsens gjennomgang.

Det fremgår av kompetanseplanen at det hvert år skal utarbeides et årshjul. Temaene vil variere på bakgrunn av behov og gjeldende trusselbilde. Det første årshjulet i Telemark fylkeskommune gjelder fra august 2025 til mai 2026, det viser hvordan arbeidet med informasjonssikkerhet og personvern er fordelt utover året. Det beskriver ulike aktiviteter og målgruppe for aktiviteten. Arbeid med å føre behandlingsprotokoller og gjennomføring av risikovurderinger, er løpende oppgaver som gjøres hele året. Det er sikkerhetsorganisasjonen som setter aktivitetene for året.

[13] Den internasjonale standardiseringsorganisasjonen ISO (International Organization for Standardization) utvikler standarder for de fleste sektorer. ISO 27001 er standarden som fylkeskommunens styringssystem for informasjonssikkerhet er basert på, den spesifiserer kravene for å etablere, implementere, vedlikeholde og kontinuerlig forbedre et styringssystem for informasjonssikkerhet.
[14] NIS2 er et EU-direktiv som vil bli innlemmet i digitalsikkerhetsloven, og som fokuserer på å styrke cybersikkerheten og øke motstandsdyktigheten for viktige enheter. NIS2 stiller for øvrig krav til at ledelsen skal gjennomføre kompetansetiltak.



Bilde 1. Telemark fylkeskommune sitt årshjul for informasjonssikkerhet og personvern 2025-2026.

Ansvar og myndighetsfordeling - praksis

Styringssystemet med tilhørende styringsdokumenter for roller, ansvar og kompetanse er som nevnt nytt av 2025. Arbeidet med implementering og opplæring er derfor nylig startet når denne forvaltningsrevisjonen gjennomføres, og fylkeskommunen opplyser at styringssystemet ikke er forankret ute i organisasjonen enda. Sikkerhetsrådgiver merkantil forteller at det skal komme opplæring til lederne iht. årshjulet i september og desember 2025, hvor informasjon om nye roller og ansvar sannsynligvis vil inngå.

Praksis ved tannklinikkene

Det er etablert et samarbeid mellom Telemark fylkeskommune og Vestfold fylkeskommune om felles journalsystem for tannhelse til minst 2028. Bakgrunnen for samarbeidet er at det ble utført en ekstern ROS-analyse av å splitte systemet da fylkeskommunen skulle deles. Analysen viste at en oppsplitting ville utgjøre en risiko for pasientsikkerheten. Det foreligger en avtale om rollefordeling mellom fylkeskommunene, med Vestfold fylkeskommune som teknisk driftsansvarlig. Den tekniske driften ivaretas av to rådgivere i Vestfold fylkeskommune. Telemark fylkeskommune har faste ukentlige møter med rådgiverne i Vestfold, og dette samarbeidet fungerer godt får vi opplyst. Hvert fylke har i tillegg en egen systemadministrator og en back-up/superbruker. Disse innehar

tannhelsefaglig kompetanse, og har ansvar for forvaltning av systemet[15], gjennomfører risikovurderinger og utarbeider retningslinjer for bruk.

Seksjonsleder for tannhelse og personvernkoordinator i seksjonen opplever at ansvars- og myndighetsfordelingen knyttet til informasjonssikkerhet og personvern er klar og tydelig – både for dem selv, seg imellom og i forhold til personvernombudet. Det innebærer bla. ansvar for protokollføring, risikovurderinger, databehandleravtaler og DPIA. De nye rollebetegnelsene og beskrivelsene er imidlertid ikke godt kjent eller implementert ennå, ettersom dette er nytt fra sommeren 2025.

Personvernkoordinatoren påpeker at rollen, til tross for en tydelig ansvars- og myndighetsfordeling, er krevende. Rollen som personvernkoordinator skal ivaretas av rådgiver for elektronisk pasientjournal[16], som også har mange andre oppgaver, og som i hovedsak har tannhelsefaglig bakgrunn. Behovet for å arbeide med personvern er «utømmelig», og det tar tid å bygge opp nødvendig kompetanse. Personvernkoordinatoren deltar i nettverket sammen med øvrige personvernkoordinatorer og personvernombud, noe som er nyttig, men det er fortsatt en utfordring at seksjonen ikke har tilstrekkelig kapasitet eller ressurser på området. Det er heller ikke en egen sjekkliste for hva personvernkoordinator skal kunne. Seksjonsleder forteller at det er vanskelig å gi nødvendig støtte og veiledning til rollen. Det finnes et generelt mandat for personvernkoordinatorer, og personvernombudet tilbyr støtte og veiledning til den som ber om det.

Seksjonsleder for tannhelse og personvernkoordinator i seksjonen forteller at de ansatte i utgangspunktet har en underliggende bevissthet rundt informasjonssikkerhet og personvern. Det skyldes blant annet at det er mye fokus på taushetsplikt og pasientsikkerhet både i utdanningen og i opplæringen i seksjonen. Sikkerhetsrådgiver merkantil har også lagt merke til en større bevissthet rundt informasjonssikkerhet og personvern i denne seksjonen ifm. avviksrapportering.

Seksjonen Tannhelse har utarbeidet et eget e-læringskurs for informasjonssikkerhet i tannhelse, med følgende innhold:

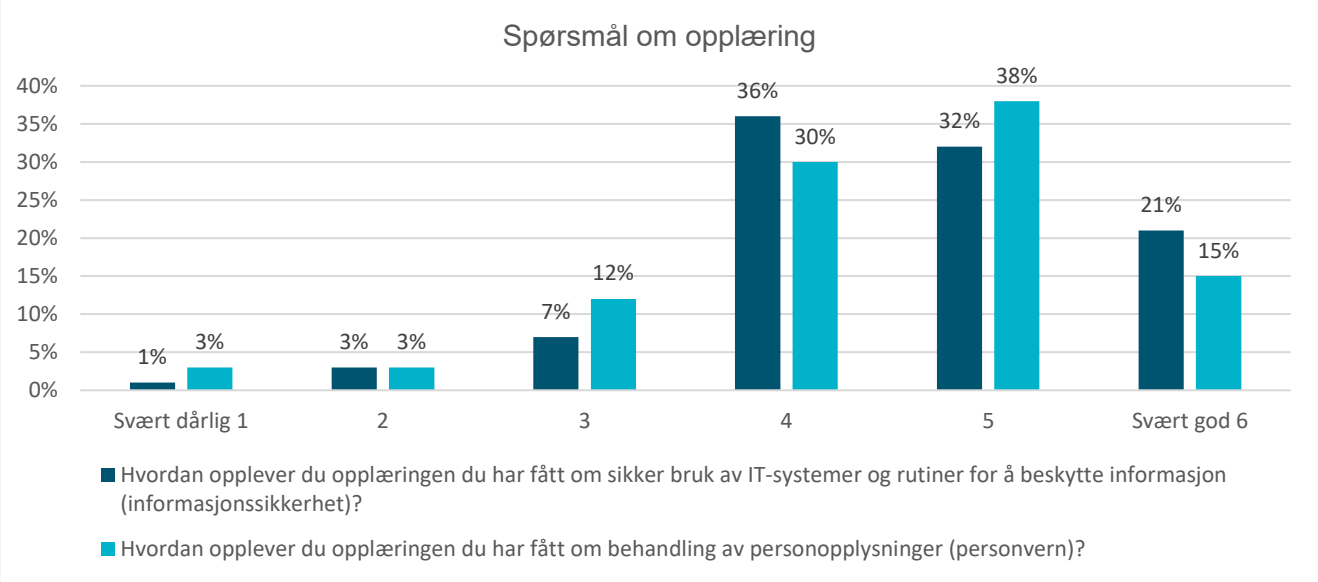
- informasjonssikkerhet i tannhelse, bla. den ansattes ansvar for informasjonssikkerhet
- personopplysninger, inkl. den registrertes rettigheter
- taushetsplikt og samtykke
- sikkerhetstiltak på pc, e-post og SMS
- avvik
- multiple choice-test fra kursinnhold om informasjonssikkerhet og personvern

Vi får opplyst at kurset skal sendes ut årlig. Kurset ble ikke sendt ut i 2024, men ble sendt ut i februar 2025. Pr august 2025 er det 33% som ikke har fullført noe av kurset, 9% har fullført noe og

[15] Gir brukerstøtte, styrer tilgangene, tester nye versjoner, håndterer alt som gjelder grensesnittet og brukernes aktiviteter i systemet inkludert økonomi, statistikk, forhåndslagrede tekster og logging.
[16] Stillingen er under ansettelsesprosess. Nåværende personvernkoordinator som er intervjuet har rollen midlertidig, ved siden av sin fulle alminnelige stilling.

58% har fullført alt. For å få kurset godkjent som fullført, må hele kurset gjennomgås og 70% av spørsmålene underveis må besvares korrekt. Klinikkleder skal sikre at ansatte ved klinikken har gjennomført kurset. Det blir sendt purringer direkte til de som ikke har gjennomført, og gitt beskjed til klinikkledere dersom det er lav gjennomføring hos deres ansatte.

Vi har spurt de ansatte ved klinikkene hvordan de opplever opplæringen de har fått om informasjonssikkerhet og personvern.[17] De aller fleste opplever denne som god, både for informasjonssikkerhet og personvern.



Figur 1. N=76.

Vi har bedt de ansatte ved tannklinikkene om å ta stilling til ulike påstander om ansvar og oppgaver knyttet til behandling av personopplysninger. De ansatte svarer gjennomgående positivt (gjennomsnitt på 5 og 6 som vil si helt enig eller enig) på alle påstandene. Det er liten spredning i svarene, slik at de aller fleste som har svart, er enige med hverandre.

Påstander	Gjennomsnitt	Standardavvik
Det er klart og tydelig hva som er mitt ansvar ved behandling av personopplysninger	5	1
Jeg vurderer alltid hvilke pasientopplysninger som er nødvendige å dokumentere	5	1
Jeg begrenser nedtegnelse av personopplysninger til det som er nødvendig	5	1
Jeg låser alltid datamaskinen når jeg forlater den, selv for kort tid	5	1
Jeg logger ut av journalsystemer og andre relevante systemer når jeg er ferdig med dem	6	1

[17] Spørreundersøkelse – se vedlegg 3 Metode for mer informasjon

Påstander	Gjennomsnitt	Standardavvik
Jeg sender ikke pasientopplysninger via usikret e-post eller andre usikrede kanaler, med mindre opplysningene er anonymisert og situasjonen er akutt og nødvendig for at pasienten skal få forsvarlig hjelp	6	1
Jeg følger rutinene for å bekrefte pasientens identitet før jeg deler informasjon	6	1
Jeg opplever at klinikken har gode rutiner for å håndtere personopplysninger	5	1
Jeg har deltatt på E-læringskurs i "informasjonssikkerhet og personvern" det siste året	5	1,5
I alt behandles personopplysninger slik at integritet, konfidensialitet og tilgjengelighet beskyttes ved klinikken	5	1

Tabell 1. Ansatte ved tannklinikkenes svar på ulike påstander. Skala helt uenig (1) – helt enig (6). N=76.

Praksis ved skolene

Team skoleutvikling har to personvernkoordinatorer og en digitalrådgiver. Rollen som koordinator kommer i tillegg til andre arbeidsoppgaver. Det løftes frem at andre arbeidsoppgaver utfordrer kontinuitet og god oppfølging på personvernområdet, at det er behov for mer profesjonalisering av koordinatorrollen, med klar ressursbruk og avklart mandat til å handle og gjennomføre prosesser.

Personvernkoordinatorene opplever at samarbeidet fungerer godt, og at det i hovedsak er en klar og tydelig fordeling av ansvar og oppgaver. Rådgiver i team skoleutvikling mener at det er en delvis klar og tydelig ansvarsfordeling mellom skolesektoren og støttetjenester som personvernombudet. Vi får også opplyst at det er uklar ansvarsfordeling mellom leder og rådgivernivå i skolesektoren, men dette har vært i prosess. Oppgavene det dreier seg om er protokollføring, risikovurderinger, databehandleravtaler og DPIA.

Rådgiver i team skoleutvikling mener at det er noe mangelfull opplæring for ansatte i administrasjonen, men at fylkeskommunen har utfyllende og gode ressurssider på intranett. Utfylling i GRC-verktøyet er også en form for løpende opplæring. En personvernkoordinator ønsker mer opplæring rundt prosesser for anskaffelse og sikkerhet. God kompetanse blir lagt frem som en forutsetning for at team Skoleutvikling skal kunne bistå med tilrettelegging av opplæring for ansatte i skolene.

De to rektorene vi har intervjuet ved Nome og Porsgrunn videregående skoler er ikke kjent med at de har fått ansvar og oppgaver ifm. protokollføring, risikovurderinger, databehandleravtaler og DPIA. Vi får opplyst at dette ansvaret ble presentert for rektorer og administrasjonsledere i september 2025.

I 2024 fikk skolene i Telemark fylkeskommune tilgang til et verktøy som kalles samskrivningsløsninger for elevoppfølging. Dette er en egen utviklet løsning for at ansatte med tjenstlig behov skal kunne sikre at informasjon som er vesentlig for sosial og pedagogisk oppfølging av eleven blir nedtegnet, og at informasjonen er tilgjengelig for andre ansatte med tjenstlig behov. Løsningen er innebygd i Teams, og har ekstra tekniske sikkerhetsmekanismer for å ivareta personvernet til elever. Ledelsen ved de to skolene er svært positive til løsningen. Vi ser

av vår spørreundersøkelse det er stor enighet blant de ansatte (70%) om at løsningen gir enkel tilgang til nødvendig elevinformasjon som trengs for å kunne tilpasse opplæringen til den enkelte elev.

De aller fleste (87%) mener samskrivningsløsningen i svært stor, stor eller noe grad brukes på en slik måte at personvern ivaretas. Der er likevel 13% som mener at personvernet ikke blir godt nok ivaretatt. Det er 6 av 70 respondenter som oppgir at de har tilgang til løsningen selv om de i svært liten grad eller i liten grad har tjenstlig behov for det. Det er delte meninger om opplæringen i samskrivningsløsningen. En betydelig andel på 37 % mener de ikke har fått god opplæring før eller samtidig som de tok i bruk løsningen. Det er videre 34 % som har lite kjennskap til innholdet i rutinen for samskrivningsløsningen.

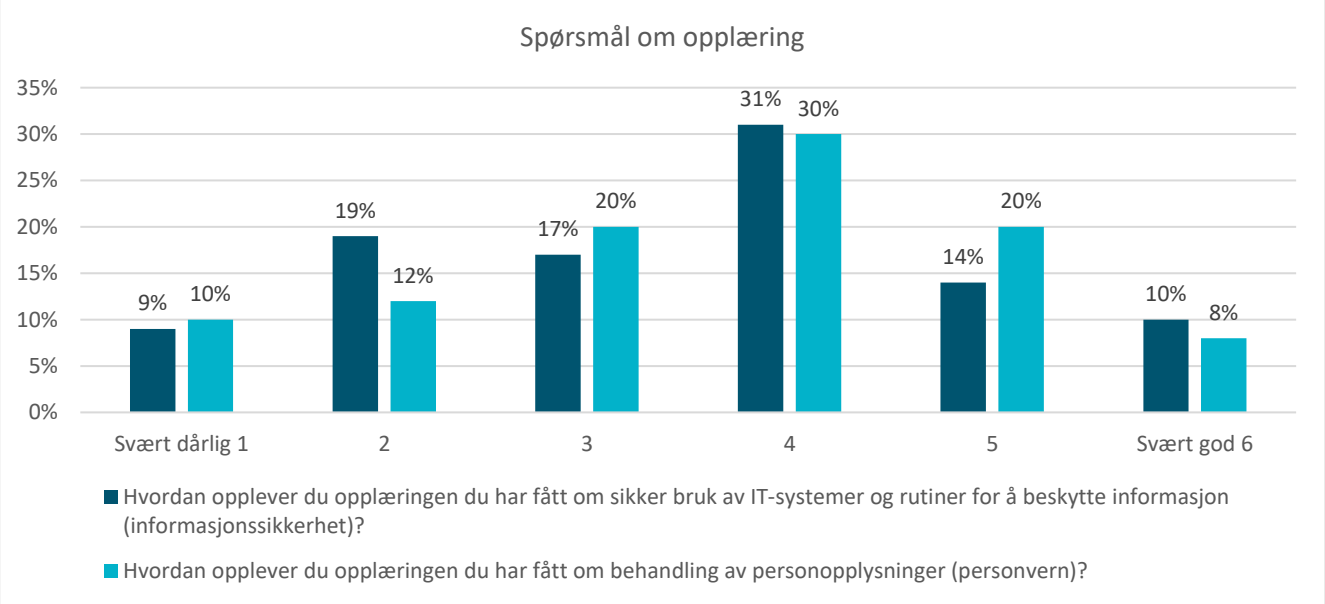
Svaralternativer	Opplæring - samskrivingslønsing	Kjennskap til rutinen for samskrivningsløsningen
I svært liten grad 1	19%	13%
2	11%	11%
3	7%	10%
4	14%	14%
5	29%	27%
I svært stor grad 6	20%	24%

Tabell 2. Svar på påstandene «Jeg har fått god opplæring i bruk av samskrivningsløsningen før eller samtidig med at løsningen ble tatt i bruk» og «Jeg er kjent med innholdet i rutinen for samskrivningsløsningen». N=70.

Rutiner for samskrivningsløsningene ligger på intranettet. Her står det at det årlig skal gjøres risiko- og sårbarhetsanalyser (ROS-analyse) på den enkelte skole, og at ansvaret for dette er lagt til rektorene. Løsningen er tatt i bruk ved de undersøkte skolene skoleåret 2025-2026, men det er ikke kjent for rektorene at den enkelte skole skal gjennomføre ROS-analyse av løsningen.

Rektorene opplever at ansvar og oppgaver for å ivareta personvern i det daglige på skolene er klare og tydelig, men at det er behov for mer opplæring blant de ansatte, f.eks. om legeerklæringer, avvik og generelt sikre at ansatte faktisk har lest og forstår rutiner om personvern. En av skolene løfter som en utfordring at skolene ikke har et eget journalsystem, og at dette utgjør en risiko for manglende dokumentasjon, at personopplysninger er spredt flere steder uten at man har oversikt og at opplysninger ikke er tilgjengelige, sikker deling av opplysninger med andre samarbeidsaktører og myndigheter og ifm. innsynsbegjæringer. Vi ser av vår spørreundersøkelse at ansatte lagrer flere av de samme type personopplysningene på mange ulike steder, f.eks. lagres elevsamtaler: i arkivet (20%), på papir innelåst (19%), i InSchool (18%), i samskrivningsløsning (10%), samt på papir ikke innelåst (7%) og på egen OneDrive (12%). Legeerklæringer lagres i hovedsak i arkivet (46%), men en del oppbevarer også dette på papir nedlåst (23%), på papir ikke nedlåst (13%) og på egen OneDrive (3%). Også for referater fra samarbeidsmøter om elever, prøve og eksamensresultater og løpende faglige og sosiale opplysninger om elever, ser vi en spredning i hvor ting lagres. Det er 13% som lagrer andre sensitive opplysninger om en bestemt elev på egen OneDrive, på papir ikke innelåst og i e-post.

Det er ikke utarbeidet eget e-læringskurs om informasjonssikkerhet eller personvern for skolene, slik det er for tannklinikkene. Vi har spurt de ansatte ved skolene hvordan de opplever opplæringen de har fått om informasjonssikkerhet og personvern. En betydelig andel på 45% for informasjonssikkerhet og 42% for personvern svarer negativt, at de opplever den som svært dårlig, dårlig eller noe dårlig.



Figur 2. N=93.

Rutinen for hvordan personvern skal ivaretas på skolene er innarbeidet i øvrige rutiner fylkeskommunen har for elevoppfølging. I gjennomsnitt svarer ansatte at de i noen grad kjenner til rutiner for hvordan man behandler personopplysninger. Det er likevel en betydelig spredning i hvor god kjennskapen er. Som nevnt er fylkeskommunens generelle rutiner om informasjonssikkerhet og personvern nye av sommeren 2025, men vi ser likevel at en del ansatte i skolen allerede kjenner noe til disse. Det er kun en liten andel på 13 % som mener rutiner for informasjonssikkerhet og personvern er til hinder for god elevoppfølging.

Svaralternativer	Kjennskap til rutiner for elev-oppfølging om personopplysninger	Kjennskap til ressurssidene på intranett om informasjonssikkerhet og personvern
Kjenner ikke til 1	9%	16%
2	13%	16%
3	23%	29%
4	25%	23%
5	20%	12%
Svært godt 6	11%	4%

Tabell 3. Svar på påstandene «Rutiner for elevoppfølging som gjelder hvordan man behandler personopplysninger» og «Ressurssidene på intranett (Innsida) om informasjonssikkerhet og personvern som ble revidert like før sommeren 2025». N=93.

En rektor trekker frem at skolen har et forbedringspotensial med å sikre at tilgjengelige rutiner leses og forstås. Det blir likevel sagt at det er vanskelig å gi opplæring som er balansert til de ulike ansattes nivå.

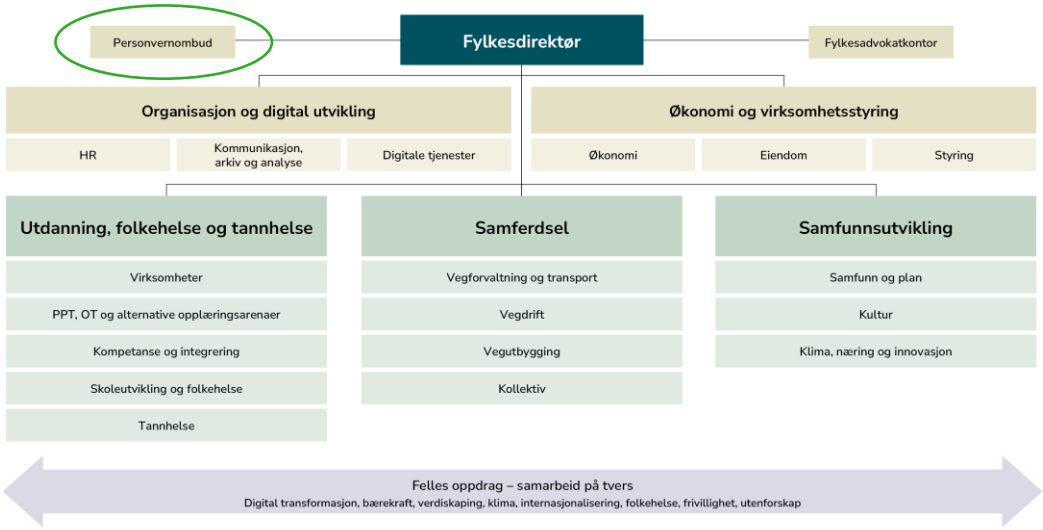
Vi har bedt de ansatte ta stilling til noen påstander om eget ansvar og praksis ved behandling av personopplysninger. Det svares med enighet positivt (gjennomsnitt på 4 og 5 som vil si enig eller helt enig) på alle påstandene. Det er liten spredning i svarene, det vil si at de aller fleste som har svart er enige med hverandre.

Påstander	Gjennomsnitt	Standardavvik
Det er klart og tydelig hva som er mitt ansvar ved behandling av personopplysninger	4	1
Det er klart og tydelig hva som er ledelsen, administrasjonens og lærernes ansvar ved behandling av personopplysninger	4	1
Jeg vurderer alltid hvilke personopplysninger som er nødvendige å dokumentere	5	1
Jeg begrenser nedtegnelse av personopplysninger til det som er nødvendig	5	1
Jeg føler meg trygg på hvordan jeg skal dokumentere elevopplysninger samtidig som personvernreglene blir ivaretatt	5	1
Jeg låser alltid datamaskinen når jeg forlater den, selv for kort tid	5	1
Jeg sender ikke helseopplysninger eller sensitive opplysninger om en elev på epost	5	1
Jeg har ikke problemer med å finne nødvendig informasjon om elever for å utføre mitt arbeid	4	1,5
Ivaretakelse av personvern diskuteres i profesjonsfellesskapet jeg deltar i (f.eks. møter)	4	1
Jeg opplever at skolen har gode rutiner for å håndtere personopplysninger	4,5	1
Alt i alt behandles personopplysninger ved skolen slik at integritet, konfidensialitet og tilgjengelighet beskyttes	5	1

Tabell 4. Ansatte ved skolene svar på ulike påstander. Skala helt uenig (1) – helt enig (6). N=93.

2.1.2. Rapportering – data

Personvernombudet skal rapportere til øverste ledelsesnivå, jf. stillingsinstruksen og fylkeskommunens rolle- og ansvarsbeskrivelse for personvernombudet. Personvernombudets årsrapport skal inngå i den årlige gjennomgangen, jf. prosedyre for ledelsens gjennomgang. Personvernombudet er plassert i en egen enhet, hvor kun personvernombudet sitter, direkte under fylkesdirektøren. Personvernombudet forteller at organiseringen av rollen bidrar til en naturlig rapportering til fylkesdirektøren.



Bilde 2. Telemark fylkeskommune sitt organisasjonskart. Personvernombudet er ringet rundt.

Personvernombudets årsrapport for den nye Telemark fylkeskommune ble lagt frem for fylkesdirektørens ledergruppe i januar 2025 for 2024. Rapporteringen fremgår også av Telemark fylkeskommune sin årsrapport for 2024. Rapportering gjennom egen årsrapport på området ble også gjort i tidligere Vestfold og Telemark fylkeskommune.

Rapporten for 2024 starter med å vise til anbefalinger gitt i Personvernombudets årsrapport for Vestfold og Telemark fylkeskommune for 2023. Anbefalingene dreide seg om å begynne arbeidet med å få på plass overordnede styringssystem for etterlevelse av personvernregelverket, prioritere arbeidet med behandlingsprotokoller, etablere felles metode, rutiner, tiltak og opplæring i gjennomføring av risikovurderinger, evaluere ansvaret for leverandøroppfølging av databehandleravtaler, fortsette arbeidet med opplæring og bevisstgjøring om å melde avvik innen personvern og informasjonssikkerhet, sette av ressurser til arbeidet og innføre obligatorisk opplæring innen personvern og informasjonssikkerhet for alle ledere og ansatte.

Personvernombudet trakk frem disse anbefalingene om ressurser:

- Å gi ressurser til fagansvaret for personvern, som er lagt til fylkesadvokaten i Telemark.
- Å sette av ressurser til personvernarbeidet da det er fortsatt et stort etterslep
- En satsing på personvernkoordinatorer i sektorene - at alle sektorer får personvernkoordinatorer, og at disse får tilbud om opplæring i personvern og får avsatt tid til personvernarbeid.
- Etablere personvernkoordinator på hver videregående skole.

Nåværende personvernombud rapporterer på status for disse områdene. Det er rapportert om status i arbeidet med å få et kvalitetssystem for informasjonssikkerhet og personvern, etablering av en sikkerhetsorganisasjon og godkjenning av styrende dokumenter. Et års-hjul var også under planlegging ved utgangen av 2024.

Anskaffelsen av GRC-verktøyet er omtalt, og det rapporteres også om at personvernombudet deltar i arbeidet med kvalitetssystem for fylkeskommunen.

Det rapporteres om samarbeidsarenaer med og opplæringstiltak for personvernkoordinatorene, og pekes på at koordinatornettverket må videreutvikles, samt at koordinatorenes rolle er en viktig suksessfaktor ute i virksomheten. Det var regelmessig møter mellom personvernombudet og koordinatorene i 2024[18], mange møter handlet om opplæring. Ombudet inviterte også koordinatorer med i protokollmøter[19] som gir praktisk læring. Det er et mål at flere av koordinatorene skal ta en aktiv rolle i slike møter. Opplæring er på agendaen i 2025.

Ombudet hadde også opplæring med alle lederne i de ulike seksjonene og seksjonene i fylkeskommunen i løpet av 2024.

Rapporteringen beskriver status for arbeidet med behandlingsprotokoller, risikovurderinger, leverandøroppfølging og avvikshåndtering. Vi vil beskrive det som kommer frem fra rapporteringen om hvert tema der dette er relevant (se kap. 2.3, 2.4, 2.6 og 2.8.)

Til slutt gir personvernombudet følgende anbefalinger for 2025:

- Delta i / støtte innføringen av kvalitetssystemer.
- Når det nye støtteverktøyet er innført, ha status- og dialogmøter om kvalitetssystemet og støtteverktøyet i sine ledergrupper sammen med koordinator, informasjonssikkerhetsrådgiver og personvernombud
- Støtte sine koordinatorer og anbefale dem og andre medarbeidere å stille opp på protokollmøter og risikovurderinger, inkludert opplæring.
- Støtte at opplæringstiltak settes i en organisatorisk ramme – ikke bare som løsrevne tilbud fra enkeltpersoner
- Etablere personvernkoordinator også ved hver VGS - med innføring av kvalitetssystem og støtteverktøy bør tiden være moden for det.

2.1.3. Revisors vurdering av organisering og rapportering

Fylkeskommunen har gjort et omfattende arbeid for å etablere et styringssystem for informasjonssikkerhet og personvern. Med det nye styringssystemet med tilhørende styringsdokumenter for roller, ansvar og kompetanse knyttet til informasjonssikkerhet og personvern, har fylkeskommunen i hovedsak klar og tydelig beskrivelse av roller og ansvar for personvern. Implementering av systemet startet i siste halvdel av 2025. Styringssystemet er godt forankret i virksomhetens ledelse, både når det gjelder etablering, vedlikehold og rapportering.

[18] Annenhver uke, med ulike temaer og learning by doing workshops.
[19] Møter for å fylle ut behandlingsprotokoll.

Innenfor tannhelse er ansvar og myndighet for behandling av personopplysninger klart plassert. Opplæringen i informasjonssikkerhet og personvern til de ansatte framstår som et godt tiltak, men det synes å være behov for mer opplæring og ressurser sentralt til personvernkoordinator.

Ansvars- og myndighetsfordelingen oppfattes ikke like klar innenfor skoleområdet. Behov for ressurser til rollen som personvernkoordinator spesielt knyttet til databehandleravtaler, samt tydeligere mandat og opplæring for å kunne utøve rollen, blir tatt opp innenfor skoleutvikling. Det er ikke utarbeidet et eget opplæringsprogram i informasjonssikkerhet og personvern til de ansatte i skolen, slik som i tannhelse. Intervju og spørreundersøkelse indikerer et behov for mer opplæring.

Vi ser at ansatte i skolen lagrer flere av de samme type personopplysningene på mange ulike steder, inkludert steder det ikke skal lagres. Vi mener det er risiko for at skolene ikke ivaretar godt nok personvernsprinsippene for lagringsbegrensning og tilgjengelighet for personopplysninger.

Samskrivningsløsningen er ny, og synes å ivareta personvern på en god måte. Løsningen har likevel særlig risiko knyttet til seg[20] (se også kap 2.5), og kontinuerlig opplæring og fokus på ivaretakelse av personvern i løsningen er viktig. En betydelig andel (37%) av de som har svart at de har tilgang til løsningen, mener at de i liten grad har fått god opplæring før eller samtidig som de tok i bruk løsningen. Det samme gjelder kjennskap til rutinen for samskrivningsløsningen (34%).

Rapportering
Fylkeskommunen har rutiner og tiltak for rapportering til ledelsen. Personvernombudets rolle og stillingsinstruks innebærer rapportering til øverste ledelsesnivå. Personvernombudet utarbeider en årsrapport som gir informasjon om status, utfordringer og tiltak, og i henhold til ny prosedyre skal personvernombudets årsrapport fra 2026 inngå i ledelsens årlige gjennomgang.

2.2. Personvernombud i Telemark fylkeskommune

Telemark fylkeskommune skal ha personvernombud, organisert i samsvar med personopplysningsloven.

Nåværende personvernombud har hatt rollen siden februar 2024, omtrent samtidig som den nye fylkeskommunen ble opprettet. Personvernombudet er ansatt som personvernombud i 100 % stilling. Personvernombudet er innplassert som en selvstendig uavhengig funksjon direkte under fylkesdirektør (se organisasjonskart i kap 2.1.2). Personvernombudet er jurist og ingeniør, og har tidligere jobbet som personvernombud på et universitet.

Beskrivelse av rollen som personvernombud i fylkeskommunen ligger på intranettet. I tillegg har personvernombudet en egen stillingsinstruks fra februar 2024. Det står at personvernombudet selv

[20] Løsningen brukes til behandling av personopplysninger for å evaluere læring, mestring og trivsel i skoler (Sårbare registrerte og systematisk monitorering.) og fremgår dermed av Datatilsynets liste over behandlingsaktiviteter som alltid krever at det gjennomføres en DPIA.

har fagansvaret for egen oppgaveløsning innen personvern, at rollen skal være uavhengig, ikke instrueres i sitt arbeid og skal rapportere til øverste ledelsesnivå.

Det er beskrevet at rollen skal informere og gi råd til hele virksomheten og dens ansatte, kontrollere etterlevelsen av personvernregelverket, og på forespørsel delta i arbeid med DPIA. Personvernombudet skal ved utførelsen av sine oppgaver ta behørig hensyn til risikoene forbundet med behandlingsaktivitetene, i det det tas hensyn til behandlingens art, omfang og sammenhengen den utføres i. Det står også at personvernombudet ikke skal ha andre oppgaver eller ansvar som gir interessekonflikter, og at dette er det behandlingsansvarlig eller databehandler sitt ansvar å sikre. Ombudet opplever selv at dette blir ivaretatt i praksis på en god måte, og at det er god lederstøtte for dette arbeidet.

Ombudet skal være kontaktpunkt for Datatilsynet og de registrerte, samt samarbeide med tilsynsmyndighetene. Informasjon om hvem som er personvernombud med kontaktinformasjon står både på fylkeskommunens intranett og den åpne nettsiden. Videre skal kontaktopplysningene til personvernombudet angis i behandlingsprotokollen og oppgis Datatilsynet[21].

Det står at personvernombudet kan utføre andre oppgaver og ha andre plikter, forutsatt at dette er forenlig med øvrige oppgaver, for eksempel at personvernombudet kan utarbeide protokoll over behandlingsaktiviteter. Personvernombudet opplyser at dette innebærer å bistå ledere og personvernkoordinatorer. Andre oppgaver er å utarbeide retningslinjer og policyer, opplæring av ansatte, koordinere fagnettverk for personvern i TFK, delta i nasjonalt nettverk for personvernombud og samarbeide internt om informasjonssikkerhet.

Vi har spurt ansatte ved tannklinikkene og skolene om de har vært i kontakt med personvernombudet eller personvernkoordinatorene i den undersøkte perioden. Omtrent 45 % ved tannklinikkene og 8% ved skolene svarer ja på dette, 40% ved tannklinikkene og 28% ved skolene svarer nei, men kjenner til hvordan de tar kontakt og 15 % ved tannklinikkene og 64% ved skolene svarer at de ikke kjenner til hvordan de tar kontakt ved behov. De aller fleste som har vært i kontakt med personvernombudet opplevde i stor/svært stor grad å få råd og veiledning.

Fylkeskommunen påpeker at mange problemstillinger vil løftes i linjen, og at ledere er godt kjent med at fylkeskommunen har et personvernombud, slik at problemstillinger knyttet til personvern vil nå frem til ombudet dersom det er nødvendig.

2.2.1. Revisors vurdering av personvernombudets organisering

Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner, dybdekunnskap om personopplysningsloven og praksis på området, samt evne til å utføre oppgavene. Personvernombudets relevante høyere utdanning og konkrete tidligere arbeidserfaring på området er egnet til å ivareta kompetansekravet.

[21] Artikkel 33 og 36.

Ansvarsområdene og rollen for personvernombudet er tydelig beskrevet i styringsdokumenter i tråd med personvernforordningen og veiledningen fra Datatilsynet. Revisjonen har ikke gitt indikasjoner på at praksisen avviker fra dette. Fylkeskommunens organisering av rollen og stillingsbeskrivelsen til rollen ivaretar også ombudets uavhengighet.

Det fremgår av personvernforordningen art. 38 nr.3 personvernombudet ikke kan avsettes eller straffes av den behandlingsansvarlige eller databehandleren for å utføre sine oppgaver. Vi har ikke sett at dette står uttrykt noe sted, og mener dette vernet med fordel kunne stått eksplisitt i beskrivelsene av ansvarsforholdet mellom personvernombudet og virksomheten.

Personvernombudets hovedoppgave er å gi råd om etterlevelse av personvernlovgivningen. Dette forutsetter at de ansatte vet hvordan de kan kontakte ombudet ved behov for råd, selv om problemstillingene også kan kanaliseres via linja/ledelsen. En stor andel ansatte ved de to undersøkte skolene kjenner ikke til dette.

2.3. Protokoll over behandlingsaktiviteter

Telemark fylkeskommune skal ha protokoll over hvilke personopplysninger fylkeskommunen behandler.

I Telemark fylkeskommune sin Policy for behandling av personopplysninger, godkjent februar 2025 fremgår det at:

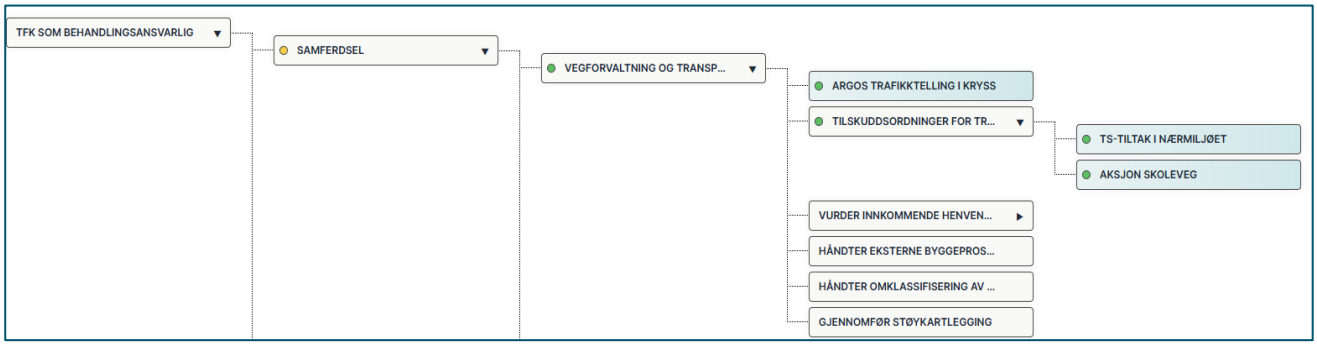
- Fylkeskommunen skal ha en oppdatert oversikt over alle behandlingsaktiviteter (behandlingsprotokoll). Når nye behandlingsaktiviteter starter opp, så skal aktivitetene registreres i protokollen. Det skal fremgå av protokollen om behandlingsaktiviteter er pågående eller avsluttede. For å sikre at protokollen er oppdatert, så skal den med jevne mellomrom gjennomgås og kvalitetssikres.
- Behandlingsprotokollen skal beskyttes med egnede sikkerhetstiltak, herunder beskyttelse mot uautorisert innsyn og uautoriserte endringer.
- Behandlingsprotokollen skal være komplett, i den forstand at det skal være mulig å ta ut en samlet liste over alle behandlingsaktiviteter som gjennomføres i fylkeskommunen. Behandlingsprotokollen skal på forespørsel utleveres til Datatilsynet. Protokollen skal kunne eksporteres i et lesbart og tilgjengelig format (som for eksempel PDF).
- Behandlingsprotokollen skal minimum inneholde informasjon spesifisert i artikkel 30, men kan utvides med mer informasjon dersom det vurderes som hensiktsmessig, som kartlegging av informasjonsverdier og lignende.

Det står også at fylkeskommunen skal definere gyldige rettslige grunnlag for alle behandlingsaktiviteter, og de rettslige grunnlagene skal dokumenteres i behandlingsprotokollen.

Policy for behandling av personopplysninger viser videre til dokumentet «roller og ansvar». Det er prosesseier (enten fylkesdirektør, fylkessjef, virksomhetsleder, seksjonsledere eller teamleder) som skal sørge for at behandlingsaktiviteten protokollføres/ dokumentere prosessen i protokoll.

Rollen som personvernkoordinator skal bidra til å sikre og dokumentere behandlingsaktivitetene i protokoll.

Telemark fylkeskommune benytter GRC-verktøyet å lage protokollen. I protokolloversikten skilles det mellom behandlinger hvor Telemark fylkeskommune er behandlingsansvarlig og der Telemark fylkeskommune er databehandler. Videre sortering i protokollen er gjort etter fylkeskommunens organisasjonskart, dvs. at behandlingsaktiviteter er sortert under hvilken sektor den hører hjemme og videre seksjon eller virksomhet.



Bilde 3. Utklipp fra Telemark fylkeskommune sin protokoll over behandlingsaktiviteter. Denne viser at Telemark fylkeskommune er behandlingsansvarlig, at de har sortert vegforvaltning og transport som en behandlingsaktivitet som foregår i sektoren Samferdsel. Behandlingsaktiviteten vegforvaltning og transport er videre spesifisert i enda mer konkrete «underkategorier» av behandlingsaktiviteten, trafikktelling i kryss og Tilskuddsordninger for trafikksikkerhet med flere.

GRC-verktøyet fungerer slik at man ved utfylling får spørsmål om behandlingsaktiviteten. Ved å svare på spørsmålene blir relevant informasjon om behandlingen dokumentert i protokollen. Ved hjelp av lys blå fargelegging gir forsiden til protokollen oversikt over hvor utfylt hver behandlingsaktivitet i protokollen er. Slik som dette:

Bilde 4. Utklipp fra Telemark fylkeskommune sin protokoll over behandlingsaktivitet. Bildet viser hvordan det ser ut når spørsmål om en behandlingsaktivitet ikke er besvart/utfylt, ferdig utfylt og delvis utfylt i GRC-verktøyet.

I personvernombudets årsrapport for 2024 står det at å føre protokoll har vært en prioritet. Det rapporteres om at det var mange protokoller som ble dokumentert dette året, over halvparten av behandlingene som ombudet har identifisert til nå. Videre påpeker ombudet at protokollen aldri blir helt ferdig, fordi behandlingene og systemene endres over tid, og protokollen må vedlikeholdes løpende. Årshjulet for informasjonssikkerhet og personvern viser at personvernkoordinatorene i mai 2026 skal gjennomgå behandlingsprotokoll og systemoversikter.

Dokumentasjonen i protokollen lages foreløpig av ombudet sammen med ansatte som kjenner de ulike behandlingene, personvernkoordinator i aktuell seksjon og ofte også sikkerhetsrådgiver merkantil. I praksis gjøres det i protokollmøter på Teams. Ombudet deltar nesten alltid i protokollføring fordi det gir mulighet for å kontrollere at regelverket følges og gi råd. På sikt er målet at personvernkoordinatorene får nok kompetanse til å ha en større rolle i forbindelse med protokollføring.

Fylkeskommunen har i løpet av revisjonsperioden utarbeidet og satt i drift et bestillingsskjema som virksomheter kan benytte når de ønsker å anskaffe nye systemer. Skjemaet er tilgjengelig på Innsida. Formålet er å sikre at risikovurderinger og dokumentasjon ifm. personvernlovgivning ivaretas. Skjema gjelder alle anskaffelser, også gratis programvare/lisenser. Et team bestående av personvernombud, tekniske ressurser, ressurser fra utdanning og sikkerhetsrådgiver merkantil tar imot bestillingene. Det blir da gjort en vurdering på personvern og en teknisk vurdering. Bestiller kalles så inn til protokollføringsmøte, der blant annet systemeier og systemansvarlig dokumenteres, samt at systemeier får bistand til å inngå databehandleravtale. Alle bestillinger blir automatisk oppført i programvareoversikten med status "ønskes anskaffet", der bestillingen får en ny status når den er vurdert. Enten om bestillingen godkjennes eller om den ikke kan benyttes. På den måten ajourføres også programvareoversikten. Fylkeskommunen er i gang med en gjennomgang av innkjøpsrutinen for anskaffelser over terskelverdi, for å sikre at riktige personer blir involvert for å ivareta personvernkravene.

Personvernombudet opplyser at det gjenstår en opplæringsjobb og forankring blant lederne som har ansvaret for protokollføring. Opplæring og forankring vil starte til høsten 2025, når de siste retningslinjene og prosedyrene i styringssystemet for informasjonssikkerhet og personvern er godkjent.

2.3.1. Stikkprøver

Vi har gjennomført stikkprøvekontroller av opplysningene som er registrert i protokollen for et utvalg behandlingsaktiviteter. Fargelegging i på forsiden av protokollen indikerer om de anbefalte feltene er ferdig utfylt eller ikke. Fylkeskommunen har registeret i overkant av 200 ulike behandlingsaktiviteter i protokollen, og vi ser at over halvparten av disse aktivitetene ikke er ferdig utfylt med obligatorisk eller anbefalt informasjon. Vi får opplyst at fylkeskommunen en kort periode brukte et annet verktøy for protokollføring. Det som lå der er overført til GRC-verktøyet, men noen behandlingsaktiviteter ble etter overføringen merket som delvis utfylt, fordi systemet hadde flere anbefalte felter for utfylling.

Vi har sett nærmere på ti tilfeldige behandlingsaktiviteter som var merket som ferdig utfylt i fylkeskommunens protokoll:[22]

- Skolestudio
- TS-tiltak i nærmiljøet

[22] Utvalg og stikkprøver ble gjort perioden 28.juli-6.august 2025.

- Dokumentasjon av feil, mangler og hendelser på fylkesvegnettet
- Klagebehandling i tannhelsetjenesten
- Tannhelsehjelp - behandling og journalføring i EPJ
- Avbrudd i studieåret
- Rekruttering
- Samtalebot Hugin
- Oppfølgingstjenester VGS
- Adgangskontroll -eiendom

Vi undersøkte om følgende utvalgte opplysninger var registrert for hver behandlingsaktivitet[23]:

- formål med behandlingen av personopplysninger
- kategorier av registrerte (hvem er det personopplysninger om),
- kategoriene av personopplysninger (dvs. hvilke personopplysninger er registrert),
- kategorier av mottakere som personopplysningene utleveres til, herunder i tredjestater mm
- om mulig, de planlagte tidsfristene for sletting av forskjellige kategorier opplysninger,
- om mulig, en generell beskrivelse av de tekniske og organisatoriske sikkerhetstiltakene[24]
- behandlingsgrunnlag[25]

For alle behandlingsaktivitetene vi har undersøkt er formålet med behandlingen og kategorier av registrerte beskrevet i protokollen.

Kategorier av personopplysninger er i hovedsak utfylt, men for en behandlingsaktivitet mangler det informasjon i protokollen om at elevenes egen produksjon behandles, slik det fremgår av personvernerklæringen. For en annen behandlingsaktivitet mangler det noe informasjon om kategoriene av mottakere som personopplysningene er blitt eller vil bli utlevert til. Det fremgår av protokollen at opplysninger deles med eksterne via e-post hvis det er aktuelt, men ikke noe om hvem det er aktuelt å dele opplysninger med.

Beskrivelse av de planlagte tidsfristene for sletting er mangelfullt beskrevet for tre behandlingsaktiviteter. For en behandlingsaktivitet vises det ikke til egne sletterutiner, men til databehandlers sletterutiner, som kun inntreffer ved opphør av databehandleravtalen. For en annen behandlingsaktivitet synes ikke sletterutinene å være tilstrekkelig avklart, og for den siste behandlingsaktiviteten er det ikke sletterutiner for alle de ulike kategoriene personopplysninger som inngår i behandlingsaktiviteten.

---

[23] Alt er hjemlet i personvernforordningen art. 34.
[24] Tiltakene er nevnt i art. 32. nr 1. Dette kan for eksempel være: pseudonymisering og kryptering av personopplysninger, evne til å sikre vedvarende konfidensialitet, integritet og tilgjengelighet, evne til å gjenopprette tilgjengelighet og tilgang, regelmessig testing, analysering og vurdering av hvor effektive sikkerhetstiltakene er. jf. personvernsforordningen art 32. nr. 1
[25] Personvernforordningen krever ikke at dette fremgår av protokollen, men det er anbefalt i Datatilsynets mal for protokoll. Videre krever forordningen art. 6, nr. 1 at kommunen må ha et gyldig behandlingsgrunnlag for å kunne *behandle* personopplysningene.

Beskrivelse av tekniske og organisatoriske sikkerhetstiltak er ufullstendig for seks av ni behandlingsaktiviteter. Det står kun beskrevet at det er tilgangskontroll. Personvernombudet opplyser at det finnes en rekke andre sikkerhetstiltak som ikke er beskrevet i protokollen.

Til slutt så vi at behandlingsgrunnlag for hver enkelt kategori personopplysninger til hvert enkelt formål var fylt ut.

2.3.2. Revisors vurdering av protokoll over behandlingsaktiviteter

Fylkeskommunen har rutiner for å sikre at det utarbeides protokoll over behandlingsaktiviteter i tråd med lovkrav. Det gjenstår imidlertid opplærings- og forankringsarbeid blant lederne og personvernkoordinatorene. Dette er planlagt.

Styringssystemet bidrar til god internkontroll, men det er et etterslep og gjenstår en del arbeid for at fylkeskommunen skal ha en fullverdig protokoll over sine behandlingsaktiviteter.

Vi ser videre av våre stikkprøver at selv om «fargelegging» gir indikasjon på at behandlingen er ferdig protokollført, så mangler det noe informasjon for flere aktiviteter.

2.4. Risikovurdering

Telemark fylkeskommune skal ha kartlagt risiko/gjort risikovurderinger.

Iht. Telemark fylkeskommune sin policy for behandling av personopplysninger skal fylkeskommunen gjøre risikovurderinger knyttet til de registrertes rettigheter og friheter. På fylkeskommunens intranett står det at risikovurderinger skal gjøres når det innføres nye digitale løsninger og når det lages ny behandlingsprotokoll i GRC-verktøyet.

Det er prosesseier, systemansvarlig, personvernkoordinatorer, IT-ansvarlig og sikkerhetsrådgiver merkantil som har ansvar og oppgaver knyttet til risikovurderinger iht. rolle- og ansvarsbeskrivelser fylkeskommunen har for personvern (se beskrivelse i kap 2.1.1).

Det fremgår av en prosedyren for risikostyring av informasjonssikkerhet og personopplysningssikkerhet godkjent i juni 2025, at risikovurderinger skal gjennomgås ved alle typer planlagte endringer og i situasjoner med vurdert sårbarhet eller endret trusselbilde. Det gis følende eksempler på slike situasjoner:

- etablering av ny behandling av personopplysninger
- endring i eksisterende behandling av personopplysninger
- endringer i relevante lover og forskrifter
- endringer i tjenestekatalogen
- endringer i trusselbildet
- organisasjonsendringer
- innføring av nye IT-systemer
- flytting av infrastruktur og tjenester til skyen
- bruk av lokaler og bygg hvor informasjon behandles
- etablering av nye leverandører og databehandlere

Prosedyren gir også eksempler på informasjonsverdier, trusler og sårbarheter, for å veilede om hvordan man identifiserer og graderer risiko.

Risikovurderinger forklares å handle om å vurdere sannsynligheten (fra lite til svært sannsynlig) for at de uønskede hendelsene kan oppstå, og konsekvensene (fra ufarlig til katastrofalt) dersom de oppstår - Risiko = sannsynlighet * konsekvens. Det gis eksempler som at hendelsen er svært sannsynlig hvis den skjer månedlig eller oftere, og at konsekvensen er farlig hvis den har merkbare virkninger, f.eks. hvis større mengder alminnelige personopplysninger eksponeres i opptil en uke.

Konsekvens for personvern skal vurderes med utgangspunkt i de registrertes rettigheter og friheter. Videre skal det vurderes hvilke risikoer virksomheten aksepterer, hvilke risikoer det må vurderes tiltak for og hvilke det må iverksettes tiltak for. Det skilles mellom risikoaksept på grønt nivå, gult nivå og rødt nivå. På grønt nivå er sikkerhetstiltak normalt ikke nødvendig. På gult nivå bør sikkerhetstiltak vurderes, og vurderingen godkjennes av nærmeste leder. På rødt nivå må sikkerhetstiltak gjennomføres og godkjennes av seksjonsleder/virksomhetsleder.

Det står at alle sikkerhetstiltak skal oppføres i risikohåndteringsrapporten og at rapporten skal godkjennes av ledelsen. Alle risikovurderinger skal dokumenteres og lagres i GRC-verktøyet, og fylkeskommunen har en praktisk veileder for hvordan man gjennomfører risikovurderinger der[26].

Resultater fra risikovurderinger og tilhørende sikkerhetstiltak skal gjennomgås i ledelsens årlige gjennomgang, jf. egen prosedyre for ledelsens gjennomgang.

Praksis

Sikkerhetsrådgiver merkantil forteller at det ikke er helt avklart hvordan risikovurderinger skal gjennomføres i praksis, og rutinene er nye. Det har frem til nå ikke vært noe strukturert system for hvordan man skal gjøre risikovurderinger, og det er utprøving og utforsking å finne de beste løsningene. Personvernombudet forteller at det sannsynligvis etter hvert vil komme en revideringsfrekvens på alle behandlingsaktiviteter i protokollen, ut fra risiko knyttet til denne aktiviteten. Pr nå er det gjort få risikovurderinger sammenlignet med systemer og behandlingsaktiviteter. Det er startet med risikovurderinger av nye systemer som innføres, og av behandlinger som er kjenner til at er mest risikofylt.

Tannhelse

Vi får opplyst at risikovurdering hovedsakelig er gjort på eget initiativ av tannhelses personvernkoordinator. To av fem behandlingsaktiviteter som ligger under Tannhelse, har blitt risikovurdert. Det opplyses at det er lite endringer i behandlingsaktiviteter, formålet med

[26] Den viser forskjellen på å gjennomføre en risikovurdering av et system og å gjennomføre risikovurdering av en konkret type behandling. Videre viser den hvordan man gjennomfører risikovurderinger, hvordan leder godkjenner risikovurderinger og hvordan man knytter risikovurderingen opp til bestemt(e) tiltak som enten reduserer sannsynligheten for eller konsekvensen av en risiko.

behandling av personopplysninger og systemene som benyttes til behandling av personopplysninger ved tannklinikkene.

Skolene
Skolene opplyser at systematisk risikovurdering gjøres sentralt i fylkeskommunen, da skolene ikke anskaffer eller tar i bruk løsninger med mindre disse er godkjent sentralt. Bare 3 av de 83 behandlingsaktivitetene/systemene som ligger under videregående opplæring i fylkeskommunens protokoll, er risikovurdert.

Skolene har nylig fått tilgang til en ny løsning som kalles «samskrivningsløsning for elevoppfølging». Fylkeskommunen har selv vurdert at løsningen har høy risiko for fysiske personers rettigheter og friheter, og at en egen DPIA dermed skal utarbeides (se kap. 2.5). Det er også laget en egen rutine for at rektorer årlig skal gjøre ROS-analyse av løsningen på egen skole og ev. iverksette risikodempende tiltak ved behov. Dette fremgår av rutinen for samskrivningsløsningen i videregående skole. Rutinen er tilgjengelig på fylkeskommunens intranett. Rektorene på de to skolene vi har undersøkt er ikke kjent med denne rutinen.

2.4.1. Revisors vurdering av risikovurdering
Fylkeskommunen har rutiner for at det skal gjøres risikovurderinger ved innføring av nye digitale løsninger, ved alle typer planlagte endringer og i situasjoner med vurdert sårbarhet eller endret trusselbilde. Det framgår ikke av rutinene at risikovurderinger skal gjøres regelmessig. Personvernsnemda har uttalt at økende trussel mot informasjonssikkerheten stiller krav til regelmessige risikovurderinger[27]. Vi mener at regelmessig risikovurdering med fordel kan tas inn i fylkeskommunens rutiner, selv om det sannsynligvis vil komme en revideringsfrekvens i protokollen.

Det er et etterslep på gjennomføringen av risikovurderinger. Det er foreløpig uavklart hvordan risikovurderinger skal gjennomføres. Rutinen for risikovurdering av samskrivningsløsningen er ikke godt nok kjent blant rektorene.

2.5. Vurdering av personvernkonsekvenser (DPIA)
Telemark fylkeskommune skal ha dokumenterte vurderinger av personvernkonsekvenser (DPIA) der dette er aktuelt.

Det fremgår av Policy for behandling av personopplysninger at fylkeskommunen skal vurdere personvernkonsekvenser (DPIA) når det vurderes å foreligge høy risiko for de registrerte.

[27] Personvernsnemda. *Brudd på personopplysnings- og informasjonssikkerheten i Østre Toten kommune – overtredelsesgebyr* (PVN-2022-13).

På fylkeskommunens intranett står det at en konkret vurdering av personvernkonsekvenser etter artikkel 35 er obligatorisk når behandling av personopplysninger vil medføre en høy risiko for personers personvern. Det gis følgende eksempler på når det kan være høy risiko, og det er lenke til Datatilsynets liste over behandlingsaktiviteter som alltid krever DPIA:

- personopplysninger om sårbare registrerte; pasienter, barn, eldre
- behandling av sensitive personopplysninger (særlige kategorier), eller opplysninger av svært personlig karakter
- bruk av ny teknologi
- behandling av personopplysninger i stor skala
- automatiske avgjørelser

Nettverket for personvernombud i fylkeskommunene har laget en veiledning og en mal for vurdering av personvernkonsekvenser som Telemark fylkeskommune bruker. Veiledningen viser prosessen som skal følges.

Organisere

Først skal det vurderes om det er behov for å gjennomføre en DPIA. Dersom svaret er ja, skal man opprette en arbeidsgruppe som ivaretar kompetanse om behandlingsaktiviteten og personvern. Sammensetningen vil variere ut fra behandlingsaktivitetens omfang og kompleksitet. Arbeidsgruppa skal ha minst en deltaker med god kjennskap til behandlingsaktiviteten og løsningen som skal vurderes, og en deltaker med kompetanse knyttet til personvern og gjennomføring av DPIA. Hvis det er hensiktsmessig, kan personvernombudet være med. I så fall skal det omtales i personvernombudets uttalelse. Det kan være aktuelt å konsultere ulike interessenter som tillitsvalgte, ombudsroller o.l. Behandlingsansvarlig representant skal informeres og konsulteres fortløpende, og særskilt dersom det avdekkes alvorlige avvik eller risikoer som må håndteres.

Beskrivelse av behandlingen

Første steg for arbeidsgruppa er å beskrive behandlingsaktiviteten utfyllende, slik at beskrivelsen gir et godt grunnlag.

Vurdering av risiko og identifisering av tiltak

Veiledningen gir en rekke spørsmål som skal bidra til å identifisere relevante risikoer. I malen er følgende risikoområder/risikoer identifisert:

- lovlighet
- rettferdighet og åpenhet
- formålsbegrensning
- dataminimering og riktighet
- lagringsbegrensning
- integritet og konfidensialitet
- rett til informasjon
- rett til innsyn

- rett til retting og sletting
- rett til begrensning
- rett til å protestere

Risikovurderingen skal gjøres ut ifra hvilke konsekvenser en uønsket hendelse eller manglende etterlevelse kan ha for den registrerte (ikke for virksomheten).

Det er den høyeste risikoen ved vurderingstidspunktet som skal vurderes. Videre skal arbeidsgruppa beskrive tiltak som arbeidsgruppa anser nødvendig eller anbefaler for å ivareta kravet. Deretter skal høyeste risiko etter tiltak beskrives.

Når informasjon om behandlingsaktiviteten legges inn i behandlingsprotokollen, vil GRC-systemet vise om det bør gjennomføres en DPIA. Systemet vil da kreve at DPIA gjennomføres, eller at det gis en begrunnelse i systemet for hvorfor det ikke er nødvendig.

Vurdering av nødvendighet og rimelighet
Arbeidsgruppa skal vurdere hvilken verdi eller nytte behandlingsaktiviteten har, om aktiviteten er nødvendig for den registrerte, for virksomheten og/eller for samfunnet. Deretter skal verdien/nytten veies opp mot hvor inngripende behandlingen av personopplysningene er for den registrerte. Hvis vurderingen viser at forholdet mellom nytte og inngrep ikke er proporsjonal eller rimelig, bør ikke arbeidsgruppa anbefale at behandlingsaktiviteten settes i gang eller fortsetter.

Vurderingen skal ta hensyn til om behandlingens art, omfang, formål og sammenhengen den utføres i, kan innebære høy risiko for fysiske personers rettigheter og friheter, jf. personvernforordningen art 35 nr. 1. Dette er beskrevet i Policy for behandling av personopplysninger og på intranettsiden om DPIA – personvernkonsekvensvurdering.

I denne fasen skal personvernombud og representant for de registrerte alltid konsulteres og få uttale seg. Personvernombudet skal vurdere om vurderingen oppfyller lovens krav, om alle viktige forhold er vurdert, og om personvernombudet er enig i arbeidsgruppas konklusjon. De registrertes uttalelse skal innhentes fra en eller flere representanter for de registrerte. Representantene bør vurdere om det er vesentlige risikoer som ikke er identifisert, om tiltakene er gode nok og om de mener at behandlingen som nødvendig og rimelig. Arbeidsgruppa kan endre sin vurdering og konklusjon basert på uttalelsen fra personvernombudet og de registrerte.

Arbeidsgruppas anbefaling
Arbeidsgruppas vurdering og anbefaling skal gi grunnlag for om virksomhetens beslutning om behandlingen kan settes i gang eller fortsette, om det er nødvendig å iverksette flere tiltak eller om behandlingen ikke skal starte. Arbeidsgruppa skal forslå både nødvendige tiltak og anbefalte tiltak.

Det anbefales at arbeidsgruppa gjennomgår vurderingen med behandlingsansvarliges representant/er før de gjør sin vurdering og beslutning om behandlingen.

Behandlingsansvarliges beslutning

Behandlingsansvarliges vurdering og beslutning skal dokumenteres i et eget dokument. Her skal behandlingsansvarliges representant(er)[28] vurdere om behandlingsaktiviteten er riktig og tilstrekkelig beskrevet, om personvernombudets og de registrertes syn er tilstrekkelig ivaretatt og om behandlingen kan settes i gang eller videreføres. Det er en egen mal for dette.

Behandlingsansvarlig kan følge arbeidsgruppas anbefaling, eller velge å basere sin beslutning på egne vurderinger. Valget skal begrunnes.

Dersom behandlingsansvarlige vurdere at behandlingsaktiviteten kan iverksettes eller videreføres, bør behandlingsansvarlige utarbeide en tiltaksplan der dette er relevant. Anbefalte tiltak fra arbeidsgruppa vil styrke personvernet, men behandlingsansvarlig kan vurdere om risikoen aksepteres uten slike tiltak, f.eks. ut fra hensyn til kostnader eller tilgjengelige ressurser.

2.5.1. Stikkprøver

Telemark fylkeskommune har gjennomført fire DPIAer. De fire DPIAene beskriver blant annet de planlagte behandlingsaktivitetene, formålet med behandlingen, vurdering av risiko og risikobegrensende tiltak. To av DPIAene er gjennomført av eksterne,[29] og følger dermed ikke fylkeskommunens mal for gjennomføring av DPIA. Det fremgår ikke om behandlingsansvarliges representant i Telemark fylkeskommune har gjennomgått DPIAen før behandlingen startet. De to andre DPIAene gjelder samskrivningsløsningen på videregående skole og tannhelsehjelp – elektronisk pasientjournal. Disse ble utført før det var tatt beslutning om hvilken mal som skulle benyttes. DPIA for elektronisk pasientjournal har ikke brukt fylkeskommunens mal for DPIA, men Direktoratet for e-helse sin. Det fremgår at fylkestannlegen har godkjent DPIAen.

DPIA for samskrivningsløsningen har brukt fylkeskommunens mal, men det er kun et utkast til DPIA som er arkivert. Personvernombudet opplyser at de tidligere ikke hadde noen god rutine rundt leders gjennomlesing, kommentar og signering. Det er opplyst at vurderingen ble lagt fram for lederne og godkjent, men ikke signert. Dokumentet er heller ikke datert, selv om vurderingen anbefaler at løsningen skal revideres etter ett år (maksimalt to år).

Det er ikke hentet inn synspunkter fra de registrerte eller deres representanter om den planlagte behandlingen, verken for samskrivningsløsningen eller folkehelseundersøkelsen. Det framgår ikke om det er vurdert å innhente slike synspunkter.

2.5.2. Revisors vurdering av DPIA

Telemark fylkeskommune har rutiner for å dokumentere vurderinger av personvernkonsekvenser (DPIA).

---

[28] Myndighet delegert til fylkessjefer, seksjonsledere/rektorer, teamledere/klinikkledere/avdelingsledere og personvernombudet, jf. administrativt delegeringsreglement.
[29] DPIA for Røst er gjennomført av Universitetet i Stavanger i september 2024 og DPIA for folkehelseundersøkelsen er gjennomført av Sikt personverntjenester.

Det er usikkert om Telemark fylkeskommune på revisjonstidspunktet har gjennomført DPIA i alle tilfeller der det sannsynligvis er høy risiko for fysiske personers rettigheter og friheter. Det er grunn til å tro at behov for DPIA vil bli fanget opp i GRC-verktøyet når protokollen blir komplett.

Stikkprøvekontrollen viser at en DPIA ikke er datert. Vi ser også at prinsippet om ansvarlighet ikke har blitt ivaretatt for tre av fire DPIAer[30]. Dokumentasjonen viser ikke om fylkeskommunen har vurdert at det ikke er relevant å innhente synspunkter fra de registrerte for to av DPIAene. Dersom fylkeskommunen har vurdert at det ikke er relevant, så bør det framgå av dokumentasjonen.

2.6. Avvikshåndtering

Telemark fylkeskommune skal ha rutiner og tiltak for å håndtere brudd på personopplysningssikkerheten.

På fylkeskommunens intranett er det lenke til fylkeskommunens kvalitetssystem, der alle typer avvik skal meldes. Avvik er definert som uønskede hendelser, og er beskrevet som brudd, feil eller mangler på eksterne eller interne retningslinjer og krav. Følgende er definert som avvik knyttet til personvern eller informasjonssikkerhet:

- En uønsket hendelse som kan føre/fører til brudd på informasjonssikkerheten eller personvernet (konfidensialitet, integritet og tilgjengelighet)
- Når vi ikke følger lover, regler og interne retningslinjer som regulerer bruken av IT-systemer og behandling av personopplysninger.

Fylkeskommunen har laget en brukerveiledning («trinn for trinn»), og det er en opplæringsvideo for hvordan man melder avvik i systemet. Fylkeskommunen har også en prosedyre for varsling av brudd på personopplysningssikkerheten, og en prosedyre for å melde avvik til Datatilsynet. Avvik på informasjonssikkerhet og personvern skal være tema i mars 2026, og er satt opp som en aktivitet i fylkeskommunens årshjul på området.

Ansatte skal melde avvik på bla. informasjonssikkerhet og personvern. Leder med personalansvar skal sørge for informasjon og opplæring til egne ansatte, oppfølging av hendelsen, eventuelle tiltak, lukke hendelsen, arbeide for å forbygge hendelser, følge med og ta ut statistikk, bevisgjørelse/bruke statistikk til å arbeide forbyggende. Vi får opplyst at sikkerhetsrådgiver merkantil, seksjonsleder digitale tjenester og personvernombud får tilsendt kopi av avvikene, slik at de har mulighet til å kontrollere håndertingen. Sikkerhetsrådgiver merkantil skal kontrollere om avvik står åpne eller er lukket månedlig[31].

[30] Datatilsynets veileder. Hvordan gjennomføre en DPIA? Sist endret 27.07.23. Ihht som iht. fylkeskommunens egne rutiner skal prinsippet ivaretas ved at behandlingsansvarliges representant/er vurderer om behandlingen kan iverksettes eller videreføres.
[31] Lagt inn som en oppgave i GRC-systemet.

Noen avvik, for eksempel alvorlige brudd på personopplysningssikkerheten, skal meldes videre til Datatilsynet. Iht. prosedyrene skal fylkeskommunen vurdere om det er slik meldeplikt for avvikene. Prosedyre for varsling av brudd på personopplysningssikkerheten og Prosedyre for å melde avvik til Datatilsynet gir ulik informasjon om hvem som skal vurdere og beslutte spørsmålet om melding til Datatilsynet. Informasjon om hvem som skal gjøre dette er lagt inn i avvikssystemet. Når et avvik er meldt, sendes det automatisk til de personene som skal håndtere det videre, inkludert de som skal vurdere og avgjøre om det skal meldes til Datatilsynet.

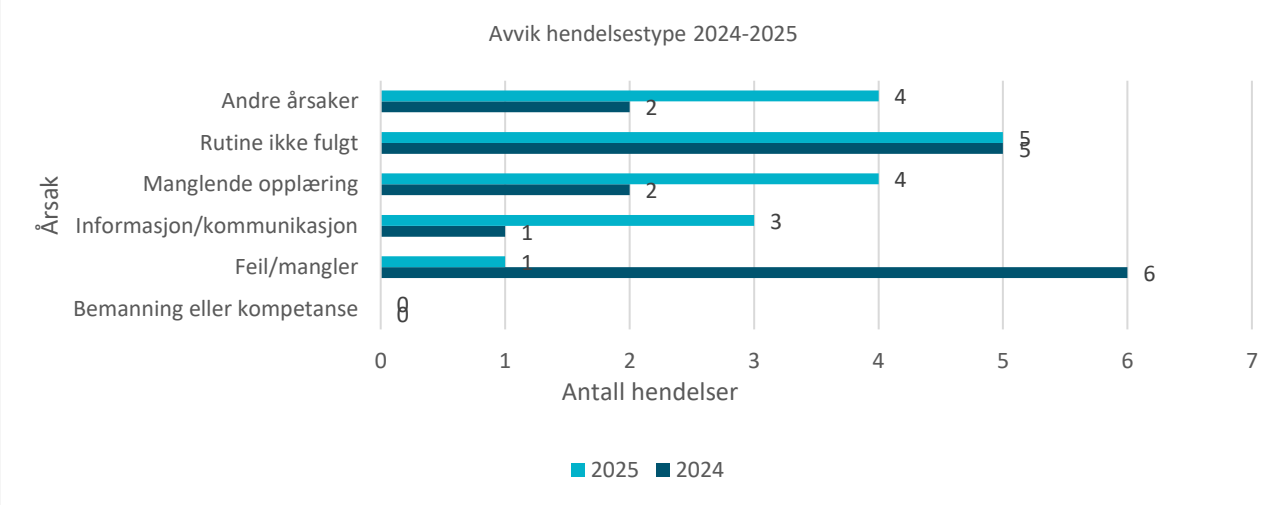
I Prosedyre for varsling av brudd på personopplysningssikkerheten står det at Datatilsynet skal varsles så raskt som mulig, senest innen 72 timer, dersom bruddet har eller vil medføre en risiko for personvernet til de registrerte. Dette er ikke omtalt i prosedyren for varsling til Datatilsynet. Begge prosedyrene sier noe om når de registrerte skal varsles, men formuleringene er noe ulike.

Det fremgår av begge prosedyrene at personvernombudets anbefaling/konklusjon om meldeplikt til Datatilsynet skal dokumenteres. I løpet av revisjonsperioden er det etablert en rutine for at denne dokumentasjonen skal legges i avvikssystem, sammen med avviket. Dette framgår av veiledningsmateriell til avvikssystemet. Avvikseier skal følge opp at dette blir ivaretatt.

Ifølge intranettet og prosedyren for varsling av brudd på personopplysningssikkerheten er det sikkerhetsrådgiver merkantilt, seksjonsleder for digitale tjenester, personvernombud og to personvernkoordinatorer (innenfor utdanning) som har fullmakt til å melde avvik til Datatilsynet. Fylkeskommunen har en mal som kan brukes som et internt arbeidsdokument for å forberede meldingen.

Praksis

I Telemark fylkeskommune er det så langt i 2025 innmeldt 17 avvik og i 2024 ble det innmeldt 16 avvik på informasjonssikkerhet og personvern. Til sammenligning ble det i gamle Vestfold og Telemark fylkeskommune i 2023 meldt åtte avvik. De fleste avvik i 2024 og 2025 dreide seg om at rutiner ikke ble fulgt og feil/mangler. Slik fordeler avvikene seg på ulike kategorier hendelser:



Figur 3. Avvik på informasjonssikkerhet og personvern 2024-2025 innmeldt i avvikssystemet TQM. Tallene er hentet ut av fylkeskommunen 24.06.2025.

Meldte avvik i 2024 og 2025:

Seksjon/virksomhet	2024	2025*
Politisk støtte	0	1
Porsgrunn vgs	1	2
Skien vgs	1	0
Seksjon PPT, OT og alternative opplæringsarenaer	1	0
Seksjon eiendom	0	1
Seksjon HR	1	1
Skien tannklinikk	2	1
Midt-Telemark tannklinikk	0	1
Seljord tannklinikk	0	1
Notodden tannklinikk	7	2
Kragerø tannklinikk	1	
Team arkiv	1	3
Utdanning, folkehelse og tannhelse	0	4
Seksjon skoleutvikling og folkehelse	1	0

*Tabell 5. Fordeling pr seksjon/virksomhet. *Tall for 2025 pr. juni 2025.*

Det er to avvik fra april og juni 2025 som ikke er lukket pr august 2025.

Ifølge personvernombudets årsrapport ble ingen avvik vurdert meldepliktige til Datatilsynet i 2024. Vi får opplyst at ingen avvik er meldt til Datatilsynet i 2025.[32] Til sammenligning ble tre av åtte avvik i gamle Vestfold og Telemark fylkeskommune meldt videre til Datatilsynet i 2023.[33]

Personvernombudet mener at det ikke er ofte at avvikene i fylkeskommunen har medført en sånn risiko for personvernet til de registrerte at det er aktuelt å melde til Datatilsynet.

Fylkeskommunens prosedyre er at personvernombudets anbefaling/konklusjon om meldeplikt til Datatilsynet skal dokumenteres. Personvernombud og sikkerhetsrådgiver opplyser at vurderingene av meldeplikt ikke har blitt dokumentert tidligere, men at rutine og praksis nylig er endret. Revisor har sett flere eksempler på innmeldte avvik hvor det er relevant å vurdere meldeplikt. I de eldste av

[32] September 2025
[33] Årsbudsjett 2023 og økonomiplan 2023 – 2026 for Vestfold og Telemark fylkeskommune.

disse er ikke vurderingen/konklusjonen dokumentert. I de nyere eksemplene på slike avvik ser vi at vurderingene er dokumentert i avvikssystemet.

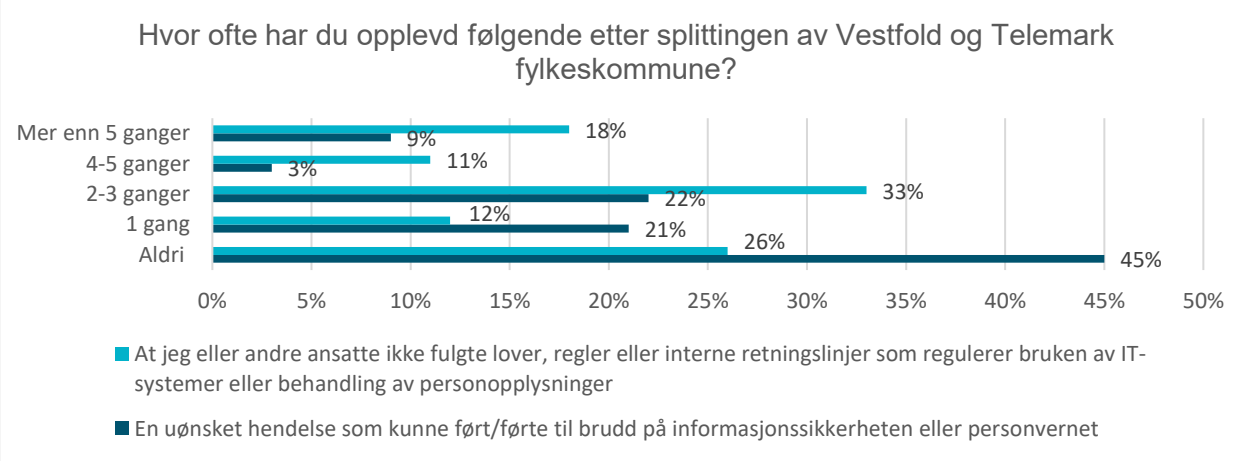
Praksis ved tannklinikkene

De ansatte ved tannklinikkene svarer i snitt at de har noe kjennskap til rutiner for å melde avvik på informasjonssikkerhet og personvern (4 på en skala fra 1 kjenner ikke til – 6 kjenner til svært godt). Flertallet kjenner godt til rutinene, men 12% kjenner ikke til eller kjenner bare til rutinen i liten grad. Vi har også spurt ansatte ved tannklinikkene om de vet hvordan de skal melde fra om brudd på personvernreglene. Svarene viser et gjennomsnitt på 4, noe som indikerer at gjennomsnittet er noe enig i at de vet dette. Flertallet på 72 % svarer positivt med enten helt enig, enig og delvis enig, 28 % svarte mot den negative siden med helt uenig, uenig og delvis uenig.

Svaralternativ	Prosent
Helt uenig 1	7%
2	7%
3	15%
4	21%
5	22%
Helt enig 6	29%

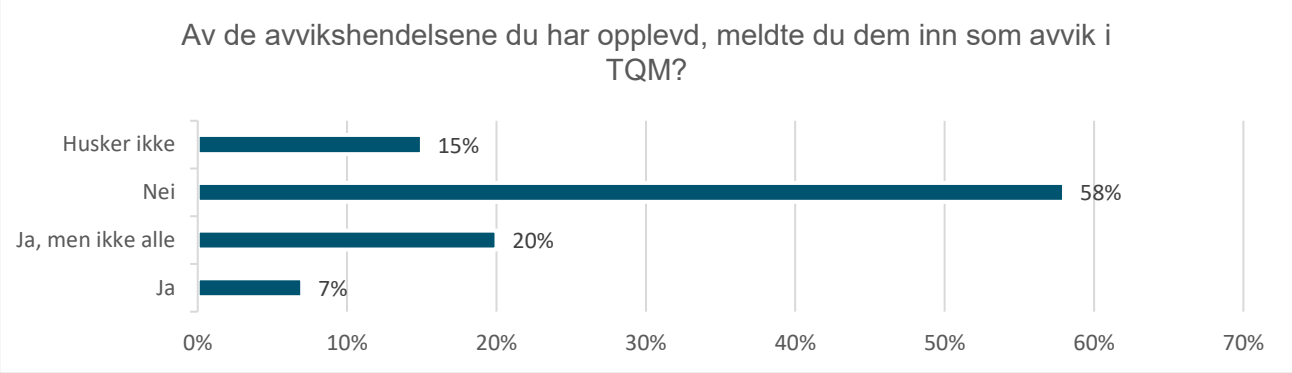
Tabell 6. Svar på påstanden «Jeg vet hvordan jeg skal melde fra om brudd på personvernreglene». N=76.

Av spørreundersøkelsen ser vi at flest ansatte ved tannklinikkene aldri har opplevde en uønsket hendelse som kunne ført/førte til brudd på informasjonssikkerhet eller personvern (45%). I gjennomsnitt har ansatte opplevd dette en gang. Noe oftere opplevde ansatte at en selv eller en annen ansatt ikke fulgte lover, regler eller interne retningslinjer som regulerer bruken av IT-systemer eller behandling av personopplysninger. Her var det 25% som aldri hadde opplevd dette, mens gjennomsnittet var mellom 1 og 2-3 ganger. Opplevde avvik fordeler seg slik:



Figur 4. N=76.

Undersøkelsen viser at de fleste som har opplevd avvik, ikke meldte dem inn i fylkeskommunens avvikssystem:



Figur 5. N=59.

De som meldte avvik, opplevde i stor grad at disse ble godt håndtert.

Seksjonsleder for tannhelse og personvernkoordinator på området mener at avvikskulturen er bedre for informasjonssikkerhet og personvern enn enkelte andre områder som HMS, da det oppleves å være en god forståelse blant de ansatte om hva som er et avvik på dette området. Derimot er det flere som mener at det er tungvint å melde avvik i avvikssystemet. Vi blir fortalt at fylkeskommunens avvikssystem ikke er tilpasset helsepersonell, at begrepene og brukergrensesnittet oppleves vanskelig. I tillegg tar avviksmelding tid fra annet viktig arbeid, samt at det ved enkelte avvik oppleves som dobbeltarbeid å melde avviket i systemet, da man samtidig også må gi beskjed til leder og/eller IKT om samme feil.

Praksis ved skolene

De ansatte ved skolene svarer i snitt at de kjenner lite til rutiner for å melde avvik på informasjonssikkerhet og personvern i avvikssystemet. Det gjennomsnittlige svaret er 3 på en skala fra 1 kjenner ikke til – 6 kjenner til svært godt. Bare 18% kjenner svært godt eller godt til rutinene og 38% kjenner ikke eller kjenner bare i liten grad til rutinene.

Vi har bedt de ansatte ved skolene om å ta stilling til påstanden «Jeg vet hvordan jeg skal melde fra om brudd på personvernreglene». Svaralternativene er fra 1 Helt uenig til 6 Helt enig. Svarene viser et gjennomsnitt på 3,5, noe som indikerer midt mellom noe uenig og noe enig. Det er en betydelig spredning i svarene: 46% svarer positivt, at de vet hvordan de melder fra, mens 48% svarer negativt, på uenigskalaen.[34]

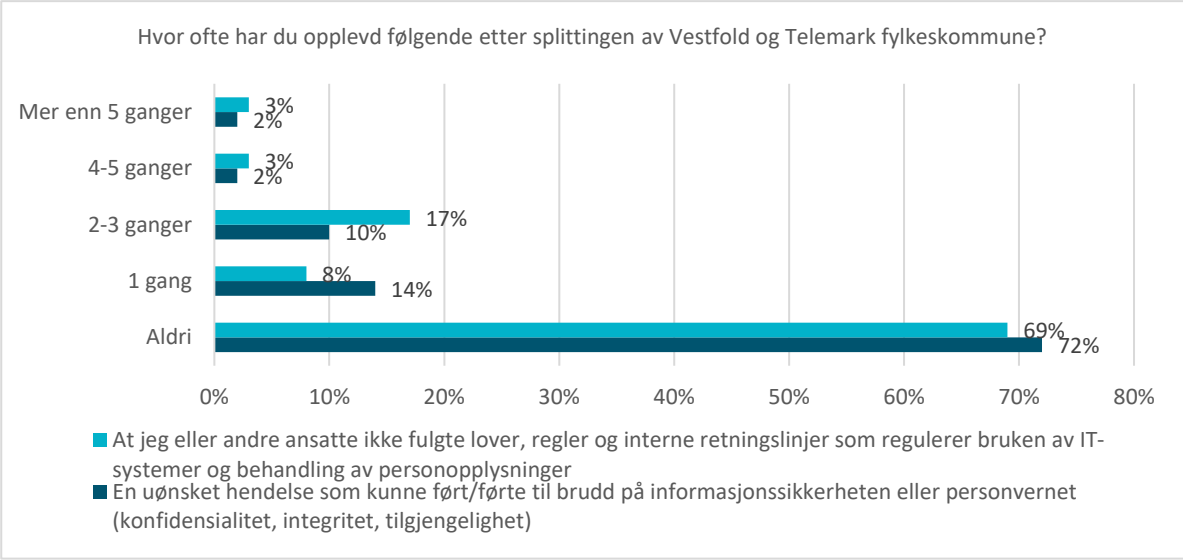
Svaralternativer	Prosent
Helt uenig 1	12%
2	18%
3	18%
4	14%

[34] Standardavvik på 1,6

Svaralternativer	Prosent
5	18%
Helt enig 6	14%
Vet ikke/ikke aktuelt	5%

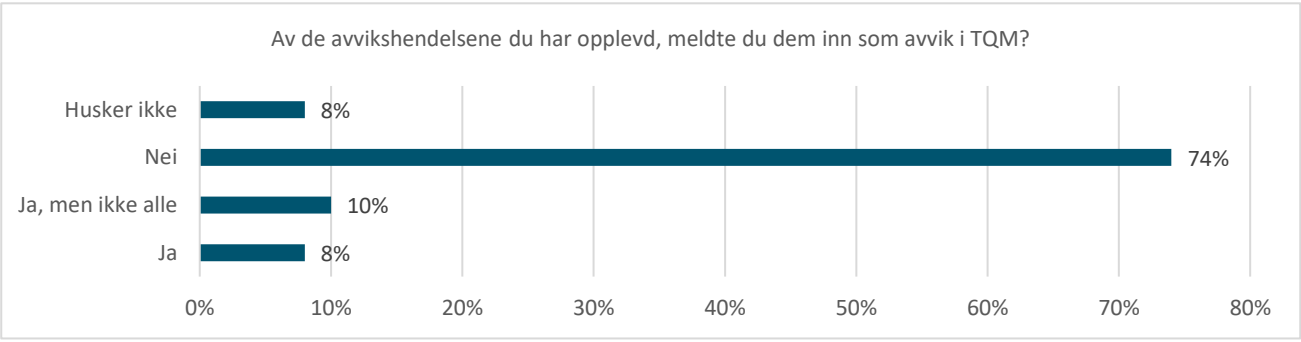
Tabell 7. Svar på påstanden «Jeg vet hvordan jeg skal melde fra om brudd på personvernreglene». N=93.

Av spørreundersøkelsen ser vi at ansatte ved skolene i gjennomsnitt aldri til en gang har opplevd en uønsket hendelse som kunne ført/førte til brudd på informasjonssikkerhet eller personvern, eller at en selv eller en annen ansatt ikke fulgte lover, regler eller interne retningslinjer som regulerer bruken av IT-systemer eller behandling av personopplysninger. Opplevde avvik fordeler seg på antall ganger slik:



Figur 6. N=104.

Undersøkelsen viser at et stort flertall av de som opplevde avvik, ikke meldte avvikene i fylkeskommunens avvikssystem:



Figur 7. N=39.

De vanligste årsakene til at avvikene ikke ble registrert, var at den ansatte var usikker på om det var et avvik, at avviket ble håndtert med en gang/meldt ifra om på annen måte og dermed

opplevdes det ikke som aktuelt å melde, eller at avviket var lite og dermed unødvendig å registrere. Det fremkommer også av intervju med ledelsen ved en av de to undersøkte skolene at avvik meldes først til nærmeste leder gjennom uformelle kanaler, altså ikke i avvikssystemet, og at det videre gjøres en vurdering av om avvikene er så alvorlige eller gjentagende at de skal meldes.

De få som meldte avvikene, opplevde i stor grad at disse ble godt håndtert.

2.6.1. Revisors vurdering av avvikshåndtering

Telemark fylkeskommune har rutiner for å håndtere brudd på personopplysningssikkerheten. To rutiner som delvis dekker samme tema, gir ulik informasjon, og bør oppdateres/samordnes innholdsmessig eller slås sammen til en rutine.

I den undersøkte perioden har ikke fylkeskommunen meldt noen avvik til Datatilsynet, eller underrettet noen registrerte om brudd. Ifølge rutinene skal vurderingene av disse tiltakene dokumenteres. Vi ser at praksis har endret seg, slik at disse vurderingene er dokumentert i de nyeste avvikene.

Revisor har sett at alle, unntatt to relativt nye avvik fra 2025, er lukket. Spørreundersøkelsene indikerer en vesentlig underrapportering på informasjonssikkerhet- eller personvernsavvik både fra tannklinikkene og skolene. For de fleste ansatte ved tannklinikkene er det ikke mangel på kjennskap til rutiner eller opplæring i hvordan melde avvik som er grunnen til mangelfull avviksrapportering. Manglende kunnskap om rutiner og system synes i større grad å være årsaken til at ansatte ved skolene ikke melder avvik. Vi ser også at ledelsen ved en av de to undersøkte skolene ikke melder avvik i samsvar med fylkeskommunens avviksrutiner, da de kun melder alvorlige eller gjentagende avvik i avvikssystemet.

Revisor mener at det er behov for ytterligere tiltak for å sikre at brudd på personopplysnings-sikkerheten meldes internt gjennom de formelle kanalene til fylkeskommunen. Avvikshåndtering handler om å lære av feil, slik at risikoen i neste omgang blir mindre[35]. Avviksstatistikk er nyttig for å sikre overordnet læring og forbedring, ut over den erfaringen det enkelte avvik gir. Terskelen for meldeplikt til Datatilsynet om brudd på personopplysningssikkerheten er lav. Den nye praksisen med å dokumentere vurderingene av meldeplikt, kan legge til rette for systematiske vurderinger av om fylkeskommunens har riktig terskel for å melde avvik til Datatilsynet og den registrerte.

2.7. Ivaretakelse av registrertes rettigheter

Telemark fylkeskommune skal ha tiltak for å ivareta de registrertes rett til informasjon og innsyn.

Det fremgår av Policy for behandling av personopplysninger at de registrerte skal informeres om alle behandlinger av deres personopplysninger, jf. GDPR (personvernforordningen) art. 12, 13 og

[35] KS veileder «Orden i eget hus - Kommunedirektørens internkontroll»

14. Policy for å ivareta de registrertes rettigheter er godkjent i mars 2025. Her fremgår det at de registrertes rettigheter omfatter rett til å bli informert, rett til innsyn, korrigering, sletting, begrensning, rett til å protestere, rettigheter ved automatiserte avgjørelser og rett til dataportabilitet (retten til å kunne ta med sine opplysninger fra en tjeneste til en annen).

Fylkeskommunen skal følge disse prinsipper for informasjon om registrertes rettigheter:

- Telemark fylkeskommune skal definere informasjon som skal gis til de registrerte i forbindelse med innsamling av deres personopplysninger.
- Informasjon om rettigheter skal gis i forkant eller i forbindelse med innsamling av personopplysninger (for eksempel som en del av et søknadsskjema). Informasjonen skal gis aktivt.
- Informasjon om rettigheter kan gis i samme format som for innsamling av personopplysninger (for eksempel som en del av et samtykkeskjema på papir).
- Informasjon om rettigheter kan samles i personvernerklæringer, og skal være kortfattet, åpen, forståelig, lett tilgjengelighet og tilpasset målgruppene.

Fylkeskommunen skal videre ivareta disse prinsippene:

- Fylkeskommunen skal etablere mekanismer for at de registrerte kan gi, endre og trekke samtykke.
- Utøvelse av retten til korrigering, protestering, begrensning og sletting skal tilsvarende skje gjennom en sikker løsning.
- Fylkeskommunen skal avklare hvorvidt det gjennomføres behandlinger som involverer automatisk beslutningstaking.
- Fylkeskommunen skal legge til rette for dataportabilitet ved å legge til rette for at de registrerte kan få utlevert sine personopplysninger i et maskinlesbart eller vanlig brukt filformat.

Policy for å ivareta de registerets rettigheter nevner også prinsipper for innsyn bla. at fylkeskommunen bør etterspørre funksjonalitet for å laste ned personopplysninger, enten via brukergrensesnittet eller via et API[36] i forbindelse med anskaffelser eller systemutvikling.

På intranettet til fylkeskommunen står at det er to lover som gir rett til innsyn: offentlighetsloven og personopplysningsloven. I tillegg kan det også kreves partsinnsyn etter forvaltningsloven. Det står at innsyn etter personopplysningsloven skal saksbehandles "uten ugrunnet opphold", maksfrist en måned. Det fremgår at alle personer som er registrert i fylkeskommunens systemer kan be om innsyn i egne personopplysninger, og hvordan disse er behandlet.

Fylkeskommunen har også en rutine for «Slik gjør vi ved innsyn etter personopplysningsloven». Rutinen viser til gjeldende rettsregler, og er godkjent i tidligere Vestfold og Telemark fylkeskommune i 2022, men gjelder frem til ny rutine er vedtatt. Denne viser retten til innsyn,

[36] En kode som brukes for å utveksle data mellom to forskjellige systemer eller apper.

unntak fra innsynsretten og steg for steg hvordan innsyn skal behandles. Rutinen viser også til informasjonsplikten og henviser til rutine for informasjonsplikt. Rutine for informasjonsplikt ble også sist revidert i 2022 i Vestfold og Telemark fylkeskommune, men er gjeldende. Rutinen for informasjonsplikt spesifiserer at som utgangspunkt skal informasjonen gis skriftlig. Den inneholder også mer konkret oversikt over hvilken informasjon den registrerte skal få, reglene for viderebehandling til andre formål og unntak fra informasjonsplikten. Fylkeskommunen opplyser at arbeidet med å revidere disse to rutinene og tilhørende maler er igangsatt.

Det føres statistikk over innsynsbegjæringer generelt. Fylkeskommunen har gjort en manuell opptelling for å gi et bilde av hvor mange innsynsbegjæringer som gjelder innsyn etter personvernreglene:

Tidsrom	Dokumentkategori	Antall totalt	Antall innsynskrav i personopplysninger
2024	Innsynskrav i	102	12
2024	Dokument inn med tittel «innsyn»	7	5
2024	E-post inn med tittel «innsyn»	69	4
2025*	Innsynskrav i	88	2
2025*	Dokument inn med tittel «innsyn»	5	3
2025*	E-post inn med tittel «innsyn»	25	4

*Tabell 8. Tall for 2025 er pr august 2025**

Arkivet har søkt på dokumentkategorien «Innsynskrav i» og etter dokumenter og e-poster som har «innsyn» i dokumenttittelen[37]. Opptellingen viser at 21 av 178 innsynsbegjæringer i 2024 gjaldt innsyn i personopplysninger spesielt, og 9 av 118 innsynsbegjæringer i 2025. Det kan være innsynskrav som er registrert uten ordet innsyn, innsynskrav som ikke er registrert eller flere dokumenter om samme sak, som ikke er med i tellingen.

Praksis

Fylkeskommunen har fem ulike personvernserklæringer tilpasset ulike grupper registrerte:

- pasienter
- skoleskyss
- ansatte
- elever i videregående
- innbyggere

Personvernerklæringene er tilgjengelig på fylkeskommunens nettside. Det er også en generell erklæring om personvern og rettigheter. Denne omtaler ikke formålene med behandlingen av personopplysningene og det rettslige grunnlaget for behandlingen, men det vises til erklæringene

[37] Det ble fjernet dokumenter som bare inneholdt ordet, men ikke var et krav.

for de ulike tjenesteområdene for slik informasjon. Personvernerklæringene informerer om at fylkeskommunen som regel henter informasjon direkte fra den registrerte, men i noen tilfeller fra andre offentlige myndigheter eller offentlige registre som for eksempel NAV, Folkeregisteret, Skatteetaten og Brønnøysundregistrene. Det står videre at personopplysningene kan bli utlevert til andre offentlige aktører som har lovlig grunnlag for å bruke opplysningene i sin saksbehandling, blant annet NAV, Skatteetaten, Statistisk sentralbyrå, Utdanningsdirektoratet, Lånekassen. Det vises også til at når fylkeskommunen benytter systemer hos eksterne leverandører, foreligger det databehandleravtale.

I den generelle erklæringen står ikke identiteten og kontaktopplysningene til den behandlingsansvarlige eller eventuelt den behandlingsansvarliges representant, men e-post-adresse til fylkeskommunens postmottak oppgis. Informasjon om hvem som er personvernombud og kontaktinformasjon fremgår ikke i den generelle erklæringen, men står oppgitt på fylkeskommunens nettside om personvern, som lenker til personvernerklæringen.

Det opplyses generelt at personopplysninger blir lagret bare så lenge det er nødvendig for at fylkeskommunen skal kunne behandle saken eller utføre den aktuelle tjenesten. Hvor lenge det er lov til å lagre opplysninger er avhengig av om hva som er formålet med at opplysningene ble registrert, og om de er arkivpliktige. Arkivpliktige opplysninger blir lagret på ubestemt tid i fylkeskommunens arkiv.

Retten til å be om innsyn, korrigering av uriktige, utdaterte eller ufullstendige personopplysninger og retten til å be om sletting er beskrevet. Det står også om begrensning og retten til dataportabilitet. Retten til å protestere er ikke omtalt, men det opplyses om klageretten til Datatilsynet.

Praksis ved tannklinikkene

Vi har undersøkt personvernerklæringen som gjelder for tannlegepasienter i fylkeskommunens tannhelsetjeneste. Her er det informasjon om formålene med konkrete behandlinger av personopplysninger, samt det rettslige grunnlaget for behandlingen. Det står at det kan være aktuelt med utlevering av personopplysninger om pasienter i forbindelse med refusjon fra Helfo. Det står også at det brukes ekstern leverandør til SMS-varsling, og hvilken løsning som benyttes til å sende røntgenbilder til andre deler av tannhelsetjenesten.

Det fremgår av erklæringen at behandlingsansvarlig for personopplysningene er fylkestannlegen. Kontaktinformasjonen til personvernombudet står også i erklæringen.

Det står at personopplysningene oppbevares så lenge det er nødvendig for å ivareta behov for helsehjelp og for å dokumentere gitt behandling, men henvisning til pasientjournalloven § 25, og at i de fleste tilfeller blir personopplysningene oppbevart permanent. Det opplyses om rett til innsyn, retting og sletting av deler av journalen med henvisning til helsepersonelloven, begrensing av behandling, dataportabilitet og klage.

På hver tannklinikk er det en skjerm i resepsjonen/venterommet med informasjon om innsyn. På skjermen er det en QR kode som kan skannes for å komme til personvernserklæringen for tannhelse.

Ansatte som har mottatt eller behandlet et krav om innsyn i personopplysninger, mener i hovedsak at de hadde nok kunnskap eller fant tilstrekkelig informasjon til å kunne behandle kravet i tråd med lovverket.

Skolene
Personvernerklæringen for elever i videregående opplæring informerer om konkrete formål for ulike behandlinger av personopplysninger i ulike systemer. Det opplyses også om det rettslige grunnlaget for behandlingen. Det spesifiseres at opplysninger om elever gis til tredjepart bare når det er en lovbestemt plikt til det, blant annet PAS/PGS, Statens Lånekasse for utdanning, Statistisk Sentralbyrå og Nasjonal vitnemålsdatabase.

Det fremgår av erklæringen at Telemark fylkeskommune ved fylkessjef for utdanning, folkehelse og tannhelse har det daglige behandlingsansvaret, og er ansvarlig for at personopplysningene behandles på en lovlig måte. Kontaktinformasjon eller hvem som er personvernombud fremgår ikke av erklæringen.

Det står at arkivpliktige opplysninger blir lagret på ubestemt tid i fylkeskommunens arkiv. Det vises til at flere konkrete opplysninger må oppbevares for å ivareta fylkeskommunens plikter i forbindelse med eventuell klagesak. Det opplyses videre om konkrete sletterutiner for ulike systemer. For tre ulike Vigo-løsninger[38] er det kun oppgitt at sletterutiner avhenger av formålet med at opplysningene ble registrert og om de er arkivpliktige.

Personvernerklæringen for elever i videregående opplæring gir ikke informasjon om hvilke rettigheter elevene har som registerte. Informasjon om dette finnes på fylkeskommunens nettsider om personvern. I fylkeskommunens rutiner for elevoppfølging står det at kontaktlærer skal gå gjennom personvernerklæringen sammen med elevene ved starten av hvert skoleår. Det er ikke spesifisert hvilken personverserklæring som skal gjennomgås. En av de to skolene kjenner til rutinen om at kontaktlærer skal informere om elevens rett til innsyn. Ingen av skolene har innarbeidet denne oppgaven i kontaktlærernes sjekklister for skolestart. Vår spørreundersøkelse viser at 32% av kontaktlærerne som har svart, ikke vet om skolen gir elever informasjon om hvor de finner fylkeskommunens personvernerklæring eller hvordan personopplysninger blir behandlet. 41% av kontaktlærerne mener at elever i svært liten eller liten grad får slik informasjon [39]. Blant andre ansatte er det omtrent 50% som ikke vet om skolen gir denne informasjonen til elevene. Blant de som har en oppfatning, er det gjennomsnittlige svaret at informasjon gis i liten grad. Vi ser

[38] Levert av selskapet NOVARI IKS (tidligere kalt Vigo).
[39] Snitt på 2,8 hvor skalaen går fra 1 som er i svært liten grad til 6 i svært stor grad. Standardavvik på 1,5.

samme tendensene for informasjon om elevenes rett til innsyn, retting eller sletting i egne personopplysninger.

Vi får opplyst at skolene bruker to ulike skjema for samtykke til utveksling og innhenting av opplysninger og for fotografering og filming av elever. Samtykkeskjemaet for deling og/eller innhenting av opplysninger, gir mulighet til å samtykke til deling med og innhenting fra følgende aktører/instanser: mor, far, annen familie, PPT, BUPA, Oppfølgingstjenesten, Barneverntjenesten i aktuell kommune, rus- og psykiatritjenesten i aktuell kommune, aktuell skole, aktuell fagopplæring, skolehelsetjenesten, NAV, samt eventuelt andre relevante instanser.

Ifølge intervju og vår spørreundersøkelse er det rektor eller andre i ledelsen som behandler krav om innsyn i personopplysninger. Ingen av de to rektorene har opplevd å få krav om retting eller sletting. En av skolene trekker frem at jobben med krav om innsyn er omfattende, og at det er risiko for manglende oversikt over personopplysningene som følge av at skolene har to arkiv[40]. I tillegg har det ene arkivet flere historiske versjoner (Gamle Telemark, Vestfold og Telemark og dagens Telemark).

2.7.1. Revisors vurdering av ivaretakelse av registrertes rettigheter

Fylkeskommunen har tiltak for å ivareta registrertes rettigheter - personvernerklæringer og andre informasjonstiltak, samt rutiner. Vi ser enkelte mangler i informasjonen som gis i personverserklæringene, og noen mangler i etterlevelsen av rutiner.

Alle personvernerklæringene bør opplyse om hvem som er behandlingsansvarlig og gi kontaktinformasjon til personvernombudet, jf. personvernforordningen art. 13 nr. 1 bokstav a) og b). Behandlingsansvarlig er fylkesdirektøren. Informasjon om behandlingsansvarliges representant skal eventuelt være supplerende informasjon.

Både den generelle personvernserklæringen og personvernserklæringen for elever i videregående opplæring mangler kontaktopplysninger til personvernombudet. Denne informasjonen skal gis ved innsamling av personopplysningene. Personvernserklæringene benyttes til dette formålet, og burde inneholdt kontaktinformasjon, selv om dette fremgår annet sted på fylkeskommunens nettside (se kap 2.2.).

Dersom behandlingen er basert på «berettiget interesse» eller en «oppgave i allmennhetens interesse» jf. personvernforordningen artikkel 21 og 6 nr. 1 bokstav e) eller f), skal det informeres om retten til å protestere. Disse behandlingsgrunnlagene gjelder for enkelte behandlinger av personopplysninger om innbyggere i fylkeskommunen, jf. personvernerklæringen for innbyggere. Slik informasjon bør derfor gis der.

Fylkeskommunen skal på tidspunktet for innsamling av personopplysninger gi den registrerte informasjon om hvilket tidsrom personopplysningene vil bli lagret. Dersom dette ikke er mulig, skal

[40] Arkivsystemet 360 og InSchool.

det informeres om kriteriene som brukes for å fastsette dette tidsrommet, jf. personopplysningsforordningen art 13 nr.2 bokstav a). Vi ser at det for ulike Vigo-løsninger kun er oppgitt at sletterutiner avhenger av formålet med at opplysningene ble registrert og om opplysningene er arkivpliktige. Denne informasjonen gir ikke den registrerte mulighet til å vurdere hvor lenge deres opplysninger blir behandlet/lagret, og er ikke tilstrekkelig.[41]

Personvernerklæringen for elever i videregående opplæring opplyser ikke om de registrertes rettigheter. Slik informasjon finnes i erklæringen «Generelt om personvern og dine rettigheter». Det fremgår ikke av fylkeskommunens rutiner hvilken personvernerklæring kontaktlærere skal gjennomgå med elevene, og det er derfor risiko for at elevene ikke får denne informasjonen. Det skal ikke være nødvendig for brukerne å måtte lete etter informasjon om behandling av personopplysninger[42].

Fylkeskommunen bør sikre at elever i videregående opplæring får informasjon om sine rettigheter på tidspunktet for innsamling av personopplysninger, i samsvar med fylkeskommunens rutiner.

2.8. Databehandleravtaler

Telemark fylkeskommune skal ha tiltak for å sikre at fylkeskommunen har databehandleravtale med alle databehandlere.

I Policy for behandling av personopplysninger står det at alle databehandlere skal reguleres med databehandleravtale. Det står også at databehandlere skal kontrolleres og revideres etter behov.

På intranettet står det at når fylkeskommunen setter ut hele eller deler av behandlingen av personopplysninger til en annen virksomhet, skal det inngås en databehandleravtale. Formålet med avtalen er å å sikre at personopplysningene kun brukes til det angitte formålet, og etter fylkeskommunens instrukser. Det refereres til personvernforordningen artikkel 28 og 29.

Aktuell leder i fylkeskommunen skal inngå databehandleravtale, vanligvis den som inngår hovedavtalen med leverandør. For å kontrollere lovligheten, må leder ta kontakt med personvernkoordinator i seksjonen (eller sikkerhetsrådgiver, eventuelt personvernombud) for å sørge for at

- systemoversikten oppdateres
- databehandleroversikten oppdateres
- tilknyttet behandlingsprotokoll oppdateres

Avtalen signeres med underskrift eller elektronisk signatur. Det vises til at delegeringsreglementet skal følges. Leder må sørge for at både hovedavtalen og databehandleravtalen arkiveres.

---

[41] Det vises til Datatilsynets avgjørelse i Sats-saken.
[42] Datatilsynets veileder. *Informasjon og åpenhet*. Sist endret 28.03.25.

Fylkeskommunen har en egen veiledning for arkivering av databehandleravtaler og vurderingen av avtalens lovlighet.

Fylkeskommunen har en mal for databehandleravtale som tilsvarer DFØ[43] sin mal.

Fylkeskommunens rutiner sier at det skal gjøres en risiko- og sårbarhetsanalyse, for å forsikre seg om at databehandleren har tilstrekkelig sikkerhetsnivå. Databehandler må kunne dokumentere hvordan de arbeider med informasjonssikkerhet. Personvernombudet skriver i årsrapporten for 2024 at fylkeskommunen ikke arbeider systematisk med leverandøroppfølging utover det som gjøres i forbindelse med anskaffelsesprosessen. Ombudet skisserer hvordan risikovurdering og leverandøroppfølging bør ivaretas. Dette arbeidet har ikke kommet i gang per november 2025.

2.8.1. Stikkprøver

Vi har undersøkt om det foreligger databehandleravtale for et uvalg behandlinger hvor fylkeskommunen benytter databehandler.

Utvalget databehandlere er basert stikkprøvene av utvalgte behandlingsaktiviteter:

- Dokumentasjon av feil, mangler og hendelser på fylkesvegnettet
- Klagebehandling i tannhelsetjenesten
- Tannhelsehjelp - behandling og journalføring i EPJ
- Avbrudd i studieåret
- Rekruttering
- Samtalebot Hugin
- Oppfølgingstjenester VGS
- Adgangskontroll -eiendom

Vi har sett på følgende databehandlere[44]:

- Gyldendal
- ACOS
- Tieto Norway AS
- Microsoft
- Triona
- Opus systemer AS, med underleverandør 21st Century mobile
- Plandent AS
- Ferrule media
- Visma
- Novari (tidligere VIGO IKS)
- OpenAI

[43] Direktoratet for forvaltning og økonomistyring.
[44] For flere av behandlingsaktivitetene er det brukt mer enn en databehandler, og samme databehandler er også brukt for flere aktiviteter.

- Xledger AS

Vi fant databehandleravtaler med ni av leverandørene. De fleste databehandleravtalene er tilgjengelige via fylkeskommunens protokoll. Vi fant ikke oppdaterte databehandleravtaler med Novari IKS, og en av avtalene var ikke oppdatert med den nye fylkeskommunen som avtalepart.

I forkant av stikkprøvekontrollen fikk vi opplyst at fylkeskommunen selv er kjent med at det mangler noen databehandleravtaler, men at dette ivaretas nå ved nye anskaffelser. Videre at GRC-verktøyet gir informasjon om manglende avtaler, og at det jobbes med å skaffe avtaler og oppdatere avtaler der det er mangler.

2.8.2. Revisors vurdering av databehandleravtaler

Fylkeskommunen har rutiner for å inngå databehandleravtale med alle databehandlere.

Fylkeskommunen gyldige databehandleravtaler med de fleste databehandlerne som vi har undersøkt. Fylkeskommunen er selv kjent med at det mangler databehandleravtaler. GRC-verktøyet vil gjøre det enklere å få oversikt over hvor det mangler avtaler.

3. Konklusjoner og anbefalinger

3.1. Konklusjoner

Har Telemark fylkeskommune etablert tiltak for å ivareta kravene i personopplysningsloven?

Fylkeskommunen har etter fylkesdelingen etablert et nytt og omfattende styringssystem for informasjonssikkerhet og personvern, inkludert rutiner, prosedyrer og et dedikert organisasjonsnettverk med personvernombud og koordinatorer på sektornivå.

Det er innført et GRC-verktøy (Governance, Risk and Compliance) for systematisk protokollføring av behandlingsaktiviteter, risikovurderinger og oversikt over databehandlere.

Fylkeskommunen har med dette etablert tiltak for å ivareta kravene i personopplysningsloven.

Som fylkeskommunen selv påpeker, gjenstår det noe opplæring- og implementeringsarbeid, særlig i skolene. Flere tiltak er beskrevet i årshjul og planer.

Våre stikkprøver viser at protokollen over behandlingsaktiviteter, risikovurderinger og databehandleravtaler på revisjonstidspunktet ikke er fullstendig, og at det er et etterslep etter fylkesdelingen. Dette er fylkeskommunen kjent med, og har forut for og i løpet av revisjonen gjort flere tiltak for å fange opp nye behandlinger, sikre protokollføring og databehandleravtaler m.m.

Fylkeskommunens tiltak for å vurdere personvernkonsekvenser når det foreligger høy risiko (DPIA) har så langt ikke ivaretatt at DPIA gjennomføres i alle tilfeller der det sannsynligvis er en høy risiko for fysiske personers rettigheter og friheter. Det er grunn til å tro at dette på sikt vil bli ivaretatt når protokollen blir fullstendig, ved hjelp av det nye verktøyet for protokoll (GRC-verktøyet).

Informasjon om registrertes rettigheter gis hovedsakelig gjennom personvernerklæringer, men disse inneholder ikke alltid all relevant og lovpålagt informasjon.

Hvordan blir personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern fulgt opp i praksis i fylkeskommunens virksomheter?

Arbeidet med opplæring og implementering av styringssystemet er så vidt i gang høsten 2025. Vi ser derfor at personopplysningsloven og fylkeskommunens egne tiltak for å ivareta personvern bare delvis er fulgt opp i praksis ved tannklinikkene og de to undersøkte videregående skolene.

Roller og ansvar for personvern er ennå ikke tilstrekkelig forankret i hele organisasjonen, spesielt innen skole, hvor det mangler tiltak for opplæring og bevisstgjøring.

Det er mangelfull praksis for gjennomføring av risikovurderinger, godkjenning og dokumentasjon av DPIA (vurdering av personvernkonsekvenser), avvikshåndtering og tiltak for å sikre at de registrerte får tilstrekkelig informasjon om sine rettigheter.

Det er viktig at implementeringsplanene gjennomføres, og at det arbeides kontinuerlig med å ivareta en god personvernskultur. Avvikshåndtering handler om å lære av feil, slik at risikoen i neste omgang blir mindre.[45] Avviksstatistikk gir viktig informasjon for å sikre relevante og treffende tiltak, ut over den erfaringen det enkelte avvik gir. Derfor er det viktig å etablere god kultur for å melde avvik i hele organisasjonen, særlig når man har et nytt styringssystemet.

3.2. Anbefalinger

Vi anbefaler fylkeskommunen å

- fortsette arbeidet med å få en oppdatert og fullstendig protokoll og oppdaterte databehandleravtaler med alle databehandlere
- sikre at det gjøres regelmessige risikovurderinger og nødvendige DPIA i tråd med lovkrav og interne rutiner
- sørge for at personvernerklæringer gir lovpålagt informasjon og god oversikt over registrertes rettigheter, og at elever og andre mottar informasjon om sine rettigheter ved innsamling av personopplysninger
- gjennomføre planlagt opplæring/implementering og vurdere særskilte tiltak for skolene
- sikre en god kultur for å melde og følge opp avvik

[45] KS veileder «Orden i eget hus - Kommunedirektørens internkontroll»

Litteratur og kildereferanser

Lover og forskrifter

- Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysingsloven/GDPR)
    - EU-forordning 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger (generell personvernforordning/GDPR)
- Lov 22. juni 2018 nr. 83 om kommuner og fylkeskommuner (kommuneloven)
- Forskrift 17. juni 2019 nr. 904 om kontrollutvalg og revisjon
- Forskrift 25. juni 2004 nr. 988 om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)

Fylkeskommunens dokumenter

- Administrativt delegeringsreglement vedtatt av fylkesdirektøren 11.08.2025
- Delegering av myndighet fra fylkestinget vedtatt 23.10.2024
- DPIAer, samarbeidsavtale og databehandleravtaler beskrevet i rapporten
- Interne administrative rutiner/prosedyrer på området
    - roller og ansvar, behandling av personopplysninger, lagring, intern revisjon, ledelsens gjennomgang, behandlingsprotokoll, kompetanseplan, avvikshåndtering, risikovurderinger, DPIA, ivareta de registerets rettigheter og innsyn, mal for bestilling av ny programvare samt tilhørende dokumenter som maler og brukerveiledninger

- Mal fra nettverk for personvernombud i fylkeskommuner: Veiledning for utarbeidelse av personvernkonsekvensvurdering
- Sikkerhetsinstruks for informasjonssikkerhet (IT-regler)

Veiledere og elektroniske kilder

Datatilsynet: https://www.datatilsynet.no/, nettside herunder følgende veiledere:

- «Behandlingsgrunnlag», sist endret 27.07.2023, hentet 16.09.2025, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/behandlingsgrunnlag/veileder-om-behandlingsgrunnlag/
- «Etablere internkontroll», sist endret 30.10.18, hentet 26.05.25, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/
- «Grunnleggende personvernprinsipper», sist endret 16.07.19, hentet 22.05.25, https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/grunnleggende-personvernprinsipper/

- «Hvordan sikre ombudets uavhengighet?», sist endret: 06.01.2023, hentet 22.05.25, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/sikre-uavhengighet/
- «Informasjon og åpenhet», sist endret 28.03.25, hentet 13.10.25, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/gi-informasjon/informasjon-og-apenhet/
- «Hvilke brudd skal meldes til Datatilsynet», sist endret 16.10.25, hentet 31.10.25, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hvilke-brudd-skal-meldes-til-datatilsynet/
- «Risikovurdering», sist endret 13.03.24, hentet 05.06.25, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/risikovurdering/
- «Tips til nye personvernombud», sist endret 06.01.2023, hentet 29.05.2025, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/tips-til-personvernombud/
- «Hvordan gjennomføre en DPIA?», sist endret 27.07.23, hentet 05.06.25, https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/hvordan-gjennomfore-en-dpia/

Datatilsynet. «Overtredelsesgebyr til Sats», 08.02.23, https://www.datatilsynet.no/regelverk-og-verktoy/lover-og-regler/avgjorelser-fra-datatilsynet/2023/overtredelsesgebyr-til-sats/

Personvernsnemda. «PVN-2022-13 Brudd på personopplysnings- og informasjonssikkerheten i Østre Toten kommune – overtredelsesgebyr», 24. 01.23, https://personvernnemnda.no/2022/09/03/pvn-2022-13-brudd-pa-personopplysnings-og-informasjonssikkerheten-i-ostre-toten-kommune-overtredelsesgebyr/

KS (2020) Orden i eget hus – kommunedirektørens internkontroll.

Vedlegg

Vedlegg 1: Fylkesdirektørens uttalelse

Vedlegg 2: Revisjonskriterier

Vedlegg 3: Metode og kvalitetssikring

Telemark
FYLKESKOMMUNE

VTR - VESTFOLD OG TELEMARK REVISJON IKS
Postboks 311
3701 SKIEN

Fylkesdirektør

Vår dato:	27.11.2025
Deres dato:	14.11.2025
Vår referanse	25/12122-10
Deres referanse:	
Vår saksbehandler:	Ketil Reed Aasgaard
Unntatt offentlighet iht.:	Offl. § 5

Svar på høring - Forvaltningsrevisjon - personvern

Vi viser til revisjonsrapport datert 14.11.2025, og takker for muligheten til å komme med kommentarer og uttalelser.

Våre innspill følger som vedlagt.

Med hilsen

Ketil Reed Aasgaard
Fylkesdirektør
ketil.reed.aasgaard@telemarkfylke.no

Dokumentet er elektronisk godkjent og sendes uten signatur.

Vedlegg:
Forvaltningsrevisjon - personvern - høring
Høringsutkast - forvaltningsrevisjon 400404 Personvern TFK

Kopi til:
Sektor for Organisasjon og digital utvikling, Elisabeth Gylder Vingereid
Seksjon Digitale tjenester, Kaja Marlene Berg-Jensen

Telemark
FYLKESKOMMUNE

24.11.2025

Høringssvar – Forvaltningsrevisjonen Personvern

Vi viser til mottatt revisjonsrapport datert 14.11.2025, og takker for muligheten til å komme med kommentarer og uttalelse i henhold til forskrift om kontrollutvalg og revisjon § 14.

Fylkesdirektørens uttalelse til forvaltningsrevisjonsrapporten «Behandling av personopplysninger – Telemark fylkeskommune»

Telemark fylkeskommune takker for en grundig og nyttig revisjonsrapport om behandling av personopplysninger, utarbeidet av Vestfold og Telemark revisjon IKS. Rapporten gir et godt innblikk i status på fylkeskommunens arbeid med informasjonssikkerhet og personvern etter fylkesdelingen, og peker på både styrker og områder med behov for videre forbedring.

Overordnede kommentarer

Fylkeskommunen har etter delingen fra Vestfold og Telemark hatt betydelige omstillingsprosesser. Vi er tilfredse med at revisjonen anerkjenner det omfattende arbeidet som er gjort for å etablere et nytt styringssystem, innføre GRC-verktøy og bygge opp et organisasjonsnettverk med personvernombud og koordinatorer. Samtidig er vi kjent med at implementeringen av systemet fortsatt er på et tidlig stadium, og at det gjenstår opplærings- og forankringsarbeid.

Kommentarer til revisjonens funn og anbefalinger

- **Protokollføring og databehandleravtaler:** Vi er enig med revisjonen i at protokollen over behandlingsaktiviteter og oversikten over databehandleravtaler må ferdigstilles og vedlikeholdes løpende. Arbeidet med å ajourføre protokollene og innhente manglende databehandleravtaler er allerede høyt prioritert. GRC-verktøyet gir bedre oversikt, og dette arbeidet videreføres systematisk.
- **Risikovurderinger og DPIA:** Fylkeskommunen har etablert rutiner og malverk for risikovurderinger og DPIA. Vi erkjenner at det fortsatt gjenstår arbeid for å sikre regelmessige risikovurderinger i alle sektorer og virksomheter, og at DPIA gjennomføres der det er påkrevd. Dette følges opp i årshjul og kompetanseplan, og forankres i lederopplæringen høsten 2025 og videre.
- **Personvernerklæringer og informasjon til registrerte:** Fylkeskommunen tar til seg revisjonens merknader om at personvernerklæringene må oppdateres for å gi all

nødvendig og lovpålagt informasjon, herunder kontaktinformasjon til behandlingsansvarlig og personvernombud. Vi vil også styrke rutinene for at elever og andre registrerte mottar informasjon om sine rettigheter på relevante tidspunkt.

- **Opplæring og forankring, særlig i skolene:** Rapporten viser at det er et særlig behov for ytterligere opplæring og bevisstgjøring i skolesektoren. Dette er et satsingsområde i inneværende og kommende år, og tiltak vil bli vurdert og tilpasset skolens behov
- **Avvikshåndtering:** Fylkeskommunen er enig i at det må arbeides videre med å utvikle en god avvikskultur og sikre at brudd meldes i henhold til rutiner. Arbeidet med å gjøre meldesystemet mer brukervennlig og å tydeliggjøre terskelen for avviksrapportering pågår.

Avsluttende kommentarer Personvern og informasjonssikkerhet er høyt prioritert i Telemark fylkeskommune. Vi ser rapporten som et verdifullt bidrag til vårt forbedringsarbeid, og vil følge opp anbefalingene i tråd med den planen som er skissert i styringssystem og årshjul. Vi vil særlig vektlegge implementering av rutiner og systematisk opplæring, og sikre at forankringen skjer på alle nivåer i organisasjonen.

Vi takker for samarbeidet med revisjonen i prosessen, og vil rapportere på fremdrift og tiltak til kontrollutvalget på egnet måte.

Vedlegg 2: Revisjonskriterier

Fylkeskommunens ansvar for forsvarlig håndtering av personopplysninger er regulert av personopplysningsloven. Personopplysningsloven gjennomfører EUs personvernforordning (GDPR) i norsk rett, jf. personopplysningsloven § 1. Loven innledes med de norske særreglene, inndelt i paragrafer, før forordningsteksten, som er inndelt i artikler (art.), følger. I rapporten vil vi derfor henvise til noen bestemmelser som paragrafer, og til andre som artikler.

Personopplysningsloven og forordningen gjelder for helt eller delvis automatisert behandling (typisk elektronisk) av personopplysninger og for ikke-automatisert behandling av personopplysninger dersom opplysningene inngår i eller skal inngå i et strukturert register, jf. personopplysningsloven § 2. Formålet med reglene er blant annet å sikre vern av fysiske personers grunnleggende rettigheter og friheter i forbindelse med behandling av personopplysninger.

Noen definisjoner

- **Personopplysninger** er enhver opplysning om en identifisert eller identifiserbar fysisk person, jf. personvernsforordningen art. 4, nr. 1.
- **Behandling** av personopplysninger er enhver operasjon som gjøres med personopplysninger.
- **Behandlingsansvarlig** er en fysisk eller juridisk person, offentlig myndighet m.m. (f.eks. Telemark fylkeskommune) som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes, jf. personopplysningsloven art. 4.
- **Den registrerte** er den fysiske person som opplysninger kan knyttes til.

Personvernombud

Regler om personvernombud står i personvernforordningen art.37, 38 og 39. Offentlige myndigheter og organer som behandler personopplysninger, skal utpeke personvernombud. Personvernombudet skal gi råd til ledelsen, kontrollere at virksomheten følger personopplysingsloven og være kontaktpunkt for Datatilsynet.

Personvernombudet skal utpekes på grunnlag av faglige kvalifikasjoner, dybdekunnskap om personopplysningsloven og praksis på området, samt evne til å utføre oppgavene. Personvernombudet kan være en ansatt, eller man kan kjøpe tjenesten.

Personvernombudet skal ikke ha andre oppgaver som kommer i konflikt med rollen, og kan ikke avsettes eller straffes for å utføre sine oppgaver som personvernombud. For å unngå å komme opp i situasjoner med konflikt eller misforståelse om rollen og oppgavene til ombudet, bør man tydelig definere arbeidsoppgaver og ansvarsforholdet mellom ombudet og virksomheten[46].

[46] Datatilsynets veileder. *Hvordan sikre ombudets uavhengighet?* Sist endret: 06.01.23

Virksomheten skal legge til rette for ombudets uavhengighet, dvs. sikre at personvernombudet ikke mottar instrukser om utførelsen av oppgavene som personvernombud. Ombudet skal selv prioritere og disponere sin tid innen de ressursrammer som er blitt gitt ombudsrollen[47].

Datatilsynet anbefaler at personvernombudet rapporterer til ledelsen. Rapporteringen skal bidra til å sikre at personvernarbeidet prioriteres, og at ledelsen er informert om status, utfordringer og tiltak. Rapportering kan skje gjennom både skriftlige rapporter og faste møter. Datatilsynet anbefaler at det etableres formelle strukturer for å sikre ledelsens oppmerksomhet.[48]

Personvernprinsippene

Når virksomheter behandler personopplysninger, skal behandlingen baseres på personvernprinsippene i personvernforordningen art. 5. Prinsippene er:

- lovlighet, rettferdighet og åpenhet
- formålsbegrensning
- dataminimering
- riktighet
- lagringsbegrensning
- integritet og fortrolighet
- ansvarlighet

Personopplysningsloven bygger på disse prinsippene, som er utdypet i Datatilsynets veileder.[49]

Lovlig, rettferdig og gjennomsiktig

Personvernforordningen art. 6 regulerer i hvilke tilfeller det er lovlig å behandle personopplysninger (behandlingsgrunnlaget). Behandlingsgrunnlaget for fylkeskommunen er gjerne at behandlingen er nødvendig for å oppfylle en rettslig forpliktelse eller for å utøve offentlig myndighet. Ellers kan grunnlaget være samtykke fra den registrerte. For særlige kategorier av personopplysninger[50] må tilleggsvilkår være oppfylt, for at behandlingen skal være lovlig, jf. forordningen art. 9 nr.2.

Formålsbegrensning

Personopplysninger skal bare brukes til det formålet de er innhentet for, jf. art. 6, nr. 1, eller til nye formålet som har behandlingsgrunnlag og er forenelig med det opprinnelige formålet.

Dataminimering

Den som behandler personopplysninger skal begrense innsamlingen til personopplysninger som er nødvendig for formålet, jf. personvernforordningen art. 5, nr. 1, bokstav c.

---

[47] Datatilsynets veileder. *Hvordan sikre ombudets uavhengighet?* Sist endret: 06.01.23
[48] Datatilsynets veileder. *Tips til nye personvernombud*. Sist endret 06.01.23
[49] Datatilsynets veileder. *Grunnleggende personvernprinsipper*. Sist endret 16.07.19
[50] Definert i personvernsforordningen art 9: personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering.

Riktighet
Personopplysninger som behandles skal være korrekte. Behandlingsansvarlig skal treffe rimelige tiltak for å sikre at personopplysninger som er uriktige, slettes eller rettes, jf. art. 5, nr. 1 bokstav d.

Lagringsbegrensning
Personopplysninger skal lagres slik at de slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for, jf. personvernforordningen art. 5, nr. 1, bokstav e.

Integritet og fortrolighet
Fylkeskommunen skal sørge for personopplysningenes integritet og fortrolighet, jf. personvernforordningen art. 5, nr. 1 bokstav f. Dette kan inkludere

- beskyttelse mot at uvedkommende får tilgang
- beskyttelse mot utilsiktet tap og endring
- sikre tilgjengelighet for de som skal ha tilgang når de trenger det
- tiltak for å unngå at et ubegrenset antall mennesker får tilgang
- tiltak for å overvåke og håndtere sikkerhetsbrudd
- systemer som beskytter mot angrep og uhell

Ansvarlighet
Fylkeskommunen må kunne sikre og vise at den faktisk opptrer i samsvar med personvernreglene, jf. personvernforordningen art. 5, nr. 2, dvs at den behandlingsansvarlige må ha internkontroll.

Internkontroll

Den behandlingsansvarlige skal gjennomføre egnede tekniske og organisatoriske tiltak og retningslinjer for å sikre og påvise at behandlingen utføres i samsvar med forordningen, jf. personvernforordningen art. 24. Dette er et krav om internkontroll.

Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen, jf. eForvaltningsforskriften § 1. Også her er det krav om internkontroll. Internkontrollen skal basere seg på anerkjente standarder for styringssystem for informasjonssikkerhet, og bør være integrert i virksomhetens helhetlige styringssystem. Mål og strategi for informasjonssikkerhet skal beskrives. Internkontrollen skal være tilpasset risiko, og stille krav til bla. prosedyrer for behandling av personopplysninger og taushetsbelagt informasjon hvis det er relevant, jf. § 15 g, jf. §§ 5 og § 26, se også personvernforordningen art 32 og 33.

Datatilsynets veileder for internkontroll og informasjonssikkerhet legger til grunn at internkontrollen skal bestå av[51]:

- styrende elementer, som i hovedsak retter seg mot ledelsen, herunder hvilke beslutninger og føringer de legger for internkontroll
- gjennomførende elementer, som i hovedsak retter seg mot ansatte (rutiner o.l.)

[51] Datatilsynets veileder. *Etablere internkontroll*. Sist endret 30.10.18

- kontrollerende elementer (avvikshåndtering og periodiske gjennomganger).

Styrende elementer
Typiske styrende elementer er blant annet tydelig plassering av ansvar og myndighet.

Videre må virksomheten identifisere hvilke personopplysninger som behandles og vurdere risiko. Ved behandlinger som vil medføre høy risiko for fysiske personers rettigheter og friheter, skal konsekvenser for personvernet vurderes særskilt (DPIA[52]), jf. personvernforordningen art. 35. Dette er f.eks. aktuelt for sensitive opplysninger f.eks. i videregående skole og tannhelse.

Vurderingen skal minst inneholde

a) systematisk beskrivelse av planlagte behandlingsaktiviteter og formål med behandlingene,
b) omtale av om behandlingsaktivitetene er nødvendige og står i rimelig forhold til formålene,
c) en vurdering av risikoene for de registrertes rettigheter og friheter, og
d) planlagte tiltak for å håndtere risikoene og påvise at personvernreglene overholdes.

Til slutt må man bedømme og evaluere, og eventuelt godkjenne vurderingen (DPIA). I denne fasen har ledelsen den viktigste rollen. Arbeidet skal sammenstilles og funn presenteres for ledelsen[53]. Vurdering og beslutning skal framgå i eget dokument.

Gjennomførende elementer
Etter at nødvendige kartlegginger og vurderinger er gjort, må fylkeskommunen lage tekniske og organisatoriske tiltak som sikrer at behandlingen utføres i samsvar med personvernsforordningen, og for å oppnå et tilstrekkelig sikkerhetsnivå, jf. personvernforordningen art. 24, og art. 32. Dette inkluderer bla nødvendige og fungerende rutiner og prosedyrer.

Personvernforordningen art. 30 krever at den behandlingsansvarlige fører protokoll over behandlingsaktiviteter. En protokoll skal inneholde følgende informasjon:

a. navnet og kontaktopplysningene til den behandlingsansvarlige/den felles behandlingsansvarlige, den behandlingsansvarliges representant og personvernombudet,
b. formålet med behandlingen,
c. en beskrivelse av kategoriene av registrerte og kategoriene av personopplysninger,
d. kategoriene av mottakere som opplysningene blir utlevert til, herunder i tredjestater m.m.
e. dersom det er relevant, overføringer av personopplysninger til en tredjestat m.m.
f. om mulig, planlagte tidsfrister for sletting av de forskjellige kategoriene av opplysninger,

[52] DPIA står for Data Protection Impact Assessment.
[53] Datatilsynets veileder. Hvordan gjennomføre en DPIA? Sist endret 27.07.23

g. om mulig, beskrivelse av etablerte sikkerhetstiltak[54]

Kontrollerende elementer
Fylkeskommunen skal ha et system for å fange opp brudd på personopplysningssikkerheten. Hvis det oppstår brudd på sikkerheten rundt personopplysninger, skal fylkeskommunen som hovedregel melde fra til Datatilsynet. Dersom det er sannsynlig at bruddet vil føre til risiko for personene det gjelder, skal fylkeskommunen også underrette de registrerte. Alle brudd på personopplysningssikkerheten skal dokumenteres, jf. personvernforordningen art. 33 og 34.

Internkontrolltiltakene skal gjennomgås og oppdateres ved behov, jf. personvernforordningen art. 24. Datatilsynet anbefaler[55] at risikovurderinger skal gjennomføres før personopplysninger behandles og før systemene tas i bruk. Virksomheten skal også gjennomføre risikovurdering ved endringer i forhold som kan påvirke informasjonssikkerheten, slik som endringer i behandlingene, oppdateringer eller fornyelser av systemer eller endringer i trusselbildet. I uttalelser fra Datatilsynet og Personvernsnemda går det fram at det skal jobbes systematisk og strukturert med IKT-sikkerhet, særlig gjennom risiko- og sårbarhetsanalyser, for å identifisere behovet for risikoreduserende tiltak. Rapporteringer fra NSM og NorSIS peker på at det er økende trussel mot informasjonssikkerheten, og dette stiller etter nemndas syn krav til regelmessige risikovurderinger[56]. Internkontroll og arbeidet med informasjonssikkerhet er et dynamisk arbeid som alltid vil være under utvikling. Det følger av at

Datatilsynet anbefaler å ha rutiner for å forbedre internkontrollen, herunder rutiner for rapportering fra sikkerhetshendelser, avvikshåndtering og egenkontroll. Rapporteringen skal beskrive hvilke erfaringer som er gjort og inneholde forslag til forbedringer. Det bør også avklares hvem som har ansvar for oppdateringer.

Den registrertes rettigheter

Personvernforordningen kapittel III omhandler den registrertes rettigheter overfor den behandlingsansvarlige. Art. 12 krever at den behandlingsansvarlige skal gi klar og tydelig informasjon til den registrerte. Datatilsynet anbefaler kommunen å ha en personvernerklæring på sine nettsider, med generell informasjon om kommunens personvernpolicy. Den registrerte skal få informasjon ved innsamling av opplysningene (art. 12, 13 og 14).

Den registrere har rett til innsyn i de personopplysningene den behandlingsansvarlige har om vedkommende (art. 15). Den registrerte skal ha rett til å få rettet uriktige personopplysninger om seg selv (art. 16), og kan også i spesielle tilfeller ha rett til å få slettet personopplysninger om seg

[54] Dette kan for eksempel være: pseudonymisering og kryptering av personopplysninger, evne til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene, evne til å gjenopprette tilgjengeligheten og tilgangen, en prosess for regelmessig testing, analysering og vurdering av hvor effektive sikkerhetstiltakene er. jf. personvernsforordningen art 32. nr. 1
[55] Datatilsynet. *Risikovurdering*. Sist endret 13.03.24
[56] Personvernsnemda. *Brudd på personopplysnings- og informasjonssikkerheten i Østre Toten kommune – overtredelsesgebyr* (PVN-2022-13).

selv (art. 17). Det er noen unntak fra disse reglene, bl.a. for opplysninger som skal bevares for arkivformål, eller som må bevares for å oppfylle en rettslig forpliktelse. Det er videre en rett til å be om begrensning av behandlingen og å protestere mot behandlingen. Den registrerte har rett til dataportabilitet (å kunne ta med sine personopplysninger over til en annen virksomhet).

Databehandleravtale

I noen tilfeller behandler en ekstern leverandør personopplysninger på vegne av den behandlingsansvarlige – man benytter en databehandler. En databehandler kan f.eks. være en leverandør av et system/programvare der det behandles personopplysninger, dersom leverandøren har oppgaver knyttet til oppdateringer, lagring, sikkerhetskopiering m.v. Forholdet mellom en behandlingsansvarlig virksomhet og databehandleren skal være regulert i en databehandleravtale, jf. personvernforordningen art. 28 nr. 3. Databehandleravtalen skal sikre at personopplysningene blir behandlet i samsvar med regelverket, også av databehandleren. En databehandleravtale kan være en frittstående avtale mellom partene, eller en integrert del av annet avtaleverk.

Den behandlingsansvarlige kan bare benytte databehandlere og underleverandører som kan dokumentere tilstrekkelige garantier for at kravene i personopplysningloven blir ivaretatt og at personopplysningene som behandles er tilstrekkelig sikret (personopplysningsloven art. 28 nr. 1). Den behandlingsansvarlige skal vurdere om databehandleren gir tilfredsstillende garantier for de personopplysningene som skal behandles.

En databehandleravtale skal inneholde:

- behandlingens art, formål og varighet
- kategorier av registrerte og typer av personopplysninger
- pliktene og rettighetene til den behandlingsansvarlige
- forpliktelsene til databehandleren

Revisjonskriterier

På denne bakgrunn har vi utledet følgende revisjonskriterier:

Fylkeskommunen skal ha:

- en organisasjon med klar plassering av ansvar og myndighet for behandlingen av personopplysninger, samt rutiner eller tiltak for rapportering
- personvernombud, organisert i samsvar med personopplysningsloven
- protokoll over hvilke personopplysninger fylkeskommunen behandler
- kartlagt risiko/risikovurderinger
- dokumenterte vurderinger av personvernkonsekvenser (DPIA) der dette er aktuelt.
- rutiner og tiltak for å håndtere brudd på personopplysningssikkerheten
- tiltak for å ivareta de registrertes rett til informasjon og innsyn
- tiltak for å sikre at fylkeskommunen har databehandleravtale med alle databehandlere

Vedlegg 3: Metode og kvalitetssikring

Forvaltningsrevisjonen startet opp ved oppstartsbrev 26.mai 2025. Oppstartsmøte ble holdt 4.juni 2025 med fylkesdirektør, fylkessjef for Organisasjon og digital utvikling, seksjonsleder for Digitale tjenester og personvernombudet i fylkeskommunen til stede. I møtet presenterte vi prosjektplanen med problemstillinger, kilder for revisjonskriterier og plan for gjennomføringen.

Forvaltningsrevisjoner skal gjennomføres på en måte som sikrer at informasjonen i rapporten er relevant og pålitelig. At dataene er relevante (gyldige/valide) innebærer at de beskriver de forholdene som problemstillingene omhandler. Pålitelighet (reliabilitet) handler om at innsamling av data skal skje så nøyaktig som mulig og at det ikke har skjedd systematiske feil underveis.

Nedenfor redegjør vi for datagrunnlaget og metoder vi har brukt for å svare på problemstillingene. Vi vil også beskrive hvilke tiltak som er brukt for å sikre dataenes relevans og pålitelighet.

Innsamling av data, relevans og pålitelighet

Datainnsamling og rapportskriving har foregått i perioden juni – oktober 2025.

For å undersøke informasjonssikkerhets- og personvernsarbeidet i fylkeskommunen har vi

- Kartlagt og gjennomgått delegeringsreglement og rutiner på området.
- Intervjuet personvernombud, sikkerhetsrådgiver merkantil, seksjonsleder for Tannhelse, personvernkoordinator for Tannhelse, rektorer ved Nome og Porsgrunn VGS med deltagere fra skoleledelsen, samt e-post intervjuer med personvernkoordinatorer for skoleutvikling og rådgiver i team skoleutvikling.
- Sendt spørreundersøkelse til alle ansatte ved alle tannklinikkene i fylkeskommunen. Det er mottatt 76 svar, det gir en svarprosent på 45%.
- Sendt spørreundersøkelse til alle ansatte[57] som behandler personopplysninger ved Nome og Porsgrunn videregående skoler. Det er mottatt 104 svar, det gir en svarprosent på 33%. Det bemerkes at det hovedsakelig er ledelsen (15%), faglærer (44%) og kontaktlærere (47%) som har svart på undersøkelsen. Rådgivere/karriereveiledere, assistenter, digitalpedagog, miljøarbeider/-terapeut/elevveileder og vikarer utgjør 11% av svarene i undersøkelsen. 15% av svarene er fra andre ansatte.
- Stikkprøver av behandlingsprotokoll, avvik, databehandleravtaler og DPIA.

Gjennomgang av dokumenter og rutiner gir data om hvordan kommunen sikrer arbeidet på området og ansvarsfordeling i kommunen, mens intervju og spørreundersøkelse kan gi data på om styrende dokumenter og rutiner blir fulgt opp i praksis og andre detaljer om faktiske forhold som er relevant for det som undersøkes.

[57] Dette inkluderer bla. drift og renhold også, 11 personer har svart at de ikke som en del av sitt arbeid behandler opplysninger om elever eller foresatte. Dermed er N=93 og svarprosenten på de fleste generelle spørsmål 29%.

Vi har intervjuet personer med kjennskap til det området revisjonen omhandler. Det er brukt semistrukturerte intervjuguider tilpasset dem vi har intervjuet. En semistrukturert intervjuguide innebærer at noen faste spørsmål er definert på forhånd, men at det også er mulig med oppfølgingsspørsmål under intervjuet. Flere av de faste spørsmålene er felles for vi har intervjuet med tilsvarende ansvarsområde for informasjonssikkerhet og personvern, dette er gjort for å få informasjon om samme tema fra flere. Informasjon fra intervju er nedtegnet i referat som er bekreftet av kildene.

Ved fremstilling av resultater fra spørreundersøkelsene har vi for alle prosentandeler avrundet til nærmeste hele prosent og for gjennomsnittstall avrundet til nærmeste hele tall. Flere av prosentfordelingene vil derfor ikke summere til nøyaktig 100%.

Ved stikkprøvekontrollen i behandlingsprotokollen og av databehandleravtaler, har vi gjort utvalg. Det er kjent at det fremdeles er mange behandlinger som ikke er ferdig utfylt i protokollen. Vi har derfor ikke valgt behandlinger hvor vi visste at det var mangelfull protokollføring. Vi valgte bare ut behandlingsaktiviteter der utfyllingen i protokollen tilsynelatende var ferdig[58]. Videre har vi valgt behandlinger fra alle fylkeskommunens sektorer. Totalt har vi valgt ut ti behandlingsaktiviteter fra protokollen, vi har valgt å se på noen flere behandlingsaktiviteter innenfor tannhelse og skole – da det i denne revisjonen er valgt ut å fokusere på praksis der.

For å undersøke om det forelå databehandleravtaler har vi gjort et utvalg basert på de samme ti behandlingsaktivitetene.

Det var gjennomført kun fire DPIAer i perioden. Vi undersøkte alle disse.

Når vi ser at det er sammenfallende informasjon fra ulike metoder og kilder, er det et tegn på at dataene gir en riktig beskrivelse av det som undersøkes. Dette styrker dataenes pålitelighet og de følgende konklusjonene. Forskjeller i data være noe vi undersøker nærmere for å finne et så riktig som mulig bilde.

Vi har sjekket ut med administrasjonen at fakta i rapporten er korrekt framstilt. Rapporten er sendt fylkesdirektøren til uttalelse, jf. forskrift om kontrollutvalg og revisjon § 14. Uttalelsen ligger i vedlegg 1.

Personopplysninger

I forbindelse med denne forvaltningsrevisjonen har vi behandlet personopplysninger som navn og epostadresse til ansatte i fylkeskommunen. Vi har også sett enkelte personopplysninger om elever. Personopplysninger om elever har vært lagret hos bare mens arbeidet med forvaltningsrevisjonen pågikk, og er slettet.

[58] Fargelagt fullstendig som indikerer at alle felter i protokollen er utfylt.

Vårt rettslige grunnlag for å behandle personopplysninger er kommuneloven § 24-2 fjerde ledd.

Vi behandler personopplysninger slik det er beskrevet i vår personvernerklæring. Personvernerklæringen er tilgjengelig på vår nettside vtrevisjon.no.

God kommunal revisjonsskikk - kvalitetssikring

Forvaltningsrevisjon skal gjennomføres, dokumenteres, kvalitetssikres og rapporteres i samsvar med kommuneloven og god kommunal revisjonsskikk.[59]

Kvalitetssikringen skal sikre at undersøkelsen og rapporten har nødvendig faglig og metodisk kvalitet. Videre skal det sikres at det er konsistens mellom bestilling, problemstillinger, revisjonskriterier, data, vurderinger og konklusjoner.

Vestfold og Telemark revisjon IKS har et system for kvalitetsstyring som er i samsvar med den internasjonale standarden for kvalitetsstyring.[60] Denne forvaltningsrevisjonen er kvalitetssikret i samsvar med vårt kvalitetsstyringssystem og i samsvar med kravene i RSK 001.

[59] God kommunal revisjonsskikk i forvaltningsrevisjon og eierskapskontroll kommer til uttrykk først og fremst i RSK 001 Standard for forvaltningsrevisjon og RSK 002 Standard for eierskapskontroll. Gjeldende standarder er fastsatt av Norges Kommunerevisorforbunds styre høsten 2020. Standarden bygger på norsk regelverk og internasjonale prinsipper og standarder, fastsett av International Organization of Supreme Audit Institutions (INTOSAI) og Institute of Internal Auditors (IIA).

[60] ISQM 1 og 2 er internasjonale standarder for kvalitetsstyring og oppdragskontroll for revisjonsforetak som utfører revisjon eller forenklet revisorkontroll av regnskaper, eller andre attestasjonsoppdrag eller beslektede tjenester.

På vakt for fellesskapets verdier

Rapporten er utarbeidet av
Vestfold og Telemark revisjon IKS

Har du spørsmål til rapporten?
Ta kontakt med oss:
Telefon: 33 07 13 00
E-post: post@vtrevisjon.no

www.vtrevisjon.no

25: 4000 404