



## Forvaltningsrevisjon | Tysnes kommune Informasjonstryggleik og personvern

Februar 2024

«Forvaltningsrevisjon av  
informasjonstryggleik og personvern»

Februar 2024

Rapporten er utarbeidd for Tysnes  
kommune av Deloitte AS.

Deloitte AS  
Postboks 6013 Postterminalen, 5892  
Bergen  
tlf: 55 21 81 00

[www.deloitte.no](http://www.deloitte.no)

[forvaltningsrevisjon@deloitte.no](mailto:forvaltningsrevisjon@deloitte.no)

# Samandrag

Deloitte har, i samsvar med bestilling frå kontrollutvalet 24. november 2022 i sak 22/22 gjennomført ein forvaltningsrevisjon av informasjonstryggleik og personvern i Tysnes kommune. Føremålet med prosjektet har vore å undersøkje om kommunen har tilfredsstillande system og rutinar for informasjonstryggleik og om etablerte standardar og gjeldande lovar og reglar blir etterlevd innan dette området. Vidare har det vore eit føremål å undersøke i kva grad Tysnes kommune etterlever sentrale krav i personvernlovgevinga.

Som datagrunnlag har revisjonen nytta dokumentasjonsgjennomgang, intervju og spørjeundersøking. Undersøkinga har blitt gjennomført frå januar til september 2023.

Tysnes kommune har nyleg starta arbeidet med å etablere system og rutinar for arbeidet med informasjonstryggleik og personvern. Kommunen etablerte mellom anna *handbok i informasjonssikkerhet og IKT-strategi 2022-2025* i 2022, og det er planlagt å gjennomføre leinga si årelege gjennomgang i 2023. Arbeidet med å implementere rutinar og system var framleis var pågåande på revisjonstidspunktet. Det er etter revisjonen si vurdering ein god del som ikkje er sett i verk på revisjonstidspunktet og kommunen manglar framleis ein del for å kunne ha tilfredsstillande system og rutinar for informasjonstryggleik.

Revisjonen vurderer at Tysnes kommune sine styrande dokument på revisjonstidspunktet langt på veg er i samsvar med krav i regelverket. Kommunen har gjennom handbok for informasjonssikkerhet og IKT-strategi 2022-2025 etablert mål og strategi for arbeidet med informasjonstryggleik i kommunen og styrande dokument er vidare tilgjengeleg for dei tilsette i organisasjonen via intranett og kvalitetssystemet (Compilo). Dette er i samsvar med krav på området (jf. eForvaltningsforskrifta § 15). Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette. Revisjonen vil påpeike at Tysnes kommune, i samsvar med denne tilrådinga, bør synleggjere kva krav og /eller anerkjende standardar dei baserer sine styrande dokument på.

Digitaliseringsdirektoratet tilrår at verksemder utformar føringar for arbeidet med informasjonstryggleik, og at struktur og innhald i styringsaktivitetane blir dokumentert på ein føremålstenleg måte slik at det er tydeleg kven som skal gjere kva, og korleis det skal gjerast (slik at dokumenteringa t.d. kan nyttast som oppslagsverk for tilsette). Revisjonen vurderer at Tysnes kommune sine styrande dokument i større grad bør tydeleggjere struktur og innhald i alle styringsaktivitetar, til dømes når det gjeld gjennomføring av tryggleiksrevisjonar. Undersøkinga viser at styrande dokument ikkje gir informasjon om kva tryggleiksrevisjonar omfattar, når det skal gjennomførast eller kven som har ansvar for dette.

Revisjonen er merksam på at kommunen sine styringsdokument relativt nyleg er etablert, og at arbeidet med å implementere rutinar og system i samsvar med dette framleis var pågåande på revisjonstidspunktet.

Revisjonen vurderer at Tysnes kommune ikkje i tilstrekkeleg grad har etablert tydelege ansvarsforhold knytt til informasjonstryggleik. Undersøkinga viser at det i all hovudsak går fram av kommunen si handbok for informasjonssikkerhet kva ansvar og oppgåver som ligg til ulike rollar i kommunen når det gjeld informasjonstryggleiksarbeidet. Undersøkinga indikerer samtidig at det står att ein del arbeid med å sikre at rollar og ansvar i dette arbeidet er tilstrekkeleg tildelt, kommunisert og etterlevd. Revisjonen vil påpeike at det er øvste leing sitt ansvar å sikre det er etablert tydelege ansvarsforhold.

Revisjonen vurderer at Tysnes kommune på revisjonstidspunktet ikkje har etablert tilstrekkeleg rutinar knytt til informasjonstryggleik. Undersøkinga viser at kommunen er i prosess med å utarbeide slike rutinar og prosedyrar, men at dette per august 2023 ikkje ennå er ferdigstilt. Revisjonen vil understreke at kommunen skal sikre at internkontrollen er systematisk og at det er etablert nødvendige rutinar og prosedyrar (kommunelova §25-1).

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik på alle område. I handbok for informasjonssikkerhet blir retningslinjer for leinga sin gjennomgang skildra, og det blir vist til at det skal gjennomførast tryggleiksrevisjonar. Desse styringsaktivitetane var ikkje gjennomført på revisjonstidspunktet. For tryggleiksrevisjonane var det på revisjonstidspunktet heller ikkje etablert formelle system og rutinar der det går fram korleis å gjennomføre tryggleiksrevisjonar. Revisjonen merkar seg også at det er ein plan om å få på plass årleg rapportering om informasjonstryggleik og personvern men at dette ikkje var implementert på revisjonstidspunktet. Revisjonen påpeiker difor at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta som seier at kommunen skal ha ein internkontroll på området som baserer seg på anerkjente standardar for styringssystem for informasjonstryggleik (§ 15).

Undersøkinga viser at det er ulike system for registrering av brukartilgangar, og at det ikkje går fram av skjema for tinging av brukaridentitet kva type tilgang brukaren skal ha (til dømes lesartilgang, full tilgang). Det blir også vist til at det er behov for å etablere skjema og rutinar som sikrar at leiarar søker om endra tilgang dersom tilsette får endra arbeidsoppgåver og dermed skal ha andre tilgangar i systema. Manglande registrering av endringar fører til ein risiko for at brukarar har tilgangar dei ikkje har behov for, og følgjeleg risiko for at krava knytt til konfidensialitet i regelverket ikkje alltid blir etterlevd. Dette er forhold som revisjonen meiner at kommunen må utbetre for å ha eit tilstrekkeleg system som sikrar tilgjenge og konfidensialitet i informasjonssystema som blir nytta i kommunen.

Revisjonen merkar seg også det at finst enkeltvise rutinar med instruksar og skjema som gjeld tilgangsstyring for nokre system. Revisjonen meiner at kommunen med fordel burde samle og gjere tilgjengeleg felles retningslinjer og rutinar for tilgangsstyring for alle kommunen sine elektroniske system slik at det blir tydeleg for dei involverte kva ansvar dei har for å sikre oppdaterte og riktige tilgangar, kven ein skal kontakte og korleis ein skal gå fram ved endring eller avslutning av brukartilgang mv.

Tysnes kommune har utnemnt eit personvernombod, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Revisjonen vil påpeike at kommunen pliktar å stille til rådighet dei ressursar som er nødvendig for at personvernombodet skal kunne utføre lovpålagde oppgåver (2. punkt i artikkel 38).

Det går vidare fram at personvernombodet opplever å i liten grad bli involvert i prosessar eller spørsmål knytt til vern av personopplysningar. Revisjonen er merksam på at noverande personvernombod har vore tilsett i kommunen i ein relativt kort perioden, og at det er sett inn fleire gode tiltak i perioden for å sikre involvering av personvernombodet. Revisjonen vil samtidig påpeike at kommunen etter personvernforordninga pliktar å sikre at personvernombodet på riktig måte og i rett tid blir involvert i alle spørsmål som gjeld vern av personopplysningar (1. punkt i artikkel 38).

Tysnes kommune har etablert personvernerklæring. Revisjonen vurderer samtidig at kommunen ikkje har sikra at denne erklæringa har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane. Datatilsynet skriv mellom anna i si rettleiing om verksemdene sine pliktar etter personvernregelverket<sup>1</sup> at verksemdene ikkje kan bruke juridisk eller teknisk sjargong når dei kommuniserer om personopplysningar, informasjonen skal vere forståeleg for målgruppa og informasjonen skal vere konkret (unngå formuleringar som «vi kan bruke personopplysningar til...»). Undersøkinga viser, etter revisjonen si vurdering, at Tysnes kommune i si fråsegn om personvern ikkje er tilstrekkeleg konkret og at det er nytta ein del omgrep og formuleringar som gjer fråsegna utfordrande å forstå for målgruppa.

Revisjonen vurderer vidare at kommunen si personvernerklæring ikkje er tilstrekkeleg lett tilgjengeleg, i samsvar med krav om dette i regelverket (artikkel 12 i personvernforordninga). Svar på spørjeundersøkinga indikerer at personvernerklæringa også er relativt ukjend for dei tilsette i kommunen; berre 12 prosent oppgjev å vere kjend med denne. Det skal ikkje vere nødvendig for brukarar å måtte leite etter informasjon om handsaming av personopplysningar, og revisjonen meiner derfor at kommunen bør plassere lenke til personvernerklæringa lett tilgjengeleg for ålmenta, til dømes på framsida for kommunen sine nettsider.

Tysnes kommune fører ikkje i tilstrekkeleg grad protokoll over behandlingsaktivitetar av personopplysningar. Undersøkinga viser at kommunen har sett i gang eit arbeid for å sikre at det framover skal førast protokoll over behandlinga av personopplysningar; det er mellom anna etablert mal for dette arbeidet og det er gjennomført workshops med nokre av leiarane i kommunen for å rette merksemd mot protokollføring. Revisjonen merkar seg likevel at kommunen på revisjonspunktet har utarbeidd få protokollar for behandling av personopplysningar og at dette heller ikkje blir gjort systematisk. Det er heller ikkje tilstrekkeleg tydeleggjort kven som skal ha dette ansvaret for dei ulik systema. Dette er ikkje i samsvar med krav om utarbeiding av behandlingsprotokollar (artikkel 30 i personvernforordninga).

Revisjonen vurderer at Tysnes kommune ikkje i tilstrekkeleg grad gjennomfører risikovurderingar av handsaming av personopplysningar, og at det heller ikkje i samband med risikovurderingar systematisk blir gjort vurderingar av personvernrisikoar (DPIA). Manglande risikovurderingar og rutinar for gjennomføring av slike gjer at kommunen ikkje har oversikt over kvar det er personvernrisikoar, og kommunen veit derfor heller ikkje kva eventuelle tryggleikstiltak som fungerer og ikkje. Kommunen manglar med dette grunnlag for å gjere eventuelle justeringar og slik kontinuerleg forbetre informasjonstryggleiken. Manglande risikovurderingar betyr vidare at kommunen heller ikkje veit kva personopplysningar dei handsamar med høg risiko, og har difor heller ikkje grunnlag for å gjennomføre vurdering av personvernkonsekvensar ved behandling av personopplysningar med høg risiko, jf. personvernforordninga artikkel 35.

---

<sup>1</sup> Datatilsynet. Virksomhetenes plikter. Informasjon og åpenhet. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/>

Tysnes kommune har ved innføring av elektronisk avviksmeldesystem sikra oversikt over avvik som blir meldt knytt til personvern. Revisjonen vurderer samtidig at kommunen ikkje i tilstrekkeleg grad har etablert retningslinjer som sikrar tilfredsstillande rutinar for kven som har hovudansvar for å melde frå til Datatilsynet dersom det blir meldt om alvorlege brot på personopplysningstryggleiken, og det går heller ikkje fram kva som er frist for å melde slike avvik vidare til tilsynsmyndigheita. Revisjonen vil understreke at personvernforordninga er tydeleg på at den behandlingsansvarlege (dvs. rådmann) utan ugrunna opphald og seinast 72 timar etter å ha fått kjennskap til brot på personopplysningstryggleiken, skal melde brotet til Datatilsynet (jf. Artikkel 33). Datatilsynet peiker i si rettleiing på at den behandlingsansvarlege ikkje treng å melde frå om brot til Datatilsynet dersom brotet truleg ikkje vil medføre risiko for fysiske personar sine rettigheter og friheiter, men peiker vidare på at dersom behandlingsansvarleg er usikker på om unntaket er oppfylt bør melde frå til Datatilsynet for sikkerheits skuld.<sup>2</sup>

Undersøkinga viser at det er meldt avvik i desember 2022 om at helsepersonell frå både legekontor, helsestasjon og psykisk helseteneste har hatt tilgang til mapper med personsensitiv informasjon utan at dei har hatt tenestleg behov for dette. Dette skuldast at det blei oppretta ei mappe innan sikker sone, men likevel på eit område der tilsette frå fleire tenester hadde tilgang. Dette syner viktigheita av å gjennomføre kontrollar og å sikre at tilsette har tilstrekkeleg kompetanse knytt til handtering av personsensitiv informasjon.

Svara i spørjeundersøkinga tyder på at ikkje alle tilsette i kommunen veit at dei skal melde avvik knytt til informasjonstryggleik når dei opplever eller observerer slike tilfelle. Ein relativt stor del av respondentane som oppgjev at dei har opplevd slike avvik svarer at dei ikkje har meldt frå om dette. Kommunen si oversikt over registrerte avvik indikerer også at det er få avvik som blir meldt. Revisjonen vil peike på at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta.

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg rutinar for å sikre at tilsette får opplæring i informasjonstryggleik. Undersøkinga viser at kommunen har etablert nokre målsettingar om at opplæring knytt til informasjonstryggleik er viktig, og det går vidare fram av handbok i informasjonssikkerhet at leiarar og superbrukarar/fagsystemansvarlege har eit ansvar for å sikre at tilsette får denne opplæringa. Det går samtidig fram at kommunen ikkje har etablert system eller rutinar som sikrar tilsette får denne opplæringa. Kommunen har heller ikkje oversikt over kva opplæring eller kurs tilsette eventuelt har fått på dette området. Revisjonen vil påpeike at dette ikkje er i samsvar med krav og anbefalingar om kommunen sitt ansvar for å sikre tilstrekkeleg informasjonstryggleikskompetanse blant dei tilsette gjennom opplæringstiltak. Dette gjer at det er høgare sannsyn for at dei tilsette ikkje har tilstrekkeleg kompetanse innan informasjonstryggleik, noko som igjen aukar risiko for brot på regelverket som gjeld for behandling av personopplysningar og for informasjonstryggleiken generelt.

Revisjonen merkar seg at kommunen kjenner til behovet for opplæring av tilsette, og at det mellom anna blir vurdert å ta i bruk e-læring for å etablere opplæringsmodular og kurs innan mellom anna informasjonstryggleik på kommunen sine intranettsider.

Basert på funna i spørjeundersøkinga, vurderer revisjonen at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Til dømes svarar om lag halvparten av alle respondentane, og om lag ein av tre respondentar med leiaransvar, at dei *ikkje* kjenner innhaldet i kommunen si handbok i informasjonssikkerhet. Svar i spørjeundersøkinga indikerer vidare at det relativt store skilnadar mellom sektorane i kommunen når det gjeld kjennskap til styrande dokument for informasjonstryggleik. Til dømes går det fram at 93 prosent av respondentane frå oppvekstsektoren oppgjev å handsame både personopplysningar og sensitive personopplysningar, men 60 prosent av respondentane frå denne sektoren kjenner ikkje til innhaldet i kommunen si handbok i informasjonstryggleik. Det er vidare 14 prosent av respondentane frå oppvekstsektoren som ikkje veit om kommunen eller eininga har tilstrekkeleg skriftlege retningslinjer for handsaming av personopplysningar og 10 prosent svarar at det «i liten grad» er tilfredsstillande retningslinjer for dette. Vidare svarar 30 prosent av respondentane som oppgjev at kommunen og/eller eininga «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer for handsaming av personopplysningar, at dei ikkje kjenner til kvar dei finn desse retningslinjene og rutinane. Revisjonen vil understreke at kommunen etter personvernforordninga er forplikta til å sette i verk eigna tiltak, både organisatoriske og tekniske, for å sikre og påvise at personopplysningar blir handsama i samsvar med krav til dette i regelverket (personvernforordninga artikkel 24). Som ein del av dette bør kommunen mellom anna sikre at kommunen sine styrande dokument for informasjonstryggleik er tilgjengeleg og kjend for dei tilsette i kommunen.

Revisjonen vurderer vidare at kommunen ikkje i tilstrekkeleg grad etterlever retningslinjer og rutinar for informasjonstryggleik. Undersøkinga indikerer at dokument med fortruleg informasjon ikkje alltid blir lagra på ein sikker

<sup>2</sup> Datatilsynet. Hvilke brudd skal meldes til Datatilsynet? Publisert 24.03.2023. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hvilke-brudd-skal-meldes-til-datatilsynet/>

måte og/eller blir oppbevart slik at uvedkomande kan få innsyn. Undersøkinga viser også at 16 prosent av respondentane ikkje følgjer ein praksis for avlogging av PC i samsvar med prinsipp om god informasjonstryggleik. Det er vidare 12 prosent av respondentane som svarer at dei har lånt ut brukarnamn og passord til andre, medan 11 prosent viser til at dei «nokre gonger» ser at dette blir gjort av andre og 3 prosent oppgjev at dei «ofte» observerer dette. Revisjonen vil i den samanheng understreke at det å dele passord med andre ikkje er i samsvar med grunnleggjande prinsipp for informasjonstryggleik, også i tilfella der det er IT-tenesta ein deler passordet med.

Revisjonen sin konklusjon og tilrådingar går fram av kapittel 6 i rapporten.

## Ordliste

**Informasjonstryggleik:** omhandlar å sikre informasjon i alle former slik at det 1) ikkje bli kjend for uvedkomande (**konfidensialitet**), 2) ikkje bli endra utilsikta eller av uvedkomande (**integritet**) og 3) er tilgjengeleg ved behov (**tilgjenge**).<sup>3</sup>

**Styringssystem for informasjonstryggleik:** Styring og kontroll på informasjonstryggleiksområdet handlar om systematiske styringsaktivitetar. Desse skal sørge for at relevante *risikoar blir vurdert*, at nødvendige og hensiktsmessige *tryggleikstiltak blir etablert*, og at det *systematisk blir kontrollert og følgt opp* at tiltaka og styringsaktivitetane faktisk fungerer som føreset.

**Behandlingsansvarleg:** Den behandlingsansvarlege er etter regelverket mellom anna ansvarleg for å behandle personopplysningar på ein lovleg, rettferdig og gjennomsiktig måte. I kommunane er det kommunedirektør/rådmann som er øvste behandlingsansvarleg for handsaming av personopplysningar i tenestene.

**Personopplysningar:** ein kvar opplysning om ein identifisert eller identifiserbar fysisk person. Ein identifiserbar fysisk person er ein person som direkte eller indirekte kan identifiserast, særleg ved hjelp av ein identifikator (t.d. eit namn, eit identifiseringsnummer, lokaliseringsopplysningar, ein nettidentifikator eller eitt eller fleire element som er spesifikke for nemnde fysiske person sin fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet).

**Sensitive personopplysningar /særlege kategoriar personopplysningar:** opplysningar om rasemessig eller etnisk opphav, politisk oppfatning, religion, filosofisk overtyding, fagforeningsmedlemskap, genetiske opplysningar, helseopplysningar, opplysningar om ein fysisk person sine seksuelle forhold, opplysningar om ein fysisk person si seksuelle orientering, straffedommar, lovbrøt, samt biometriske opplysningar med det formål å eintydig identifisere ein fysisk person.

**Fortruleg informasjon:** Fortruleg informasjon er informasjon som anten gjennom lov eller instruks er unnateke offentlegheit, eller som på anna grunnlag er å vurdere som konfidensiell.

**IKT-tryggleik/datatryggleik:** Metodar, tenester og verktøy som sikrar at digital informasjon og digitale system ikkje blir utilgjengeleg, går tapt, blir lest eller endra. Datatryggleik omhandlar både sikring mot hendingar som skuldast vondsinna handlingar, og sikring mot hendingar som skuldast system- og brukarfeil.<sup>4</sup>

<sup>3</sup> Digitaliseringsdirektoratet (Digdir): Informasjonssikkerhet – en forutsetning for å nå virksomhetens mål:

<https://www.digdir.no/informasjonsikkerhet/informasjonsikkerhet-en-forutsetning-na-virksomhetens-mal/1123>

<sup>4</sup> Det store norske leksikon: Datasikkerhet: <https://snl.no/datasikkerhet>

# Innhald

1	Innleiing	8
2	Organisering av arbeidet med informasjonstryggleik	10
3	Styringssystem for informasjonstryggleik	11
4	Etterleving av krav i personvernlovgevinga	20
5	Kompetanse blant tilsette	29
6	Konklusjon og tilrådingar	40
	Vedlegg 1 : Høyringsuttale	44
	Vedlegg 2 : Utvida høyringsuttale	45
	Vedlegg 3 : Kommentar til utvida høyringsuttale	55
	Vedlegg 4 : Revisjonskriterier	58
	Vedlegg 5 : Sentrale dokument og litteratur	62

# Detaljert innhald

1	Innleiing	8
1.1	Bakgrunn	8
1.2	Føremål og problemstillingar	8
1.3	Avgrensing	8
1.4	Metode	8
1.4.1	Dokumentanalyse	8
1.4.2	Intervju	8
1.4.3	Spørjeundersøking	9
1.4.4	Verifiseringsprosessar	9
1.5	Revisjonskriterier	9
2	Organisering av arbeidet med informasjonstryggleik	10
2.1	Organisering	10
3	Styringssystem for informasjonstryggleik	11
3.1	Problemstilling	11
3.2	Revisjonskriterier	11
3.3	Styrande dokument for informasjonstryggleik	12
3.3.1	Datagrunnlag	12
3.3.2	Vurdering	13
3.4	Rutinar og ansvarsforhold	14
3.4.1	Datagrunnlag	14
3.4.2	Vurdering	17
3.5	System for og gjennomføring av kontroll og etterprøving av informasjonstryggleik	17
3.5.1	Datagrunnlag	17
3.5.2	Vurdering	19
4	Etterleving av krav i personvernlovgjevinga	20
4.1	Problemstilling	20
4.2	Revisjonskriterier	20
4.3	Personvernombod og personvernerklæring	21
4.3.1	Datagrunnlag	21
4.3.2	Vurdering	23
4.4	Protokoll over behandlingsaktivitetar	23
4.4.1	Datagrunnlag	23
4.4.2	Vurdering	24
4.5	Risiko- og konsekvensvurderingar av behandling av personopplysningar	24
4.5.1	Datagrunnlag	24
4.5.2	Vurdering	25
4.6	Oversikt over avvik knytt til personvern	26
4.6.1	Datagrunnlag	26
4.6.2	Vurdering	28
5	Kompetanse blant tilsette	29
5.1	Problemstilling	29



5.2	Revisjonskriterier	29
5.3	Rutinar for opplæring i informasjonstryggleik	29
5.3.1	Datagrunnlag	29
5.3.2	Vurdering	30
5.4	Kjennskap til og etterleving av retningslinjer og rutinar for informasjonstryggleik	31
5.4.1	Datagrunnlag	31
5.4.2	Vurdering	39
6	Konklusjon og tilrådingar	40
	Vedlegg 1 : Høyringsuttale	44
	Vedlegg 2 : Utvida høyringsuttale	45
	Vedlegg 3 : Kommentar til utvida høyringsuttale	55
	Vedlegg 4 : Revisjonskriterier	58
	Vedlegg 5 : Sentrale dokument og litteratur	62

## Figurar

Figur 1:	Administrativ organisering av Tysnes kommune	10
Figur 2:	Kjennskap til ansvar og oppgåver knytt til informasjonstryggleik i eiga rolle	16
Figur 3:	Kjennskap til kommunen sitt personvernombod	22
Figur 4:	Informasjonstryggleiksavvik meldt mellom juni 2022 og august 2023 (Kjelde: Tysnes kommune)	26
Figur 5:	Melding om opplevde informasjonstryggleiksavvik	28
Figur 6:	Del respondentar som handsamar personopplysningar og sensitive personopplysningar gjennom sitt arbeid	31
Figur 7:	Har kommunen og/eller eininga tilfredsstillande skriftlege retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og anna fortruleg informasjon?	32
Figur 8:	Tilfredsstillande retningslinjer for handsaming av personopplysningar delt på sektorane i kommunen	32
Figur 9:	Kjennskap til innhald i styrande dokument om informasjonstryggleik og personvern	33
Figur 10:	Kjennskap til handbok i informasjonssikkerhet delt på sektortilhøyrslø	33
Figur 11:	Informasjon frå leiar om retningslinjer, tryggleiksorganisering og informasjonstryggleiks rutinar	34
Figur 12:	Nødvendig autorisering og kompetanse for å ivareta informasjonstryggleik	34
Figur 13:	Tilstreккеleg opplæring	35
Figur 14:	Svar på tilstrekkeleg opplæring fordelt på sektorar i kommunen	35
Figur 15:	Informasjon om ulike informasjonstryggleikstiltak	36
Figur 16:	Oppbevaring av dokument med fortruleg informasjon	37
Figur 17:	Observasjon av informasjonstryggleiksbrot	37
Figur 18:	Kor ofte har du observert at brukarnamn og passord blir gitt til andre, som t.d. IT-leiar? (N=158)	38
Figur 19:	Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du nyttar? (N=163)	38
Figur 20:	Fokus på informasjonstryggleik i Tysnes kommune	39

## Tabellar

Tabell 1:	Oversikt over svar per sektor i Tysnes kommune	9
Tabell 2:	Strategiar for innsatsområdet personvern og informasjonssikring (Kjelde: Tysnes kommune)	12
Tabell 3:	Rolle- og ansvarsdeling knytt til informasjonstryggleik i Tysnes kommune	14

# 1 Innleiing

## 1.1 Bakgrunn

Deloitte har gjennomført ein forvaltningsrevisjon av informasjonstryggleik og personvern i Tysnes kommune. Prosjektet blei bestilt av kontrollutvalet i Tysnes kommune i sak 22/22 den 24. november 2022.

## 1.2 Føremål og problemstillingar

Formålet med prosjektet har vore å undersøkje om kommunen har tilfredsstillande system og rutinar for informasjonstryggleik og om etablerte standardar og gjeldande lovar og reglar blir etterlevd innan dette området. Vidare har det vore eit føremål å undersøke i kva grad Tysnes kommune etterlever sentrale krav i personvernlovgevinga.

**Med bakgrunn i formålet er det utarbeidd følgjande problemstillingar som har blitt undersøkt:**

1. I kva grad har Tysnes kommune etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner?
  - a) Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
  - b) Er det etablert klare rutinar og ansvarsforhold knytt til informasjonstryggleik?
  - c) Har kommunen system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?
2. I kva grad etterlever Tysnes kommune sentrale krav i personvernlovgevinga?
  - a) Har kommunen utnemnt eit personvernombod og etablert personvernerklæring i samsvar med krav om dette i regelverket?
  - b) Fører kommunen protokoll over behandlingsaktivitetar av personopplysningar?
  - c) I kva grad blir det gjort risiko- og konsekvensvurderingar av behandling av personopplysningar der det er krav om dette?
  - d) I kva grad har kommunen oversikt over avvik knytt til personvern, og i kva grad blir slike avvik meldt til Datatilsynet?
3. I kva grad har dei tilsette i kommunen tilstrekkeleg kompetanse om informasjonstryggleik?
  - a) Er det etablert rutinar for å gje tilsette i kommunen opplæring i informasjonstryggleik?
  - b) I kva grad har dei tilsette i kommunen kjennskap til ev. retningslinjer og rutinar for informasjonstryggleik, og i kva grad blir desse etterlevd?

## 1.3 Avgrensing

Undersøkinga har primært fokusert på krav stilt til handsaming og sikring av personopplysningar. Personopplysningslova og -forordninga (GDPR) stiller strenge krav til handsaming og sikring av slike opplysningar, og ein lekkasje av denne typen informasjon kan få store konsekvensar, både for kommunen og personane som blir råka. Revisjonen har ikkje gjennomført undersøkingar, testingar eller analysar av teknisk konfigurasjon, tryggingstiltak eller operative driftsrutinar.

## 1.4 Metode

Oppdraget er utført i samsvar med gjeldande standard for forvaltningsrevisjon (RSK 001) og kvalitetssikra i samsvar med krava til kvalitetssikring i Deloitte Policy Manual (DPM).

Oppdraget er gjennomført i tidsrommet januar 2023 til september 2023.

### 1.4.1 Dokumentanalyse

Rettsreglar har blitt gjennomgått og nytta som revisjonskriterium. Vidare har informasjon om Tysnes kommune og dokumentasjon på etterleving av interne rutinar, regelverk m.m. blitt samla inn og analysert. Innsamla dokumentasjon har blitt vurdert opp mot revisjonskriteria.

### 1.4.2 Intervju

For å få supplerande informasjon til skriftlege kjelder har Deloitte intervju utvalde personar frå Tysnes kommune som er involvert i eller har ansvar for informasjonstryggleik og personvern. Dette inkluderer rådmann, personvernombod, IT-leiar og sektorleiar for helse og omsorg. Vi har intervju totalt fire personar.

### 1.4.3 Spørjeundersøking

For å få informasjon om i kva grad tilsette i Tysnes kommune har kjennskap til og etterlever etablerte retningslinjer og rutinar knytt til informasjonstryggleik, har revisjonen utarbeidd ei spørjeundersøking. Revisjonen har sendt ut ei digital spørjeundersøking til alle tilsette og leiarar i kommunen, totalt 347 mottakarar. Etter fleire utsettingar av frist og 14 påminningar per e-post til dei tilsette som ikkje hadde svara, fullførte 163 personar undersøkinga, noko som utgjer ein svarprosent på 47 prosent. Fordelinga per tenesteområde av dei som har svart på undersøkinga går fram av tabell 1.

Tabell 1: Oversikt over svar per sektor i Tysnes kommune

Sektor	Tal Inviterte tilsette	Tal respondentar	Svarprosent av total
Stabs- og fellestenester (t.d. økonomi, personal, rådmannen)	33	19 (57 %)	12 %
Oppvekst (t.d. skule, barnehage, barn og familie)	120	84 (70 %)	52 %
Helse og omsorg (t.d. pleie og omsorg, helsetenester, legevakt, NAV)	177	43 (24 %)	26 %
Teknisk (t.d. drift og vedlikehald, reinhald, brann og redning)	18	17 (94 %)	10 %
<b>TOTAL</b>	<b>347</b>	<b>163</b>	<b>47 %</b>

### 1.4.4 Verifiseringsprosessar

Oppsummering av intervju er sendt til dei som er intervjuar for verifisering og det er informasjon frå dei verifiserte intervjureferata som er nytta i rapporten.

Datadelen av rapporten er sendt til rådmannen for verifisering, og innspel og kommentarar frå verifiseringa blei innarbeidd i rapporten. Høyringsutkast av rapporten blei sendt til rådmannen for uttale. Revisjonen mottok først ein høyringsuttale 27.09.2023 som blei lagt ved rapporten (vedlegg 1). I framlegging av rapport for kontrollutvalet ga rådmann uttrykk for at han hadde fleire innvendingar til rapporten som ikkje kom fram i verifiseringssvaret eller i høyringssvaret til rapporten. Kontrollutvalet vedtok difor i sak 15/23 den 5. oktober 2023 at rådmann fekk ny svarfrist for å kome med utvida uttale til rapporten innan 01.12.2023 der dei nye innvendingane kunne bli tydeleggjort. Utvida høyringsuttale datert 21.12.2023 ligg som vedlegg 2 til rapporten. Revisjonen har lagt inn nokre kommentarar til den utvida høyringsuttalen i vedlegg 3 til rapporten.

## 1.5 Revisjonskriterier

Revisjonskriteria er dei krav og forventningar som forvaltningsrevisjonsobjektet skal bli vurdert opp mot. Kriteria er utleia frå autoritative kjelder i samsvar med krava i gjeldande standard for forvaltningsrevisjon. I dette prosjektet er revisjonskriteria i hovudsak henta frå lov om behandling av personopplysningar, eForvaltningsforskrifta og rettleiingsmateriell frå Digitaliseringsdirektoratet og Datatilsynet. Kriteria er summert opp innleiingsvis under kvart tema, og presentert utfyllande i vedlegg 3 vedlegg til rapporten.

## 2 Organisering av arbeidet med informasjonstryggleik

### 2.1 Organisering

Tysnes kommune er, som framstilt i figur 1 under, delt inn i fire ulike einingar: stabs- og fellestenester, oppvekst, helse og omsorg og teknisk. Det er kommunalsjefar for dei tre sistnemnde områda, og desse er mellom anna tillagt ansvar og oppgåver når det gjeld opplæring og personvern innan sine sektorar.

Figur 1: Administrativ organisering av Tysnes kommune



Kommunen opplyser at IT-leiar, personvernombod og kvalitetsrådgjevar ligg til eininga for stabs- og fellestenester. Kvalitetsrådgjevar har oppgåver knytt til kommunen sitt kvalitetssystem Compilo og har mellom anna ansvar for å gje tilsette innføring og opplæring i kvalitetssystemet.

Kommunen peiker på at strategisk leiargruppe har møte kvar 14. dag. Rådmannen og kommunalsjefane er saman med økonomisjef faste deltakarar i strategisk leiing, og ved behov blir IT-leiar og personvernombodet i kommunen kalla inn til møte i strategisk leiargruppe.

## 3 Styringssystem for informasjonstryggleik

### 3.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

*I kva grad har Tysnes kommune etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner?*

Under dette:

- Er styrande dokument for informasjonstryggleik i samsvar med krav i regelverket?
- Er det etablert klare rutinar og ansvarsforhold knytt til informasjonstryggleik?
- Har kommunen system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?

### 3.2 Revisjonskriterier

Krav til kommunen når det gjeld styringssystem for informasjonstryggleik blir utleia frå kommunelova, personopplysningslova, personvernforordninga og eForvaltningsforskrifta.

Kommunen skal:

- iverksette egna tekniske og organisatoriske tiltak for å sikre at behandling av personopplysningar skjer i samsvar med personvernforordninga. Nemnde tiltak skal gjennomgåast på nytt og skal oppdaterast ved behov (personvernforordninga artikkel 24 og 28).
- ha skildra mål og strategi for informasjonstryggleik i verksemda (tryggleiksmål og tryggleikstrategi) som skal danne grunnlaget for kommunen sin internkontroll (styring og kontroll) på informasjonstryggleiksområdet. Tryggleiksstrategien og internkontrollen skal inkludere relevante krav som er fastsett i anna lov, forskrift eller instruks (eForvaltningsforskrifta § 15)
- ha eit internkontrollsystem basert på anerkjende standardar for styringssystem for informasjonstryggleik (eForvaltningsforskrifta § 15).
- ha systematisk internkontroll tilpassa verksemda si størrelse, eigenart, aktivitetar og risikoforhold for å sikre at lover og forskrifter følges (kommunelova § 25-1).
- kontrollere at rutinar for handtering av personopplysningar blir brukt og fungerer etter føremålet. Kommunen må jamleg teste, vurdere og evaluere kor effektive tryggleikstiltaka er. Ein tryggleiksrevisjon skal omfatte vurdering av organisering, tryggleikstiltak, og bruk av tryggleikspartar og databehandlarar. Resultatet frå tryggleiksrevisjon skal dokumenterast og vere ein del av leiinga sin gjennomgang (Datatilsynet<sup>5</sup>).

Jamfør punkt tre over, er Digitaliseringsdirektoratet (Digdir) peika ut som ansvarleg for å gi tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast av offentlege verksemder. Digdir tilrår mellom anna at:

- Kommunen delegerer og følger opp arbeidet med informasjonstryggleik på ein føremålstenleg måte. Det må kommuniserast tydeleg, og tilstrekkeleg ofte, kvifor det er viktig med styring av informasjonstryggleik. Kva leiarar som gjer kva er avhengig av verksemda sin storleik, organisering, eigenart og delegeringspraksis.
- Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette.<sup>6</sup>

<sup>5</sup> Datatilsynet. Virksomhetenes plikter/informasjonsikkerhet og internkontroll/Etablere internkontroll/sikkerhetsrevisjon og egenkontroll. Sist endret: 23.06.2018. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonsikkerhet-internkontroll/etablere-internkontroll/>

<sup>6</sup> Digitaliseringsdirektoratet. Informasjonsikkerhet. Internkontroll i praksis. Etableringsaktiviteter. Utforme føringer. <https://www.digdir.no/informasjonsikkerhet/utforme-foringer/3159>

- Verksemdar gjennomfører systematiske aktivitetar som inngår i leiinga si styring og oppfølging. Digdir peiker på at aktivitetane involverer både øvste leiar og leiarar på andre nivå i organisasjonen. Følgande styringsaktivitetar blir nærare omtalt i rettleiingsmateriell frå Digdir:
  - leiinga sin gjennomgang,
  - delegering og oppfølging gjennom styringslinja,
  - sikre finansielle rammer,
  - kommunisere viktighet,
  - løfte og handtere problemstillingar gjennom styringslinja og
  - beredskap og krisehandtering,<sup>7</sup>
- Kommunen etablerer føringar for verksemda innan informasjonstryggleiksområdet og at føringane blir dokumentert på ein føremålstenleg måte slik at dei:
  - fungerer som oppslagsverk, der tilsette kan sette seg inn i føringar
  - fungerer som samfunnsdokumentasjon (arkivplikt)
  - ved behov kan gi eksterne interessantar informasjon om korleis ting fungerer i kommunen

Sjå vedlegg 4 for utfyllande revisjonskriterium.

### 3.3 Styrande dokument for informasjonstryggleik

#### 3.3.1 Datagrunnlag

Kommunen opplyser at handbok i informasjonssikkerhet og IKT-strategi 2022-2025 samla er kommunen sine styrande dokument for arbeidet med informasjonstryggleik.

Tysnes kommune har relativt nyleg etablert *handbok i informasjonssikkerhet*<sup>8</sup> som overordna styrande dokument for kommunen sitt arbeid med informasjonstryggleik. Rådmannen viser i intervju til at handbok i informasjonstryggleik blei utarbeidd i 2022. Han peiker på at kommunen tidlegare har hatt nokre rutinar om informasjonstryggleik og personvern, men at desse rutinane ikkje har vore samla i eit dokument.

Handboka ligg tilgjengeleg for alle tilsette på kommunen sine intranettsider. Handboka skildrar mellom anna mål for informasjonstryggleik i kommunen (under punktet «kvifor treng me denne handboka») og det er også sett opp ni punkt om tryggleiksstrategi for kommunen, til dømes at «arbeidet med informasjonstryggleik skal forankrast i øvste leiing og inngå i ansvarsområdet til einingsleiarane i kommunen». Det er vidare eit eige kapittel om internkontroll i handboka, der tema er handsaming av avvik, loggføring av aktivitet i fagsystem som handsamar personinformasjon, innsynskrav, den årlege gjennomgangen av informasjonstryggleik for leiinga, krav ved overvaking gjennom lydopptak og kamera, ID-kort og avhending av datautstyr. Nokre av punkta i interkontrollkapittelet er svært kortfatta og framstår som sjekkpunkt, som til dømes «avhending av datautstyr» og «ID-kort» som skildrar kortfatta at utrangert datautstyr skal leverast til IT og at tapt ID-kort må slettast, medan andre punkt som til dømes leiinga sin årlege gjennomgang, er meir utdjupa.

Det er vidare til dømes skildra i handboka at det skal gjennomførast tryggleiksrevisjonar og at resultat frå desse årleg skal gjennomgåast i strategisk leiing, men det går ikkje fram anna informasjon om kva slike revisjonar omfattar, når det skal gjennomførast eller kven som har ansvar for dette..

Kommunen har også nyleg etablert ein *IKT-strategi for 2022-2025*, og det går fram av strategien at kommunen har valt å prioritere fire innsatsområde i planperioden, der personvern og informasjonssikring inngår som eit av dei fire områda. Det blir vidare peikt på at det er definerte strategiar innanfor kvar av dei fire innsatsområda som skal leggest til grunn for det vidare IKT-arbeidet, og at kommunen ved oppfølging av IKT-strategien skal utarbeida handlingsplanar med tiltak knytt til dei enkelte strategiane. I tabellen under er strategiane for innsatsområdet personvern og informasjonssikring presentert.

Tabell 2: Strategiar for innsatsområdet personvern og informasjonssikring (Kjelde: Tysnes kommune)

Strategi	Skildring
<b>Ivareta informasjonstryggleik og personvern frå start til slutt</b>	Vurdere informasjonstryggleik og personvern frå start til slutt i kommunen sine digitale løysingar for å sikre tillit frå verksemdar og innbyggjarar. Informasjonstryggleik må følgje informasjonen frå den oppstår til den blir sletta.

<sup>7</sup> Digitaliseringsdirektoratet: <https://www.digdir.no/informasjonssikkerhet/ledelsens-styring-og-oppfolging/3044>.

<sup>8</sup> Tysnes kommune. *Handbok i informasjonssikkerhet for Tysnes kommune*. 2022.

<b>Leggja til rette for å gje innbyggaren innsyn og kontroll over egne data</b>	Kommunen skal leggja til rette for å gje innbyggjarane lovbestemt innsyn i alle typar data som er registrert om dei. Innsyn vil kunna medføra rettingar som igjen gjev ei betring av datakvaliteten i kommunen.
<b>Understøtta sikre tenester for elektronisk kommunikasjon med innbyggjarane</b>	Sikre at relevant informasjon for innbyggjarar og næringsliv er lett tilgjengeleg og vidare at informasjonen er påliteleg, trygt lagra og at sensitiv informasjon ikkje kjem på avveg. For å vareta personvernet skal alle lovkrav knytt til informasjonssikring i offentleg sektor vera oppfylt. Bruk av autentiseringsløysingar som ID-porten skal samtidig gje innbyggjarane den nødvendige grad av tryggleik og også bidra til effektivisering.
<b>Syta for rett sikkerheitsnivå og oppdaterte sikkerheitsrutinar</b>	For å oppnå så god kombinasjon av brukarvenlegheit og tryggleik som mogleg, er det viktig å definere rett nivå av tryggleik på data som ligg i dei ulike fagsystema. Behandlingsansvarlige (systemeigarar) har som ansvar å kjenna lovkrava og gje nødvendig informasjon til IT-avdelinga slik at aktuelle tryggleikstiltak blir gjort i infrastrukturen og drifta til kommunen. Kommunen må til ei kvar tid ha gode nok tryggleiksrutinar og bruke sikringsløysingar som sikrar for at informasjonen berre når autoriserte personar.
<b>Gjennomføra organisatoriske tiltak for å vareta personvern og informasjonssikkerhet</b>	Ved innkjøp av nye system skal det stillast krav til leverandøren om innebygd personvern. Gjennomføre risikovurdering for å avdekka eventuelle tryggleiksmessige utfordringar ved innføring av nye tenester eller endring av eksisterande. Det skal etablerast fungerande internkontroll som skal sikre at kommunen handsamar personopplysningar i tråd med lova.
<b>Bevisstgjera og gje opplæring</b>	Kommunen skal sikre at dei tilsette har lett tilgang til retningslinjer, prosedyrar, rutinar og kurs. Å bygga og halda oppe ein tryggleikskultur er ein kontinuerleg prosess.
<b>Sikra moderne og effektive løysingar for å vareta informasjonstryggleik</b>	Kommunen må tilpassa seg kontinuerleg teknologisk utvikling ved å implementera moderne og effektive løysingar som kan handtere kommande tryggleiksutfordringar.

Kommunen har per august 2023 ikkje utarbeidd handlingsplanar med tiltak når det gjeld strategiane for innsatsområdet personvern og informasjonssikring.

Det blir i intervju vist til at informasjonstryggleik og personvern blir tatt opp som tema i møta i strategisk leiing, utvida leiarteam og einingsleiarmøte, men at det ikkje er etablert praksis for å ha dette oppe som fast tema i desse leiarmøta. Det blir elles vist til at det er etablert egne system og rutinar for å sikre medvit om og arbeid med informasjonstryggleik og personvern ute i einingane. Det blir mellom anna vist til at det i institusjonstenestene (under helse- og omsorgseininga) blir gjennomført internkontrollmøte annakvar veke og kvalitetsmøte kvar veke der informasjonstryggleik og personvern er tema, og at det ligg inne i årshjulet til *open omsorg* at informasjonstryggleik jamleg skal vere tema i personalmøte.

Det blir i intervju påpeikt at kommunen på revisjonstidspunktet har manglande styring på området informasjonstryggleik og personvern. Rådmannen understrekar også i intervju at det er viktig å vere open på at Tysnes kommune har ein veg å gå når det gjeld arbeid med informasjonstryggleik og personvern. Han peiker samtidig på at dette er viktige fokusområde i kommunen våren 2023, og at målet er å sikre etterleving av rutinar og retningslinjer og samstundes sikre at informasjonstryggleik og personvern er ein integrert del av måten dei tilsette tenkjer kvalitet på. Rådmannen viser til at kommunen på revisjonstidspunktet er i prosess med å formidle innhaldet i handboka ut i verksemda (meir om kjennskap til rutinar og retningslinjer blant tilsette i kapittel 5).

### 3.3.2 Vurdering

Revisjonen vurderer at Tysnes kommune sine styrande dokument på revisjonstidspunktet langt på veg var i samsvar med krav i regelverket. Kommunen har gjennom handbok for informasjonssikkerhet og IKT-strategi 2022-2025 etablert mål og strategi for arbeidet med informasjonstryggleik i kommunen og styrande dokument er vidare tilgjengeleg for dei tilsette i organisasjonen via intranett og kvalitetssystemet (Compilo). Dette er i samsvar med krav på området (jf. eForvaltningsforskrifta § 15). Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette. Revisjonen vil på peike at Tysnes kommune, i samsvar med denne tilrådinga, bør synleggjere kva krav og /eller anerkjende standardar dei baserer sine styrande dokument på.

Digitaliseringsdirektoratet tilrår at verksemder utformar føringar for arbeidet med informasjonstryggleik, og at struktur og innhald i styringsaktivitetane blir dokumentert på ein føremålstenleg måte slik at det er tydeleg kven som skal gjere kva, og korleis det skal gjerast (slik at dokumenteringa t.d. kan nyttast som oppslagsverk for tilsette). Revisjonen vurderer at Tysnes kommune sine styrande dokument i større grad bør tydeleggjere struktur og innhald i alle styringsaktivitetar, til dømes når det gjeld gjennomføring av tryggleiksrevisjonar. Undersøkinga viser at styrande dokument ikkje gir informasjon om kva tryggleiksrevisjonar omfattar, når det skal gjennomførast eller kven som har ansvar for dette.

Revisjonen er merksam på at kommunen sine styringsdokument relativt nyleg er etablert, og at arbeidet med å implementere rutinar og system i samsvar med dette framleis var pågåande på revisjonstidspunktet.

### 3.4 Rutinar og ansvarsforhold

#### 3.4.1 Datagrunnlag

##### Ansvar og rollar knytt til informasjonstryggleik

I kommunen si *handbok for informasjonssikkerhet* går det fram at rolle- og ansvarsdelinga for informasjonstryggleiksområdet i kommunen er som vist i tabellen under. Rådmannen har det øvste ansvaret for behandling av personopplysningar i kommunen, medan dei daglege oppgåvene for å sikre behandlaransvaret er delegert til einingsleiarane i kommunen.

Tabell 3: Rolle- og ansvarsdeling knytt til informasjonstryggleik i Tysnes kommune

Rolle	Skildring	Ansvar
<b>Rådmann</b>	Rådmannen har hovudansvaret for behandling av personopplysningar i Tysnes kommune	
<b>Einingsleiarar</b>	Ansvar for den daglege behandlinga av personopplysningar Einingsleiarar er også <b>systemeigar</b> , og med dette eigar av fagsystema/IT-systema som naturleg høyrer inn under området einingsleiar er ansvarleg for.	<ul style="list-style-type: none"> <li>Einingsleiar er systemeigar, og er eigar av fagsystema/IT-systema som naturleg høyrer inn under området einingsleiar er ansvarleg for.</li> <li>ansvarleg for å behandla personopplysningar på ein lovleg, rettferdig og gjennomsiiktig måte, ha eit behandlingsgrunnlag, behandla personopplysningane på ein sikker måte og sikra at dei registrerte får utøvd rettane sine.</li> <li>syta for å etablere alle nødvendige organisatoriske og tekniske tiltak for å sikra at regelverket til kvar tid blir etterlevd. Einingsleiar må kunna visa at han opptre i samsvar med reglane.</li> <li>Som systemeigar er einingsleiar Systemeigar er ansvarleg for å vareta informasjonssikkerhet i fagsystema/IT-systema, samt å sikre at informasjonen blir ivareteken på ein sikker måte når systemet ikkje lenger skal brukast.</li> </ul>
<b>Personvernombod</b>	Personvernombod kontrollerer etterleving av forordninga og skal kunna gje råd i personvernkonsekvens-utgreiingar og kontrollere gjennomføringa.	<ul style="list-style-type: none"> <li>Personvernombod skal hjelpe tilsette, registrerte og leiinga i spørsmål om personvern og informasjonssikkerhet.</li> <li>Personvernombod har teieplikt, skal ikkje få instruksjonar i samband med utføring av oppgåvene som personvernombod, og rapporterer til rådmannen.</li> </ul>
<b>IT-leiar</b>	IT-leiar er ansvarleg for at informasjonstryggleiken blir varetatt i infrastruktur, maskinvare og tryggleikssystem.	<ul style="list-style-type: none"> <li>IT-leiar varetar sentral beredskapsplan for å handtera driftsavbrot som blir vurdert å vera av eit slikt omfang at dei skaper vesentlege forstyrringar for større delar av kommuneverksemda, og/eller som kan gi følgjeskadar for tredjepart.</li> <li>IT-leiar er ansvarleg for at fagsystema/IT-systema er tilgjengeleg for tilsette.</li> <li>Hjelper til med teknisk kompetanse i dialog med superbrukar/fagsystemansvarleg.</li> </ul>



<b>Leiarar</b>	Den enkelte leiar har det daglege ansvaret for den praktiske oppfølginga av tryggleiksarbeidet i eiga verksemd. Leiar er også ansvarleg for å initiera og hjelpa til i risikovurderingar.	<ul style="list-style-type: none"> <li>• Ansvarleg for å melda frå til personal, IT og superbrukar for aktuelle fagsystem når tilsette sluttar, samt for innsamling av nøklar og ID-kort i desse tilfella.</li> <li>• Leggje til rette for at tilsette lagrar og behandlar opplysningar på rett stad i fagsystema, på heime- eller fellesområdet eller i Teams for kommunen.</li> <li>• Ansvar for at formålet med behandling av data skal registrerast i samsvar med GDPR reglane. Det skal utarbeidast ROS analysar ved nye system eller større endringar i eit fagsystem.</li> <li>• Ansvarleg for at tilsette har underteikna tilsetjingskontrakt og erklæring om teieplikt før dei får tilgang til IT- og fagsystema.</li> <li>• Ansvar knytt til å sikre riktig og nødvendige tilgangar for tilsette i si verksemd, samt at slike tilgangar blir avslutta når tilsette sluttar jf. rutinar om avslutning av arbeidsforhold vedteke av kommunestyret.</li> </ul>
<b>Superbrukar/fagsystemansvarleg</b>	Superbruker/fagsystemansvarleg er utpeikt av einingsleiar.	<ul style="list-style-type: none"> <li>• Hovudansvar for å gi opplæring til tilsette om forsvarleg forvaltning av informasjonen i fagsystema/IT-systema.</li> <li>• Ansvar å utarbeida risikoaanalyse.</li> </ul>
<b>Tilsette</b>	Alle tilsette skal overhalde informasjonstryggleiks-reglementet, og vere med på å verne informasjon i fagsystem, elektroniske einingar og infrastruktur.	<ul style="list-style-type: none"> <li>• Alle tilsette skal ha kjennskap til korleis avvik skal registrerast i avvikssystemet til kommunen (Compilo).</li> <li>• Den enkelte tilsette har ansvar for at det vert rydda opp i it-utstyr, mapper, filer, e-post-system o.s.v. før vedkomande sluttar.</li> <li>• Tilsette skal følgja kommunen sine retningslinjer om bruk av program, utstyr og tenester knytt til utstyret. Tilsette skal rapportera forhold som kan ha noko å seia for tryggleiken i IT-utstyret til IT avdeling så raskt som mogleg.</li> </ul>

I tillegg til det som går fram av oversikta over er det etablert jamlege møte mellom rådmann, IT-leiar og personvernombod. Føremålet med møtet er å sikre tilstrekkeleg merksemd på arbeid med informasjonstryggleik og personvern i kommunen. Det er fast agenda på desse møta, og ein går mellom anna gjennom meldte avvik og status for rutine- og systemarbeid innan personvern.

Det går vidare fram i intervju at det er IKT-rettleiarar ved dei enkelte skulane i Tysnes kommune, og at desse mellom anna skal konsulterast før innføring a av nye system i undervisningssamanheng. Denne rolla er ikkje skildra i verken handboka eller IKT-strategien som er utarbeidd av kommunen.

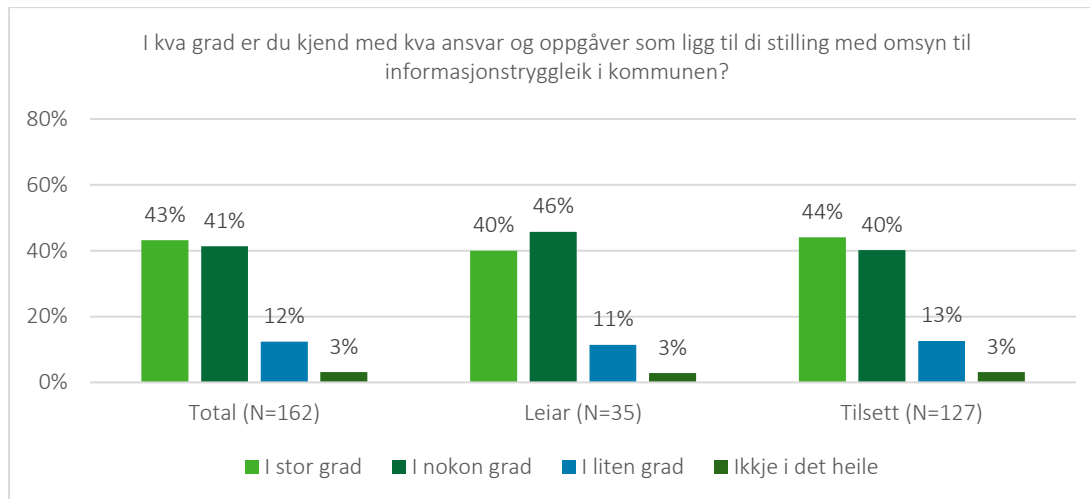
I intervju er det fleire som peiker på at sjølv om rollar og ansvar knytt til informasjonstryggleik er skildra i handboka, så har kommunen framleis ein veg å gå på dette området. Mellom anna blir det vist til at rollar og ansvar er tydeleg fordelt i toppleiargruppa, men at det står att ein del når det gjeld å tydeleggjere kva ein som tilsett eller leiar på ulike nivå er pålagt å gjere seg kjend med knytt til informasjonstryggleik.

Det blir vist til at kommunen gjer vurderingar om internkontrollsystem innan personvern og informasjonstryggleik er tilstrekkeleg. Til dømes blir det vist til at kommunen har registrert at andre kommunar har meir omfattande rolleskildringar på dette området, og at kommunen med bakgrunn i dette vil vurdere om rolleskildringane skal reviderast. Kommunen opplyser at det i revisjonsperioden er gjort enkelte presiseringar i handboka når det gjeld rollar og ansvar, mellom anna er det lagt inn tilvisingar til oppgåveskildringar i handboka (t.d. tilgang og brukarkontroll) under skildring av leiaransvar.

Rådmannen peiker på at det generelt er Rådmannen sitt ansvar å sikre at kommunen har system som sikrar at krav i lov og forskrift blir etterlevd på informasjonstryggleiksområdet. Han viser til at det er hans ansvar å utpeike personvernombod og å sikre at rollane knytt til internkontroll blir etterlevd. Han har vidare ansvar for all internkontroll, også når det gjeld informasjonstryggleik og personvern i kommunen, og han påpeiker at informasjonstryggleik og personvern er den tredje bjelken i god internkontroll saman med HMS og tenestekvalitet. Han viser samtidig til at det er ei utfordring å oppretthalde merksemda på informasjonstryggleik og personvern i kommunen.

Dei tilsette som deltok i spørjeundersøkinga fekk spørsmål om i kva grad dei er kjende med kva ansvar og oppgåver som ligg til deira stilling med omsyn til informasjonstryggleik i kommunen. Som framstilt i figuren under svarar total 3 prosent av både leiarar og tilsette utan leiaransvar at dei «ikkje i det heile» er kjend med dette, medan høvesvis 11 prosent av leiarar og 13 prosent av tilsette utan leiaransvar svarer «i liten grad» på dette spørsmålet. 46 prosent av leiarane og 40 prosent av tilsette utan leiaransvar viser til at dei «i nokon grad» har kjennskap til kva ansvar og oppgåver som ligg til deira stilling.

Figur 2: Kjennskap til ansvar og oppgåver knytt til informasjonstryggleik i eiga rolle



Respondentane blei vidare spurt om dei kjenner til kven i kommunen dei skal kontakte dersom dei har spørsmål knytt til informasjonstryggleik og/eller handsaming av personopplysningar. Totalt er det 59 prosent av respondentane som svarar «ja» på dette spørsmålet, medan 41 prosent svarar «nei». Det er langt fleire respondentar frå stabs- og fellestjenester som svarar «ja» på dette spørsmålet (95 prosent) samanlikna med respondentar frå dei andre sektorane. Innan oppvekst og teknisk svarar over halvparten av respondentane (om lag 52 prosent) at dei ikkje kjenner til kven i kommunen dei skal kontakte dersom dei har slike spørsmål.

### Rutinar knytt til informasjonstryggleik

Tysnes kommune har utover handbok i informasjonssikkerhet, ikkje etablert overordna skildringar av korleis, når og på kva måte oppgåver innan informasjonstryggleik skal gjennomførast. Det går til dømes fram av handboka at leiar har ansvar for at føremålet med handsaming av data skal registrerast i samsvar med GDPR reglane og at det skal gjennomførast ROS-analysar ved nye system eller større endringar i eit fagsystem, men det er ikkje etablert felles rutinar eller skildringar av korleis eller kor ofte dette skal gjennomførast. Det går vidare til dømes fram av handboka at det skal gjennomførast årleg gjennomgang av informasjonstryggleiksarbeidet i leiinga, utan at det er etablert dokument, prosedyrar eller anna som skildrar dette nærare.

Ved søk i kvalitetssystemet til kommunen (Compilo) i august 2023 finn revisjonen at det er etablert utkast til fleire prosedyreskildringar for arbeidet med informasjonstryggleik og personvern, men ikkje alle er ferdig utfylte.<sup>9</sup> Det er til dømes etablert ei mappe med namn «prosedyrer GDPR» med undermapper som inneheld dokument knytt til styrande-, kontrollerande-, gjennomførande-, administrative- og daglege prosessar knytt til arbeid med informasjonstryggleik og personvern. Under «styrande prosessar» er det lagt inn ein prosessskildring knytt til internkontrollsystem der det blir vist til mellom anna årshjul for leiinga sin gjennomgang og prosedyrar for risikostyring, men utan at det er lagt inn nærare skildring eller dokumentasjon knytt til dette.

Kommunen har etablert nokre malar, skjema mv. som støtte i informasjonstryggleiksarbeidet. Det er mellom anna etablert eit skjema<sup>10</sup> for tinging av brukartilgang som leiarar skal nytte ved tildeling av nye brukartilgangar. Skjema ligg tilgjengeleg på kommunen sine intranettsider. Det er vidare utarbeidd sjekklister for handsaming av personvernopplysningar, mal for behandling av personvernopplysningar og mal for personvernkartlegging av fagsystem. Dei nemnte sjekklister og malane ligg også tilgjengeleg på kommunen sine intranettsider. Revisjonen finn også at det per august 2023 er etablert ei skildring av korleis ein skal føre protokoll over handsaming av

<sup>9</sup> Tysnes kommune. Compilo: Støtteprosessar. GDPR/personvern.

<sup>10</sup> Tysnes kommune. Tinging av brukarident. Ikkje datert.

personopplysningar, og denne ligg tilgjengeleg saman med mal for handsaming av personopplysningar på kommunen sine intranettsider.

### 3.4.2 Vurdering

Revisjonen vurderer at Tysnes kommune ikkje i tilstrekkeleg grad har etablert tydelege ansvarsforhold knytt til informasjonstryggleik. Undersøkinga viser at det i all hovudsak går fram av kommunen si handbok i informasjonssikkerhet kva ansvar og oppgåver som ligg til ulike rollar i kommunen når det gjeld informasjonstryggleiksarbeidet. Undersøkinga indikerer samtidig at det står att ein del arbeid med å sikre at rollar og ansvar i dette arbeidet er tilstrekkeleg tildelt, kommunisert og etterlevd. Revisjonen vil påpeike at det er øvste leiing sitt ansvar å sikre det er etablert tydelege ansvarsforhold.

Revisjonen vurderer at Tysnes kommune på revisjonstidspunktet ikkje har etablert tilstrekkeleg rutinar knytt til informasjonstryggleik. Undersøkinga viser at kommunen er i prosess med å utarbeide slike rutinar og prosedyrar, men at dette per august 2023 ikkje ennå er ferdigstilt. Revisjonen vil understreke at kommunen skal sikre at internkontrollen er systematisk og at det er etablert nødvendige rutinar og prosedyrar (kommunelova §25-1).

## 3.5 System for og gjennomføring av kontroll og etterprøving av informasjonstryggleik

### 3.5.1 Datagrunnlag

#### Kontroll av informasjonstryggleik

I kommunen si *handbok i informasjonssikkerhet* går det fram at det skal gjennomførast tilfredsstillande internkontroll og under dette tryggleiksrevisjonar og den årlege gjennomgangen til leiinga. Kommunen opplyser at kommunen hausten 2022 starta innføringa av eit nytt kvalitetssystem (Compilo), og at dette systemet mellom anna skal bidra til å systematisere kommunen sitt arbeid med internkontroll på informasjonstryggleiksområdet.

Det går fram av handboka at *den årlege gjennomgangen for leiargruppa* skal samanfatte status for arbeidet med informasjonstryggleik i kommunen og avdekke om informasjonstryggleiken er tilstrekkeleg ivaretatt. Det blir vidare vist til at det er nokre faste punkt som skal bli gjennomgått og vurdert i den årlege gjennomgangen for leiinga, til dømes resultat og hovudkonklusjonar frå informasjonstryggleiksrevisjonar, registrerte avvik og rapportar frå offentlege og interne tilsyn. Det skal i samband med gjennomgangen i leiargruppa også fastsettast tiltak for det vidare tryggleiksarbeidet i kommunen.

Leiinga sin årlege gjennomgang har på revisjonstidspunktet ikkje vore gjennomført i kommunen. Rådmannen opplyser at planen er å gjennomføre dette i løpet av 2023.

Det blir i intervju vist til at kommunen jobbar for å få på plass regelmessig rapportering om informasjonstryggleik og personvern og at det etter planen framover skal utarbeidast ein årleg rapport på tema. Rapporten skal utarbeidast av IT-leiar med innspel og merknader frå personvernombod og vil utgjere grunnlaget for årleg gjennomgang til leiinga. Det blir vist til at det ikkje er planlagt at leiarar skal involverast i rapporten knytt til årleg gjennomgang av personvernarbeidet, men at ein truleg vil ta utgangspunkt i mal for HMT-arbeid i arbeidet med denne rapporten og at det dermed er naturleg at rapporten vil omtale dei enkelte tenesteområda.

Det er ikkje spesifisert i handbok i informasjonssikkerhet korleis eller kor ofte tryggleiksrevisjonar skal gjennomførast eller kven som skal gjennomføre dette. Revisjonen merkar seg at det per august 2023 er lagt inn ei prosedyreskildring av «egenkontroll og sikkerhetsrevisjon» i kvalitetssystemet til kommunen. Det går her fram at leiar skal gjennomføre tryggleiksrevisjon/eigenkontroll jamleg, og minimum ein gang årleg, og det er lagt inn skildring av ansvaret til høvesvis behandlingsansvarleg (rådmann), tryggleiksleiar, personvernombod og leiar når det gjeld slike tryggleiksrevisjonar.

Det går fram at kommunen på revisjonstidspunktet ikkje har kome i gang med tryggleiksrevisjonar. Det er etter det revisjonen kjenner heller ikkje etablert formelle system og rutinar for korleis leiarar skal gjennomføre kontroll tryggleiksrevisjonar innan sine respektive ansvarsområde.

#### Tilgangsstyring

Tilgang og brukarkontroll er mellom anna omtalt under kapittelet om leiarar sitt ansvar i kommunen si handbok i informasjonssikkerhet. Her går det til dømes fram at leiarar er ansvarlege for å sikre at tilgangen til dei tilsette i

system og program er avgrensa til berre det dei har behov for i sitt arbeid, og vidare at tilgangen blir avslutta når tilsette avsluttar arbeidsforhold i organisasjonen.<sup>11</sup>

Som nemnt i avsnitt 3.4.1 er det etablert eit skjema for tinging av brukartilgang som leiarar skal nytte ved tildeling av nye brukartilgangar, og som ligg tilgjengeleg på kommunen sine intranettsider<sup>12</sup>. Det går fram at leiarar i kommunen gjennom dette skjema sender bestilling på systemtilgangar til IT-leiar, og at det deretter er IT-leiar som gir systemtilgangar til dei aktuelle nye brukarane. I skjema går det fram informasjon om at leiarar, før brukartilgang blir gitt, skal gjennomgå kapittel 1 og 2 i handbok i informasjonssikkerhet med den tilsette. Dersom den nye brukaren har ei leiarrolle, så skal ein også ha gjennomgått kapittel 3 i handboka. Det går ikkje fram av skjema for tinging av brukartilgang kva type tilgang brukaren skal ha i kommunen sine system (til dømes lesetilgang, full tilgang mv.), og det er heller ikkje lagt inn tilvising eller lenke til kva ein finn dette omtalt.

I intervju med IT-leiar går det fram at han ved førespurnad om ny brukartilgang gjennomgår skjema og sjekkar at alt er riktig utfylt. Dersom dette er ok gir han beskjed til superbrukar i det aktuelle systemet om tilgang og gir deretter beskjed til leiar om at det er oppretta tilgang («brukarident»).

Det går fram av intranettsidene at skjema for bestilling av brukartilgang kan nyttast for å søke tilgang i system for tilsette som *ikkje* høyrer til oppvekstområdet, og at oppvekstleiarane må kontakte ein IKT-rettleiar ved ein av skulane i kommunen for å skaffe brukartilgang i relevante system.<sup>13</sup> Det går ikkje fram om det er etablert rutine eller verktøy for å sikre at leiarar i desse tilfella gjennomgår handbok i informasjonstryggleik med nyttilsette.

Det blir vidare vist til at det er etablert eit skjema som skal fyllast ut når tilsette sluttar og tilgangar skal avsluttast. Det blir vist til at dette skjema ligg tilgjengeleg på kommunen sine intranettsider og at det skal sendast via e-post til IT-leiar. Revisjonen kan ikkje per august 2023 sjå at eit slikt skjema føreligg på kommunen sine intranettsider.

I intervju blir det påpeikt at det er behov for å etablere skjema og rutinar som sikrar at leiarar søker om endra tilgang dersom tilsette får endra arbeidsoppgåver og dermed skal ha andre tilgangar i systema. Det går fram at det per i dag ikkje er etablert rutinar for dette.

Kommunalsjef for helse og omsorg peiker på at dei innanfor hennar sektor har ein rådgjevar som er ansvarleg for pleie- og omsorgssystemet opp mot leverandør og tenestene (superbrukar), og at denne rådgjevaren nyleg har gjennomgått administrasjonsinnstillingane i fagsystemet til helse og omsorg (CosDoc) for å sikre at tilsette har riktige tilgangar.

Kommunen viser til at det i kommunen sin digitale arkivplan<sup>14</sup> under mappa «informasjonstryggleik og tilgangsstyring» og «Instruks for handsaming av elektroniske system» er lagt inn eit *skjema for tildeling av brukarar i fagsystem*. Det går fram av skjema at leiaren til den nyttilsette skal sende dette skjema til *systembrukaransvarleg*, eventuelt til systembrukaransvarleg via e-post til fellestenesta i kommunen. I skjema skal det mellom anna fyllast inn kva fagprogram brukar skal ha tilgang til og kva type tilgangar vedkomande skal ha. Det går fram at skjema skal fyllast ut ved nyttilsetjing, endring av arbeidsoppgåver og avslutting av arbeidsforhold. Det er vidare i kommunen sin digitale arkivplan lagt inn instruks for handsaming av elektroniske system for 10 av kommunen sine elektroniske system.<sup>15</sup> I desse skildringane går det fram ansvar for tildeling og ajourhald av brukarrettigheter i systema. Ikkje alle instruksane er ferdig utfylte, til dømes når det gjeld rettigheter for ulike rollar i systemet. Det er ikkje lagt inn tilvising til retningslinjer, regelverk eller rutinar knytt til informasjonstryggleik i desse dokumenta.

Rådmann viser til at det har vore behov for å sikre betre kontroll med bestilling av brukartilgangar, og at kommunen tidlegare mellom anna har oppdaga at brukarar som ikkje lenger var tilsette framleis hadde tilgang til kommunale fagsystem. Då dette blei oppdaga blei brukarane sletta.

I gjennomført GDPR-kartlegging av system som blir nytta i den kommunale NAV-tenesta og i Flyktningtenesta, går det fram at alle tilsette i har tilgang til alle opplysningar om alle brukarar i systema. Kommunalsjef for helse og omsorg peiker på at det berre er tre personar som er tilsette i NAV og at det derfor er behov for at alle tilsette på eininga har full tilgang til informasjon om alle brukarane. Ho viser til at denne tenesta er sårbar ved sjukdom og fråvær, og at det dermed er vurdert at kommunen kan gi betre tenester til brukarane gjennom at alle tilsette har

<sup>11</sup> Det blir her vist til rutinar om avslutning av arbeidsforhold vedtatt av kommunestyret, men det er ikkje lagt inn lenke eller liknande til dette vedtaket og det går heller ikkje fram dato for vedtaket.

<sup>12</sup> Tysnes kommune. *Tinging av brukarident*. Ikkje datert.

<sup>13</sup> Ein kan gjennom intranettskjema bestille brukartilgang for tilsette i domenet @tysnes.kommune.no, men ikkje for tilsette i domenet @tysnesoppvekst.no.

<sup>14</sup> Tysnes kommune. Arkivplan. <https://tysnes.arkivplan.no/>

<sup>15</sup> ESA (sak og arkivsystem), DIPS Sosial, CosDoc, Agresso UBW, GIS/LINE, Visma Flyktning, Visma Flyt Skole (for kvar av dei tre skulane) og Visma Flyt barnehage.

tilgang og kan hjelpe brukarane ved behov. Kommunalsjef peiker på at det i systemet er mogeleg å skjerme mottakar ved behov, til dømes dersom inhabilitet hos tilsette er ei utfordring. Det er vidare mogeleg å undersøke kva tilsette som har opna og lest mapper knytt til enkeltpersonar. Det går ikkje fram at kommunen har rutinar for å jamleg undersøke logg for kva tilsette som har gått inn i ulike mapper, og kommunalsjefen kjenner heller ikkje til at ein har undersøkt dette verken på eige initiativ eller på førespurnad frå brukarar.

### 3.5.2 Vurdering

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik på alle område. I handbok for informasjonssikkerhet blir retningslinjer for leiinga sin gjennomgang skildra, og det blir vist til at det skal gjennomførast tryggleiksrevisjonar. Desse styringsaktivitetane var ikkje gjennomført på revisjonstidspunktet. For tryggleiksrevisjonane var det på revisjonstidspunktet heller ikkje etablert formelle system og rutinar der det går fram korleis å gjennomføre tryggleiksrevisjonar. Revisjonen merkar seg også at det er ein plan om å få på plass årleg rapportering om informasjonstryggleik og personvern men at dette ikkje var implementert på revisjonstidspunktet. Revisjonen påpeiker difor at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta som seier at kommunen skal ha ein internkontroll på området som baserer seg på anerkjente standardar for styringssystem for informasjonstryggleik (§ 15).

Undersøkinga viser at det er ulike system for registrering av brukartilgangar, og at det ikkje går fram av skjema for tinging av brukaridentitet kva type tilgang brukaren skal ha (til dømes lesartilgang, full tilgang). Det blir også vist til at det er behov for å etablere skjema og rutinar som sikrar at leiarar søker om endra tilgang dersom tilsette får endra arbeidsoppgåver og dermed skal ha andre tilgangar i systema. Manglande registrering av endringar fører til ein risiko for at brukarar har tilgangar dei ikkje har behov for, og følgeleg risiko for at krava knytt til konfidensialitet i regelverket ikkje alltid blir etterlevd. Dette er forhold som revisjonen meiner at kommunen må utbetre for å ha eit tilstrekkeleg system som sikrar tilgjenge og konfidensialitet i informasjonssystema som blir nytta i kommunen.

Revisjonen merkar seg også det at finst enkeltvise rutinar med instruksar og skjema som gjeld tilgangsstyring for nokre system. Revisjonen meiner at kommunen med fordel burde samle og gjere tilgjengeleg felles retningslinjer og rutinar for tilgangsstyring for alle kommunen sine elektroniske system slik at det blir tydeleg for dei involverte kva ansvar dei har for å sikre oppdaterte og riktige tilgangar, kven ein skal kontakte og korleis ein skal gå fram ved endring eller avslutning av brukartilgang mv.

# 4 Etterleving av krav i personvernlovgjevinga

## 4.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

*I kva grad har etterlever Tysnes kommune sentrale krav i personvernlovgjevinga?*

Under dette:

- Har kommunen utnemnt eit personvernombod og etablert personvernerklæring i samsvar med krav om dette i regelverket?
- Fører kommunen protokoll over behandlingsaktivitetar av personopplysningar?
- I kva grad blir det gjort risiko- og konsekvensvurderingar av behandling av personopplysningar der det er krav om dette?
- I kva grad har kommunen oversikt over avvik knytt til personvern, og i kva grad blir slike avvik meldt til Datatilsynet?

## 4.2 Revisjonskriterier

Krav til kommunen når det gjeld etterleving av krav i personvernlovgjevinga blir utleia frå personopplysningslova og personvernforordninga.

Kommunen skal:

- utpeike eit personvernombod og sikre at personvernombodet blir involvert i rett tid i alle spørsmål som gjeld vern av personopplysningar og stille tilstrekkeleg med ressursar til rådighet for at personvernombodet kan gjennomføre oppgåvene pålagt stillinga (personvernforordninga artikkel 37 og 38)
- peike ut personvernombod på grunnlag av faglege kvalifikasjonar og særleg på grunnlag av djupnekunnskap om personvernlovgjeving og praksis på området samt evne til å utføre oppgåvene nemnt i artikkel 39 (personvernforordninga artikkel 37 punkt 5).
- informere registrerte personar om at kommunen handsamar personopplysningar om dei og at slik informasjon er kortfatta, open, forståeleg, lett tilgjengeleg på eit klårt og enkelt språk (personvernforordninga artikkel 12, 13 og 14).
- føre ein protokoll over behandlingsaktivitetane av personopplysningar som blir utført (personvernforordninga artikkel 30).
- gjennomføre risikovurderingar av behandlinga av personopplysningar i dei tilfella der slik behandling medfører høg risiko for rettar og fridom for fysiske personar (personvernforordninga artikkel 35 og 36).
- dokumentere avvik knytt til personvern og om verknadane av det og kva tiltak som er satt i verk for å utbetre avviket. Brot på personopplysningstryggleiken skal utan ugrunna opphald og så snart som mogleg meldast til Datatilsynet innan 72 timar (personvernforordninga artikkel 33).

Sjå vedlegg 4 for utfyllande revisjonskriterium.

## 4.3 Personvernombod og personvernerklæring

### 4.3.1 Datagrunnlag

#### Personvernombod

Tysnes kommune har utnemnt eit personvernombod og etablert stillingsskildring for personvernombod i kommunen<sup>16</sup>. Rolle og ansvar for personvernombodet er også skildra i kommunen si *handbok i informasjonsikkerhet*.

I stillingsskildringa for kommunen sitt personvernombod går det fram føremål med stillinga, ansvar og mynde og arbeidsoppgåver. I følge stillingsskildringa skal personvernombodet medverke til at verksemda varetek sine plikter i personvernregelverket gjennom å gje informasjon og råd, samt samarbeide med tilsette, leiarar og relevante stabs- og støttefunksjonar. Personvernombodet skal vidare vere ein uavhengig rolle som skal sikre at personopplysningar vert handsama i samsvar med regelverket. Det er rådmannen som utpeiker personvernombod i verksemda.

Det går vidare fram at for å sikre at personvernombodet får varetatt sine oppgåver, pliktar leiinga i kommunen å syte for 1) innsyn i alle personvernrelaterte avvik, 2) oversending av informasjon og resultat knytt til DPIA, nye system og nye handsamingar, 3) tilgang til verksemda sine rutinar og protokollar for datahandsaming, og 4) jamleg rapporteringsmøte til rådmann/strategisk leiing.

Det går fram av intervju at det har vore utfordringar knytt til kontinuitet i rolla som personvernombod i kommunen. Det blir vist til at kommunen hadde eit aktivt personvernombod då personvernforordninga blei innført i 2018, men at kommunen grunna sjukefråvær, i praksis var utan personvernombod i store delar av perioden mellom 2020 og 2023. Det går fram at noverande personvernombod i kommunen har hatt denne rolla sidan januar 2023, og at personvernombodsrolla utgjer 15 prosent av stillinga til vedkomande.

Rådmannen viser til at personvernombodet i kommunen er utpekt i samsvar med Datatilsynet sine vurderingar knytt til kvalifikasjonskrav for personvernombod.<sup>17</sup> Han påpeiker vidare at personvernombodet har relevant praksis og er godt skikka for oppgåvene som ligg til rolla. Rådmann understrekar vidare at kommunen har følgd opp Datatilsynet si tilråding om å gi tilleggsutdanning som er tilpassa rolla som personvernombod. Noverande personvernombod starta på denne tilleggsutdanninga formelt eit halvt år før vedkomande tiltredde funksjonen og fullførte eksamen etter tiltreding. Personvernombod tar også på revisjonstidspunktet studiepoeng i personvern ved Høgskulen i Innlandet.

Personvernombod peiker på at det våren 2023 har vore utfordrande å sette av tid på å jobbe systematisk i rolla som personvernombod, då 85 prosent stillinga som kommunikasjons- og personalrådgjevar har tatt mykje av kapasiteten. Det går vidare fram av intervju at personvernombod opplever å i svært liten grad bli involvert i prosessar eller spørsmål knytt til vern av personopplysningar. Personvernombod opplever samtidig at det er utfordrande å ha oversikt over kva prosessar vedkomande eventuelt bør involverast i, då det på revisjonstidspunktet ikkje har vore tilstrekkeleg med tid til å sette seg inn i dette.

Rådmann påpeiker at det er gjennomført viktige tiltak for å sikre involvering av personvernombod. For det første er personvernombod fast deltakar i møte i utvida leiarteam, noko som omfattar alle kommunale mellomleiarar på einingsnivå, samt kommunalsjefar og fleire av rådgjevarfunksjonane. Personvernombod blir vidare invitert til møte i strategisk leiing ved behov, og det går fram at vedkomande har deltatt i desse møta. Rådmann viser til at det kan vere aktuelt å ha med personvernombod fast i møta i strategisk leiing for å gjennomgå meldte avvik saman med kvalitetsrådgjevar i kommunen. Rådmann viser vidare til at det er etablert faste møtepunkt mellom rådmann, IT-leiar og personvernombod ein gang i månaden, der det er sett halvanna time per møte til å gjennomgå avvik, nye system, informasjon og arbeid retta mot verksemda, rutine og systemarbeid innanfor personvern, relevante kompetansetiltak mv.

Rådmannen påpeiker i intervju at personvernombodet i kommunen har ei autonom rolle. Han viser vidare til at han jamleg søker rettleiing frå personvernombodet og at personvernombod mottar alle avvik knytt til personvern og informasjonstryggleik i sanntid gjennom avvikssystemet i Compilo Rådmannen viser til at tiltak som er sett i

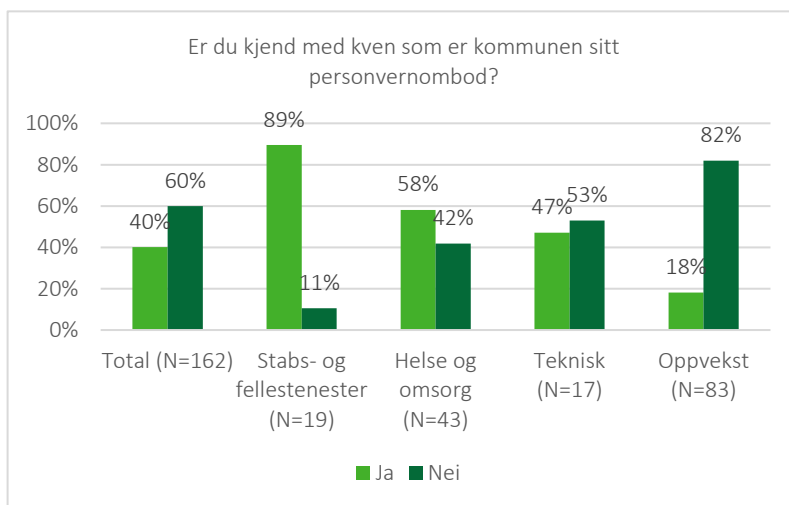
<sup>16</sup> Tysnes kommune. Personvernombod. Ikkje datert

<sup>17</sup> Datatilsynet. Hvilke kvalifikasjoner trenger et personvernombud? Sist endret 06.01.2023. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvilke-kvalifikasjoner-trenger-et-personvernombud/>

verk er i samsvar med Datatilsynet sine tilrådingar om å leggja til rette for at personvernombodet kan utføra sitt arbeid.<sup>18</sup>

Respondentane som svarte på spørjeundersøkinga i samband med denne forvaltningsrevisjonen blei bedt om å svare på om dei er kjende med kven som er kommunen sitt personvernombod. På dette spørsmålet svarar totalt 60 prosent «nei». Som vist i figur 3, er det relativt stor skilnad mellom sektorane når det gjeld kjennskap til personvernombodet. Heile 82 prosent av respondentane frå oppvekstsektoren svarar at dei ikkje kjenner til kven som er personvernombod.

Figur 3: Kjennskap til kommunen sitt personvernombod



### Personvernerklæring

Tysnes kommune har etablert ei *fråsegn om personvern* som er tilgjengeleg på kommunen sine nettsider.<sup>19</sup> Ein kjem fram til personvernerklæringa via kommunen si framside ved å gå inn på overskrifta «om Tysnes», for deretter å gå inn på sida «administrasjon», og vidare trykke på lenka «personvern» der ein kan gå inn på «Fråsegn om personvern». Det er ikkje lagt inn lenke eller snarveg til personvernerklæringa på framsida for kommunen sine nettsider (tysnes.kommune.no).

I personvernerklæringa går det fram at kommunen har som mål at informasjonstryggleik og personvern skal vera ein naturleg del av verksemda. Vidare gjer kommunen i personvernerklæringa greie for korleis personopplysningar skal handsamast. Overordna inneheld personvernerklæringa ei utgreiing om følgjande tema i egne faner:

- Grunnprinsipp
- Føremål
- Kva er grunnlaget for at me kan nytta personopplysningane dine?
- Rett til personvern og teieplikt
- Innsyn
- Rett til å få korrigert personopplysningar som er feil
- Rett til å avgrense handsaming
- Overføring av personopplysningar
- Rett til å få sletta personopplysningar
- Kven deler me dine personopplysningar med?
- Innebygd personvern og personvern som standardinnstilling
- Informasjonskapslar og analyse
- Personvernombod

Under punktet «rett til å få sletta personopplysningar» står det at «du kan ha rett til å få sletta opplysningar om deg sjølv. Denne retten har likevel også unntak. Retten gjeld til dømes ikkje for opplysningar som er arkivpliktige eller er naudsynte for å kunne fremja og ivareta rettskrav». Det er deretter lenka til personopplysningslova (artikkel 12 og 17) og det blir vist til arkivregelverket.

Under punktet «overføring av personopplysningar» står det at «for einskilde handsamingar kan du ha rett til det som vert kalla dataportabilitet. Det vil sei at du kan krevja å få overført personopplysningane frå oss til nokon andre. Denne retten har likevel fleire unntak». Det blir deretter lenka til personopplysningslova (artikkel 12 og 20).

<sup>18</sup> Datatilsynet. Hvordan tilrettelegge for personvernombudets arbeid? Sist endret 06.01.2023. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvordan-tilrettelegge/>

<sup>19</sup> Tysnes kommune. Fråsegn om personvern: <https://www.tysnes.kommune.no/raasegn-om-personvern.594897.nn.html>



Respondentane som svarte på spørjeundersøkinga blei spurt om dei er kjend med kommunen si personvernerklæring. På dette spørsmålet svarar halvparten av respondentane «delvis» medan 38 prosent svarar «nei» og 12 prosent svarar «ja».

#### 4.3.2 Vurdering

Tysnes kommune har utnemnt eit personvernombod, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Revisjonen vil påpeike at kommunen pliktar å stille til rådighet dei ressursar som er nødvendig for at personvernombodet skal kunne utføre lovpålagde oppgåver (2. punkt i artikkel 38).

Det går vidare fram at personvernombod opplever å i liten grad bli involvert i prosessar eller spørsmål knytt til vern av personopplysningar. Revisjonen er merksam på at noverande personvernombod har vore tilsett i kommunen i ein relativt kort perioden, og at det er sett inn fleire gode tiltak i perioden for å sikre involvering av personvernombodet. Revisjonen vil samtidig påpeike at kommunen etter personvernforordninga pliktar å sikre at personvernombodet på riktig måte og i rett tid blir involvert i alle spørsmål som gjeld vern av personopplysningar (1. punkt i artikkel 38).

Tysnes kommune har etablert personvernerklæring. Revisjonen vurderer samtidig at kommunen ikkje har sikra at denne erklæringa har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane. Datatilsynet skriv mellom anna i si rettleiing om verksemdene sine pliktar etter personvernregelverket<sup>20</sup> at verksemdene ikkje kan bruke juridisk eller teknisk sjargong når dei kommuniserer om personopplysningar, informasjonen skal vere forståeleg for målgruppa og informasjonen skal vere konkret (unngå formuleringar som «vi kan bruke personopplysningar til...»). Undersøkinga viser, etter revisjonen si vurdering, at Tysnes kommune i si fråsegn om personvern ikkje er tilstrekkeleg konkret og at det er nytta ein del omgrep og formuleringar som gjer fråsegna utfordrande å forstå for målgruppa.

Revisjonen vurderer vidare at kommunen si personvernerklæring ikkje er tilstrekkeleg lett tilgjengeleg, i samsvar med krav om dette i regelverket (artikkel 12 i personvernforordninga). Svar på spørjeundersøkinga indikerer at personvernerklæringa også er relativt ukjend for dei tilsette i kommunen; berre 12 prosent oppgjev å vere kjend med denne. Det skal ikkje vere nødvendig for brukarar å måtte leite etter informasjon om handsaming av personopplysningar, og revisjonen meiner derfor at kommunen bør plassere lenke til personvernerklæringa lett tilgjengeleg for ålmenta, til dømes på framsida for kommunen sine nettsider.

## 4.4 Protokoll over behandlingsaktivitetar

### 4.4.1 Datagrunnlag

I Tysnes kommune si *handbok i informasjonssikkerhet* går det fram at behandlingsprotokoll etter GDPR-reglar skal førast dersom personopplysningar blir handsama i ein av kommunen sine løysingar og at personvernombodet skal kontaktast dersom ein treng meir informasjon om behandlingsprotokollar.

Kommunen har også på sine intranettsider laga ei sjekklister for behandling av personopplysningar der det går fram kva ein må vurdere før ein skal handsame personopplysningar, til dømes at ein må definere eit klart føremål, identifisere behandlingsgrunnlag mv.<sup>21</sup> Sjekklister har lenker til utdjupande informasjon på Datatilsynet sine nettsider.

Kommunen har vidare etablert ein mal for utarbeiding av protokoll for behandling av personopplysningar, og denne ligg tilgjengeleg på kommunen sine intranettsider.<sup>22</sup> På intranettsida føreligg det også ei kort skildring av korleis ein skal fylle ut protokoll. I malen for utarbeiding av protokoll er det lagt inn eksempel på korleis å fylle inn protokollen og det er lagt inn lenke til relevant støttemateriell. Til dømes er det under kolonna «formål med

<sup>20</sup> Datatilsynet. Virksomhetenes plikter. Informasjon og åpenhet. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/>

<sup>21</sup> Tysnes kommune. *Sjekklister for behandling av personopplysningar*. Tilgjengeleg frå: <https://tysnes.intra.custompublish.com/sjekklister-for-behandling-av-personopplysningar.6580227-587357.html>.

<sup>22</sup> Tysnes kommune. *Protokoll over behandling av personopplysningar*. Tilgjengeleg frå: <https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fimg1.custompublish.com%2Fgetfile.php%2F5111947.2571.tplbbpjumwuwmi%2FProtokoll%2Bover%2Bbehandlinger%2Bav%2Bpersonopplysningar.xlsx%3Freturn%3Dtysnes.intra.custompublish.com&wdOrigin=BROWSELINK>

behandlinga» lagt inn lenke til Datatilsynet og deira skildring av fastsetting av formål<sup>23</sup> og det er under kolonna «kategoriar av personopplysning» lagt inn lenke til Datatilsynet si skildring av kva ein personopplysning er.<sup>24</sup>

Det går ikkje fram av tilsendt dokumentasjon kven som har ansvaret for å fylle ut behandlingsprotokollar og sikre at protokollar er oppdatert og speglar dei behandlingane som kommunen gjennomfører. Rådmann viser i intervju til at det er einingsleiarar og brukarane av systema som er ansvarlege for å halde oversikt over kva personopplysningar som blir behandla i dei ulike einingane, men at det i siste instans er rådmannen som har dette ansvaret.

Rådmann viser til at kommunen i 2023 har kjøpt inn modul for personvern i kvalitetssystemet (Compilo). Kommunen opplyser at utfylte behandlingsprotokollar blir lagra i Compilo. Per utgangen av august 2023 er det lagra 16 protokollar i Compilo for handsaming av personopplysningar i kommunen sine informasjonssystem. Alle systema er tilknytt arbeid i sentraladministrasjonen (til dømes innkjøp, rekruttering og personal). Det er ikkje lagra behandlingsprotokollar for system nytta til dømes i oppvekst- eller helse og omsorgssektoren i kvalitetssystemet. Behandlingsprotokollane lagra i Compilo følgjer ikkje kommunen sin etablerte mal som føreligg på kommunen sine intranettsider.

Det går fram av intervju at det ikkje er utarbeidd protokollar for behandling av personopplysningar innan helse- og omsorgssektoren i kommunen. Kommunalsjef for sektoren peiker på at det er kommunalsjef, saman med einingsleiarane som systemeigarar, som har ansvaret for at det blir utarbeidd behandlingsprotokollar. Det går vidare fram av intervju at skulane har starta eit arbeid med å føre behandlingsprotokollar, men at dette så langt ikkje er lagt fram for personvernombod eller leiinga i kommunen.

Rådmann peiker i intervju på at personvernombodet er i gang med å planlegge og gjennomføre workshops for leiarar og tilsette i kommunen om informasjonstryggleik og personvern, og at desse samlingane mellom anna rettar merksemd mot utarbeiding av behandlingsprotokollar. I april 2023 blei det gjennomført workshop for sentraladministrasjonen og personvernombodet opplyser om at tilsvarande har vært gjennomført med rektorane og IKT-rettleiarane ved skulane. Personvernombodet peiker på at protokollføring inngjekk i denne opplæringa.

Rådmannen viser til at det er ei utfordring å sikre etterleving av retningslinjene for informasjonstryggleik i kommunen, og at det derfor mellom anna er sett i gang eit arbeid med å sikre at behandlingsprotokollar er godt nok oppdatert av dei ansvarlege leiarane. Rådmann peiker på at oversikt over personopplysningar som blir handsama er eit fokusområde i kommunen, og at det blir arbeidd med å sikre at kommunen har nødvendige og oppdaterte behandlingsprotokollar.

#### 4.4.2 Vurdering

Tysnes kommune fører ikkje i tilstrekkeleg grad protokoll over behandlingsaktivitetar av personopplysningar. Undersøkinga viser at kommunen har sett i gang eit arbeid for å sikre at det framover skal førast protokoll over behandlinga av personopplysningar; det er mellom anna etablert mal for dette arbeidet og det er gjennomført workshops med nokre av leiarane i kommunen for å rette merksemd mot protokollføring. Revisjonen merkar seg likevel at kommunen på revisjonspunktet har utarbeidd få protokollar for behandling av personopplysningar og at dette heller ikkje blir gjort systematisk. Det er heller ikkje tilstrekkeleg tydeleggjort kven som skal ha dette ansvaret for dei ulike systema. Dette er ikkje i samsvar med krav om utarbeiding av behandlingsprotokollar (artikkel 30 i personvernforordninga).

## 4.5 Risiko- og konsekvensvurderingar av behandling av personopplysningar

### 4.5.1 Datagrunnlag

Det går fram av Tysnes kommune si *handbok i informasjonssikkerhet* at det ved innkjøp av nye datasystem skal gjennomførast risiko- og sårbarheitsanalyse (ROS-analyse) og under dette alltid vurderast behov for å utarbeide ei vurdering av personvernkonsekvensar (DPIA (Data Protection Impact Assessment)). Det går vidare fram av handboka at ROS-analysar skal gjennomførast før løysningar blir tatt i bruk og at systemeigar skal oppdatere risikovurderingane ved årleg gjennomgang av informasjonstryggleik i samråd med personvernombod og IT-leiar.

<sup>23</sup> Datatilsynet. Virksomhetenes plikter. Fastsette formål. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/fastsette-formal/>

<sup>24</sup> Datatilsynet. Hva er en personopplysning. Sist endret 26.07.2023. <https://www.datatilsynet.no/rettigheter-og-plikter/personopplysninger/>

Systemeigar er også pliktig til å rådføre seg med personvernombod og IT-leiar i alle spørsmål knytt til personvern og behandling av personopplysningar.

Tysnes kommune viser til 12 ROS-analysar av system henta frå KS sin Fiks-plattform (til dømes SvarUt, Fiks bekymringsmelding og Fiks folkeregister).<sup>25</sup> Ved gjennomgang av analysane viser det seg at felt som skal fyllast ut av kommunen ikkje er gjennomført. Ein kan hente ROS- malar på Fiks-portalen til KS og det går fram at malane på plattformen er dei same som kommunen viser til i samband med forvaltningsrevisjonen.

Det går fram følgjande på KS sine nettsider:

For de fleste Fiks-tjenestene har KS laget maler dere kan ta utgangspunkt i når dere gjør deres egne risiko- og sårbarhetsanalyser (ROS) og vurderer personvernkonsekvenser (DPIA). **Vi håper malene kan være til hjelp, men dere må selv gjøre deres egne vurderinger og tilpasse innholdet til kommunens situasjon** (revisjonen si utheving).

Risikokartlegginga i alle desse ROS-analysemalane inneheld generiske eksempel på aktørar og scenario til dømes «aktør: Arne Administrator, scenario: stjeler informasjon ved å gjøre et uautorisert innsyn i mottatte meldinger, som er et konfidensialitetsbrudd». Det er lagt inn rettleiing i dokumenta og spesifisert kvar kommunen skal legge inn sine vurderingar mv. Kommunen har i all hovudsak ikkje fylt ut dette. I den eine ROS-analysen som omhandlar Fiks bekymringsmelding er det lagt inn noko informasjon frå kommunen (risikovurdering av rolla til IT-leiar), og det er lagt inn status «føreslått» på eit av ti felt der kommunen sjølv skal legge inn statusskildring og ev. kommentar.

Revisjonen har ikkje fått tilsendt ROS-vurderingar for andre system som blir nytta i kommunen.

I intervju peikar rådmannen på at Tysnes kommune stort sett kjøper system som «hyllevarer» til dømes system gjennom Fiks-plattformen til KS, og at det ofte er lite føremålstenleg at kommunen sjølv utfører risikovurdering av systema. Systema er standardløysingar som gjeld alle kommunar, og Tysnes kommune har derfor ikkje vurdert det som nødvendig å gjennomføre sjølvstendige risiko- og konsekvensvurderingar for handsaming av personopplysningar i desse systema.

Rådmannen og IT-leiar fortel også i intervju på at dei ikkje er sikre på om det er gjennomført risiko- og konsekvensutredningar av handsaming av personvernopplysningar i alle tilfelle der det er krav om det. Rådmannen påpeiker at det framover vil bli stilt krav om at risikovurderingar skal førast og systemskildringar skal førast til Compilo, og at dette gir betre moglegheit til å følgja opp dei vurderingane som blir gjort knytt til risikovurderingar for kvart einskilde fagsystem og også at dei blir jamleg revidert.

Det går vidare fram at ein i kommunen er usikre på om det er gjennomført konsekvensvurderingar av handsaming av personvernopplysningar (DPIA) i alle system kommunen brukar og der dette er nødvendig. Det blir vist til at kommunen har brukt nokre av systema over lang tid, og at det truleg ikkje er gjennomført DPIA når det gjeld desse systema.

Revisjonen har ikkje informasjon som tyder på at Tysnes kommune systematisk gjennomfører eller har prosedyrar for gjennomføring av vurdering av personvernkonsekvensar for behandling av personopplysningar som medfører høg risiko.

Det går fram at kommunen har brukt mal frå Fiks-plattformen for å gjennomføre DPIA for Fiks bekymringsmelding. Det blir vist til at fleire relevante tilsette var involvert i dette DPIA arbeidet, og at noverande personvernombod deltok i eitt av møta i samband med arbeidet (DPIA blei gjennomført før 1.1. 2023, og vedkomande var dermed ikkje ennå formelt tilsett som personvernombod). Personvernombodet peiker på at det i møte blei påpeikt at kommunen i for liten grad forankra arbeidet, då arbeidsgruppa i hovudsak tok i bruk KS sin mal for DPIA og fylte den ut.

Personvernombod påpeiker at personvernombodet så tidleg som mogeleg bør koplast på i vurdering av behov for DPIA, og at dette er noko ho har drøfta med rådmann.

#### 4.5.2 Vurdering

Revisjonen vurderer at Tysnes kommune ikkje i tilstrekkeleg grad gjennomfører risikovurderingar av handsaming av personopplysningar, og at det heller ikkje i samband med risikovurderingar systematisk blir gjort vurderingar av personvernrisikoar (DPIA). Manglande risikovurderingar og rutinar for gjennomføring av slike gjer at kommunen

<sup>25</sup> KS FIKS Tjenesteplattform er en plattform for utvikling og drift av kommunale applikasjonstjenester. Fiks-plattformen er utvikla og drifta av KS. Kjelde: KS.no

ikkje har oversikt over kvar det er personvernrisikoar, og kommunen veit derfor heller ikkje kva eventuelle tryggleikstiltak som fungerer og ikkje. Kommunen manglar med dette grunnlag for å gjere eventuelle justeringar og slik kontinuerleg forbetre informasjonstryggleiken. Manglande risikovurderingar betyr vidare at kommunen heller ikkje veit kva personopplysningar dei handsamar med høg risiko, og har difor heller ikkje grunnlag for å gjennomføre vurdering av personvernkonsekvensar ved behandling av personopplysningar med høg risiko, jf. personvernforordninga artikkel 35.

## 4.6 Oversikt over avvik knytt til personvern

### 4.6.1 Datagrunnlag

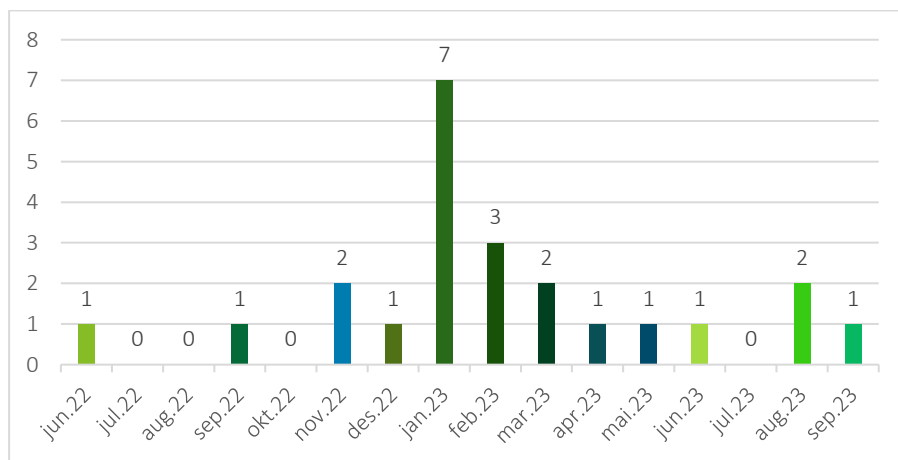
Tysnes kommune omtalar melding av avvik knytt til informasjonstryggleik og personvern i handbok i informasjonssikkerhet. I kapittel 3 om informasjonstryggleik for leiarar går det fram at alle tilsette skal ha kjennskap til korleis avvik skal registrerast i Compilo. Det går vidare fram i same kapittel at alle tilsette som oppdagar brot på informasjonstryggleiken og brot på reglementet, skal varsle om dette til personvernombod, og på den måten hjelpa til med å avgrensa eller hindra at opplysningar kjem på avvegar, blir urettmessig endra eller forsvinn.

Det er under kapittel 4 i handboka om internkontroll eit avsnitt som omhandlar handsaming av avvik. Her går det mellom anna fram at personvernombod kan få avviksmeldinga som ein munnleg førespurnad, tekstmelding, telefon eller som eit avviksmeldingsskjema. Det går fram at personvernombodet også kan sette i gang avviksbehandling på eige initiativ, utan at ei formell avviksmelding er mottatt. Det er deretter lagt inn ei punktliste som skildrar mottak og handsaming av avviksmeldingar. Første punkt viser til at avvika skal registrerast i Compilo og vidare at dersom avviket er av ein slik karakter at det er fare for at personopplysningar har komme på avvegar, vorte urettmessig endra eller gått tapt, så skal avviket meldast Datatilsynet.

Det er vidare omtalt i handbok for informasjonssikkerhet kva situasjonar som utløyer meldeplikt til Datatilsynet, og at personvernombodet, IT-leiar, behandlingsansvarleg og systemeigar har ansvar for å vurdere omfanget av innmeldte avvik, alvorsgrad og iverksetting av tiltak. Dei skal også vurdere om situasjonen løyser ut plikt til å varsle Datatilsynet. Det er ikkje omtalt i handboka eller i kommunen si *rutine for avvik og alvorlege hendingar*<sup>26</sup> at brot på personopplysningstryggleik skal meldast til Datatilsynet innan 72 timar (jf. personvernforordninga artikkel 33).

I Compilo føreligg det **oversikt over meldte avvik** relatert til personvern/informasjonstryggleik i perioden etter at kvalitetssystemet har blitt implementert i kommunen.<sup>27</sup> Det går her fram at det frå juni 2022 til og med august 2023 er meldt 21 slike avvik og at 11 av desse omhandla personopplysningar på avvege, 8 omhandla svikt i systematisk internkontroll knytt til personvern og 10 av avvika omhandla avvik knytt til tilgang til informasjon/system. To av avvika har blitt vurdert til å ha høg alvorsgrad, åtte er vurdert å ha låg risiko og elleve som middels risiko. Det går fram av intervju at ingen av dei meldte avvika er meldt vidare til Datatilsynet.

Figur 4: Informasjonstryggleiksavvik meldt mellom juni 2022 og august 2023 (Kjelde: Tysnes kommune)



<sup>26</sup> Tysnes kommune. Rutine for avvik og alvorlege hendingar. Compilo. Ikkje datert.

<sup>27</sup> Revisjonen har ikkje mottatt avviksstatistikk frå tida før kvalitetssystemet Compilo blei innført.

Per 1. september 2023 er ti av dei meldte avvika ikkje lukka. Avvika som framleis er under handsaming har blitt meldt mellom desember 2022 til september 2023, og det inkluderer avvik som har blitt vurdert å ha høg alvorsgrad.

Revisjonen har fått tilgang til mellom anna avviket meldt desember 2022 og som er vurdert å ha høg alvorsgrad. Avviket er knytt til lagring av personlege mapper innanfor sikker sone på eit område der tilsette frå legekontor, helsestasjon og psykisk helse har tilgang. Rådmann viser til at kvalitetsrådgjevar i tillegg hadde tilgang, då vedkomande er jordmor og har i periodar arbeidd ved helsestasjon. Dette avviket er på revisjonstidspunktet ikkje lukka og ikkje meldt til Datatilsynet. Rådmann peiker på at når dette avviket blei meldt og det blei gjort merksam på at det her kunne ligge informasjon som er personsensitiv, så valde rådmann å suspendere tilgangen for alle medarbeidarar. Han viser vidare til at det er gjennomført fleire tiltak for å følgje opp dette avviket og at det har vore fleire oppfølgingsaktivitetar våren 2023. Rådmann peiker på at alle tiltak blei gjennomført relativt tidleg og at avviket kunne vore lukka då, men at ein likevel har vurdert at avviket kunne stå ope til kommunen faktisk ser at iverksette tiltak fungerer. Rådmann viser til at IT-leiar gjennomførte slik kontroll i september 2023 og at det er såleis grunn til å lukke avviket.

Rådmann peiker på at det har vore ulike aktivitetar knytt til oppfølging av dette avviket som gjer at avviket er vurdert å kunne stå ope til rotårsaka er lukka. Han viser vidare til at saka ikkje er meldt til Datatilsynet på bakgrunn av rådmannen si vurdering av at brotet truleg ikkje vil «medføre ein risiko for fysiske personar sine rettigheter eller friheiter»<sup>28</sup>, og såleis ikkje skal meldast til Datatilsynet. Rådmann viser til at det er fleire tilhøve som er vurdert opp mot om brotet medfører ein slik risiko og at det er viktig å understreka at informasjonen ligg innanfor sikker sone, og at det er berre autorisert helsepersonell som ville kunne ha tilgang til informasjonen.

Det blir både i intervju og i spørjeundersøkinga peikt på at det førekjem i kommunen at det blir lagra sensitiv informasjon om tilsette og innbyggjarar på område der uvedkommande har innsyn.

Rådmann viser til eit anna eksempel på informasjonstryggleiksavvik og oppfølginga av dette i kommunen. I dette tilfellet blei det meldt avvik på at døra til fløyen til sentraladministrasjonen sto open om morgonen 1. desember 2022. Avviket blei vurdert som eit avvik i høve til informasjonstryggleik og personvern då det kan gje uvedkommande tilgang til kontor. Rådmann peiker på at det same dag som avviket blei meldt, blei informert om dette på kontormøte for sentraladministrasjonen og at avviket kunne, og ville i mange samanhengar blitt lukka gjennom eit slikt tiltak. Han viser til at kommunen valde å gå lenger ned i årsaka til avviket og sjå på låsesystem og skalsikring for heile rådhuset, og at dette førte til at det blei identifisert ein mogleg risiko ved at einskild tilsette nytta andre inngangar enn hovudinngangen. Det går vidare fram at det blei skifta låsesylindrar på alle dører, etablert ei rutine for låsing og sendt ut informasjon til alle tilsette. Rådmann peiker på at det tok 43 dagar å lukka dette avviket, og understrekar at det kan vere eit viktig poeng å bruke tid på å følgje opp meldte avvik.

Rådmannen peiker på at kommunen fram til nyleg ikkje har hatt gode system for, eller god nok oversikt over, avvik i tenestene. Han viser til at kommunen ved innføringa av Compilo langt på veg har byrja få nødvendig oversikt over avvik. Compilo blei innført i kommunen hausten 2022, og rådmann viser til at kommunen tidlegare ikkje har hatt digitalt avvismeldesystem, og avvik har blitt meldt inn skriftleg på papir. Rådmannen meiner at kommunen har hatt stor nytte av å innføre Compilo og at det gjer registrering av avvik enklare, samtidig som det gjer det mogleg å få oversikt over meldte avvik og å hente ut avviksstatistikk.

Det går fram av intervju at avvik knytt til informasjonstryggleik er eit av dei faste punkta på agenda i dei jamlege møta mellom personvernombod, rådmann og IT-leiar. Det blir vidare vist til at ein i dette møtet i april 2023 drøfta om nokre av dei meldte avvika burde meldast vidare til Datatilsynet, men at dei ikkje fekk avklart dette i møtet. Det blir vidare i intervju vist til at det ikkje er tilstrekkeleg tydeleg kven av dei tre som har ansvar når det gjeld å melde avvik til Datatilsynet.

I samband med verifiseringa av rapporten blir det påpeikt at i kommunen er det rådmannen som er behandlingsansvarleg å såleis har plikt til å melda avvik vidare til Datatilsynet. Det blir vidare haldt fram at dersom nokon skulle meine at denne plikta ikkje vert ivareteke av rådmann, så kan personvernombod, eller einkvan annan tilsett i verksemda varsle til Datatilsynet etter kommunen si rutine for varsling av kritikkverdige tilhøve.<sup>29</sup>

I spørjeundersøkinga fekk respondentane spørsmål om dei har opplevd eit eller fleire avvik knytt til informasjonstryggleik. Over ein av fire respondentar svara «ja» på dette spørsmålet (28 prosent), medan om lag halvparten svara «nei» (53 prosent) og om lag ein av fem svara «veit ikkje» (19 prosent). Respondentane som

<sup>28</sup> Personvernforordninga artikkel 35, første ledd.

<sup>29</sup> Tysnes kommune. Rutine for intern varsling av kritikkverdige forhold. Vedtatt i kommunestyret 10. juni 2009. Rullering i kommunestyret 24. september 2020.

svara at dei har opplevd informasjonstryggleiksavvik<sup>30</sup> blei vidare spurt om kor mange av avvika dei meldte vidare. Som framstilt i figur 5 svara om lag ein av tre (31 prosent) at dei ikkje har meldt frå om nokre av avvika, medan ein av fire svarar at dei høvesvis har meldt frå om «dei fleste» eller «nokre» av avvika dei har opplevd. Litt over ein av fire oppgjev å ha meldt frå om alle informasjonstryggleiksavvika dei har opplevd.

Vidare fekk respondentane som ikkje svara at dei har meldt frå om alle avvika eit oppfølgingsspørsmål der dei blei bedt om å svare på kva som er årsaka/årsakene til at dei ikkje meldte alle dei opplevde informasjonstryggleiksavvika.<sup>31</sup> Fleire av respondentane svarer at det ikkje har vore system for å melde avvik i kommunen, og mange påpeiker vidare at det ikkje er kultur eller rutinar for å melde avvik. Nokre respondentar viser også til at dei fleire gonger hadde meldt om same type avvik (og dermed ikkje såg nytta av å melde frå enda ein gong) eller at avvik blei levert av kollega.

Respondentane som svara at dei meldte frå om «alle», «dei fleste», «nokre» eller «dei færreste» av avvika fekk spørsmål om avvika dei har meldt frå om har blitt følgt opp.<sup>32</sup> Om lag halvparten (52 prosent) svarer at avvika blei følgt opp, medan 16 prosent oppgjev at avvika delvis blei følgt opp. Litt over 13 prosent svara at avvika dei melde inn ikkje blei følgt opp og 19 prosent svarar «veit ikkje» på dette spørsmålet.

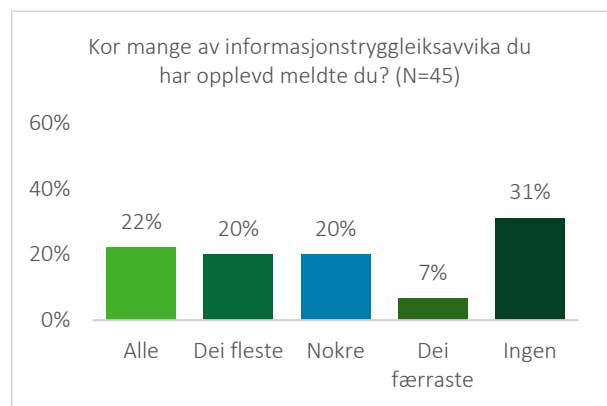
#### 4.6.2 Vurdering

Tysnes kommune har ved innføring av elektronisk avviksmeldesystem sikra oversikt over avvik som blir meldt knytt til personvern. Revisjonen vurderer samtidig at kommunen ikkje i tilstrekkeleg grad har etablert retningslinjer som sikrar tilfredsstillande rutinar for kven som har hovudansvar for å melde frå til Datatilsynet dersom det blir meldt om alvorlege brot på personopplysningstryggleiken, og det går heller ikkje fram kva som er frist for å melde slike avvik vidare til tilsynsmyndigheita. Revisjonen vil understreke at personvernforordninga er tydeleg på at den behandlingsansvarlege (dvs. rådmann) utan ugrunna opphald og seinast 72 timar etter å ha fått kjennskap til brot på personopplysningstryggleiken, skal melde brotet til Datatilsynet (jf. Artikkel 33). Datatilsynet peiker i si rettleiing på at den behandlingsansvarlege ikkje treng å melde frå om brot til Datatilsynet dersom brotet truleg ikkje vil medføre risiko for fysiske personar sine rettigheter og friheiter, men peiker vidare på at dersom behandlingsansvarleg er usikker på om unntaket er oppfylt bør melde frå til Datatilsynet for sikkerheits skuld.<sup>33</sup>

Undersøkinga viser at det er meldt avvik i desember 2022 om at helsepersonell frå både legekontor, helsestasjon og psykisk helseteneste har hatt tilgang til mapper med personsensitiv informasjon utan at dei har hatt tenestleg behov for dette. Dette skuldast at det blei oppretta ei mappe innan sikker sone, men likevel på eit område der tilsette frå fleire tenester hadde tilgang. Dette syner viktigeita av å gjennomføre kontrollar og å sikre at tilsette har tilstrekkeleg kompetanse knytt til handtering av personsensitiv informasjon.

Svara i spørjeundersøkinga tyder på at ikkje alle tilsette i kommunen veit at dei skal melde avvik knytt til informasjonstryggleik når dei opplever eller observerer slike tilfelle. Ein relativt stor del av respondentane som oppgjev at dei har opplevd slike avvik svarer at dei ikkje har meldt frå om dette. Kommunen si oversikt over registrerte avvik indikerer også at det er få avvik som blir meldt. Revisjonen vil peike på at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta.

Figur 5: Melding om opplevde informasjonstryggleiksavvik



<sup>30</sup> N=45

<sup>31</sup> N=27

<sup>32</sup> N=31

<sup>33</sup> Datatilsynet. Hvilke brudd skal meldes til Datatilsynet? Publisert 24.03.2023. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hvilke-brudd-skal-meldes-til-datatilsynet/>

## 5 Kompetanse blant tilsette

### 5.1 Problemstilling

I dette kapittelet vil vi svare på følgjande hovudproblemstilling med underproblemstillingar:

*I kva grad har dei tilsette i kommunen tilstrekkeleg kompetanse om informasjonstryggleik?*

Under dette:

- Er det etablert rutinar for å gje tilsette i kommunen opplæring i informasjonstryggleik?
- I kva grad har dei tilsette i kommunen kjennskap til ev. retningslinjer og rutinar for informasjonstryggleik, og i kva grad blir desse etterlevd?

### 5.2 Revisjonskriterier

Krav til kommunen når det gjeld kompetanse blant tilsette blir utleia frå kommunelova og eForvaltningsforskrifta.

Kommunen skal:

- skal ha internkontroll med administrasjonen si verksemd for å sikre etterleving av lover og forskrifter (kommunelova § 25-1).
- ha eit internkontrollsystem basert på anerkjende standardar for styringssystem for informasjonstryggleik (eForvaltningsforskrifta § 15).
- gjennomføre eigna tekniske og organisatoriske tiltak for å sikre og påvise at behandlinga av personopplysningar blir utført i samsvar med personvernforordning. Dei nemnte tiltaka skal gjennomgåast på nytt og skal oppdaterast ved behov (artikkel 24 i personvernforordninga)

Digitaliseringsdirektoratet tilrår at kommunen bør<sup>34</sup>:

- kartlegge behov – sette i gang på relevante område
- velje målgruppe: Når det er konkludert med at det er behov for opplæring, er det viktig å identifisere målgruppa for opplæringa.
- ta i bruk passande tiltak
- tenkje heilskapleg – sjå tiltak i samanheng (både opplæring innan informasjonstryggleik og anna opplæring i verksemda)
- måle effekten av tiltak
- gjennomføre jamlege øvingar på området, og evaluere øvinga i etterkant.

Sjå vedlegg 4 for utfyllande revisjonskriterium.

### 5.3 Rutinar for opplæring i informasjonstryggleik

#### 5.3.1 Datagrunnlag

I kommunen sin IKT strategi for 2022-2025 går det fram at eit av satsingsområda innan IKT er prosess, kvalitet og kompetanse. Under satsingsområdet kompetanse er det ei målsetting at kommunen mellom anna skal syte for kontinuerleg kompetanseutvikling av sine tilsette for å sikre ei effektiv og forsvarleg IKT-drift. Vidare går det fram av strategien at eit av kommunen sine strategiske grep knytt til personvern og informasjonstryggleik er å bevisstgjere og gi opplæring til dei tilsette. Opplæring blir omtala som svært viktig for å få fram gode haldningar, spreie kunnskap og auke forståinga for personvern og informasjonstryggleik. Det går vidare fram at kommunen skal sikre at dei tilsette har lett tilgang til retningslinjer, prosedyrar, rutinar og kurs.

---

<sup>34</sup> Digitaliseringsdirektoratet. Veileder i kompetanse- og kulturutvikling innen digital sikkerhet.

I Tysnes kommune si handbok i informasjonssikkerhet går det fram at leiarar har ansvar i samband med opplæring av dei tilsette i personvern og informasjonstryggleik. Dette inneber:

- grunnleggjande kompetanse i kontorstøtteverktøy
- å kunna følgja retningslinjer for kor informasjonen blir lagra, blir brukt og delt
- opplæring i aktuelle fagprogram og rutinar knytt til bruken av system
- kunnskap om innhaldet i informasjonsikkerhetshandboka

Det går vidare fram av handboka at superbrukarar/fagsystemansvarleg har hovudansvar for å gi opplæring til tilsette i fagsystema/IT-systema og forsvarleg handsaming av informasjon i systema.

Tysnes kommunen har vidare vedtatt eit introduksjonsprogram for nyttilsette<sup>35</sup>. Introduksjonsprogrammet er ei rutine ved tilsetjing som mellom anna inneheld ei sjekkliste som leiar og kontaktperson for den nyttilsette skal bruke for å sikre at den nyttilsette mottar viktig informasjon og opplæring. Nokre av punkta i sjekklista er at den nyttilsette skal få opplæring i dataprogram og sikkerheitsrutinar, retningslinjer for varsling av kritikkverdige forhold og avvik i løpet av dei første to vekene av tilsettinga. Gjennomgang av handbok i informasjonssikkerhet er ikkje spesifisert som del av punkta som skal gjennomgåast med nyttilsette. Introduksjonsprogrammet er utforma før kommunen etablerte handbok i informasjonssikkerhet og det går ikkje fram at introduksjonsprogrammet er oppdatert sidan 2017.

Kommunen har ikkje utarbeidd konkrete rutinar, verktøy eller hjelpemiddel for å sikre at tilsette får opplæring eller informasjon om informasjonstryggleik.

Det blir samtidig påpeikt i intervju at det blir gjennomført noko opplæring i personvern og informasjonstryggleik blant tilsette. Personvernombodet fortel i intervju at tilsette får tilsendt KS sitt KiNS-kurs i grunnleggjande informasjonstryggleik.<sup>36</sup> Kommunen har etter det revisjonen kjenner til, ikkje oversikt over kor mange tilsette som eventuelt har fått tilsendt eller gjennomført dette kurset.

Det blir også vist til at IT-leiar sender phishing-testar til tilsette, samt Nano-læring (gjennom Junglemap) for å sikre informasjon om datatryggleik. Det går fram at desse e-postane ikkje blir sendt til tilsette i skular og barnehagar, og det blir peikt på at årsaka til dette er at dei tilsette innanfor denne sektoren, som nemnt under avsnitt 3.5.1 om tilgangsstyring, ikkje høyrer til same domene som resten av dei tilsette i kommunen. Dette vil seie at om lag ein av tre tilsette i kommunen ikkje får desse e-postane.<sup>37</sup> I intervju blir det vist til at det er lenge sidan det er sendt ut nanolæring frå IT-leiar. Det blir påpeikt at nanolæringa ikkje ligg tilgjengeleg for tilsette på intranett eller liknande. Revisjonen har ikkje fått døme på tilsendte phishing-testar eller nanolæring sendt frå IT-leiar, men har fått tilgang til ei rekkje e-postar frå IT-leiar som i hovudsak omhandlar døme på mottatt phishing e-post og åtvaring mot å trykke på lenkjer mv. i denne typen e-postar.

Det blir i intervju vist til at kommunen vurderer å ta i bruk e-læringsmodulen KS Læring for å etablere opplæringsmodular og kurs innan mellom anna informasjonstryggleik på kommunen sine intranettsider. Personvernombodet peiker vidare på at det er ønskeleg å legge kommunen si handbok for informasjonssikkerhet inn i e-læringsformat for dei tilsette i kommunen.

Rådmannen peiker på at hovudutfordringa når det gjeld informasjonstryggleik og personvern i Tysnes kommune er å få på plass ei grunnleggjande forståing av GDPR, personvern og informasjonstryggleik hos dei tilsette. Mellom anna fortel rådmannen at det er behov for språklege avklaringar og «avkodifisering» av omgrep innanfor fagområdet. Det går også fram av årsmelding frå 2021 at ei av dei tre største utfordringane innan IT er brukaropplæring av tilsette.<sup>38</sup>

### 5.3.2 Vurdering

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg rutinar for å sikre at tilsette får opplæring i informasjonstryggleik. Undersøkinga viser at kommunen har etablert nokre målsettingar om at opplæring knytt til informasjonstryggleik er viktig, og det går vidare fram av handbok i informasjonssikkerhet at leiarar og superbrukarar/fagsystemansvarlege har eit ansvar for å sikre at tilsette får denne opplæringa. Det går samtidig

<sup>35</sup> Tysnes kommune. *Introduksjonsprogram for nyttilsette*. Vedtatt i kommunestyret 12.12.2017.

<sup>36</sup> Foreningen kommunal informasjonssikkerhet – KiNS. KiNS e-læring. Kurset omfattar 100 læringspunkt som skal bidra til å auke kunnskap om korleis personvern og informasjonstryggleik kan varetakast for brukarar, innbyggjarar og tilsette

<sup>37</sup> Det er om lag 120 tilsette i skular og barnehagar og til saman om lag 350 tilsette i heile kommunen.

<sup>38</sup> Tysnes kommune. *Årsmelding 2021*. 31.03.2021.



fram at kommunen ikkje har etablert system eller rutinar som sikrar tilsette får denne opplæringa. Kommunen har heller ikkje oversikt over kva opplæring eller kurs tilsette eventuelt har fått på dette området. Revisjonen vil påpeike at dette ikkje er i samsvar med krav og anbefalingar om kommunen sitt ansvar for å sikre tilstrekkeleg informasjonstryggleikskompetanse blant dei tilsette gjennom opplæringstiltak. Dette gjer at det er høgare sannsyn for at dei tilsette ikkje har tilstrekkeleg kompetanse innan informasjonstryggleik, noko som igjen aukar risiko for brot på regelverket som gjeld for behandling av personopplysningar og for informasjonstryggleiken generelt.

Revisjonen merkar seg at kommunen kjenner til behovet for opplæring av tilsette, og at det mellom anna blir vurdert å ta i bruk e-læring for å etablere opplæringsmodular og kurs innan mellom anna informasjonstryggleik på kommunen sine intranettsider.

## 5.4 Kjennskap til og etterleving av retningslinjer og rutinar for informasjonstryggleik

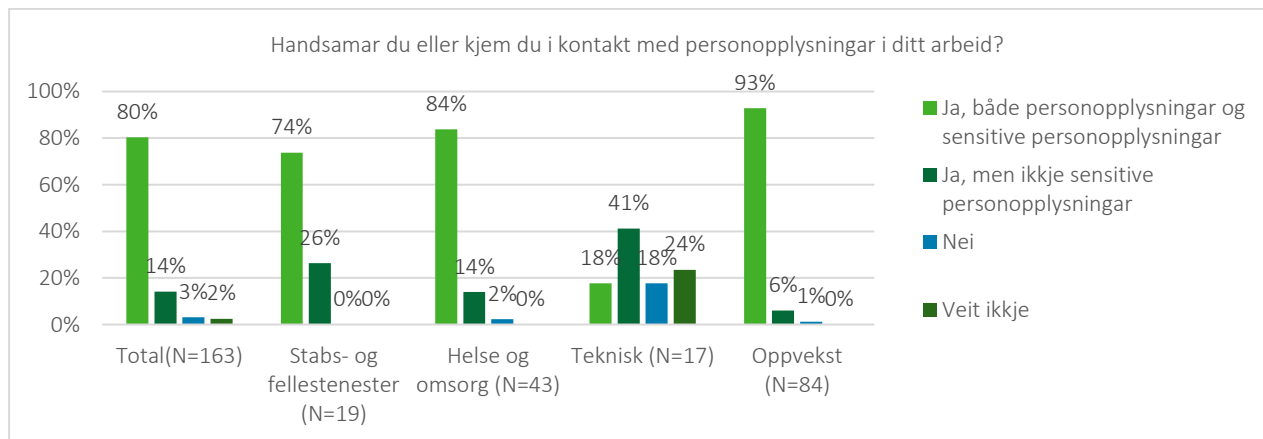
### 5.4.1 Datagrunnlag

#### Kjennskap til retningslinjer og rutinar for informasjonstryggleik

Innleiingsvis i spørjeundersøkinga fekk respondentane spørsmål om dei handsamar eller kjem i kontakt med personopplysningar i sitt arbeid.<sup>39</sup> Som vist i figuren under svarar totalt 80 prosent av dei 163 respondentane som deltok i spørjeundersøkinga at dei handsamar eller kjem i kontakt med både personopplysningar og sensitive opplysningar, og 14 prosent svarar at dei berre handsamar eller kjem i kontakt med personopplysningar og ikkje sensitive personopplysningar.

93 prosent av respondentane frå oppvekst, 84 prosent frå helse og omsorg og 74 prosent frå stabs- og fellestenester svarar at dei handsamar eller kjem i kontakt med både personopplysningar og sensitive personopplysningar i sitt arbeid. 41 prosent av respondentane frå teknisk sektor svarar at dei handsamar personopplysningar, men ikkje sensitive personopplysningar, medan 18 prosent frå same sektor viser til at dei handsamar eller kjem i kontakt med begge typar personopplysningar. 24 prosent av respondentane frå teknisk sektor svarar «veit ikkje» på dette spørsmålet.

Figur 6: Del respondentar som handsamar personopplysningar og sensitive personopplysningar gjennom sitt arbeid



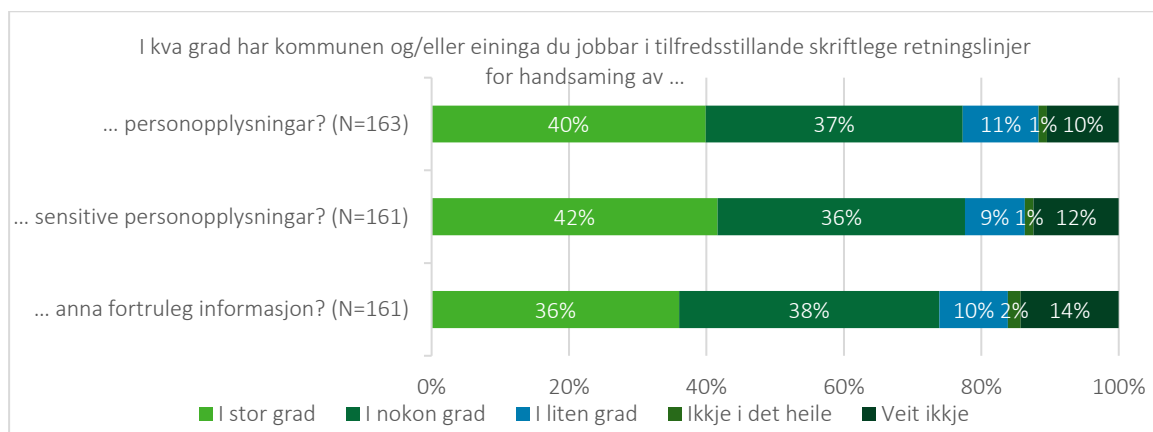
Respondentane blei også stilt spørsmål om dei handsamar anna *fortruleg informasjon*.<sup>40</sup> Her svara om lag 80 prosent *ja* og 11 prosent *nei*, medan 9 prosent svarar «veit ikkje». Fordelinga mellom sektorane er på dette spørsmålet relativt likt som svara framstilt i figuren over.

Respondentane blei bedt om å svare på i kva grad kommunen og/eller eininga der dei jobbar har tilfredsstillande skriftlege retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og anna fortruleg informasjon. Som framstilt i figuren under svarar om lag to av fem respondentar at det «i stor grad» er tilfredsstillande retningslinjer for handsaming av alle dei tre typane informasjon, medan om lag to av fem svarer at dette «i nokon grad» er tilfredsstillande. Om lag 10 prosent svarer «i liten grad» på desse tre spørsmåla, medan mellom 10 og 14 prosent svarar «veit ikkje».

<sup>39</sup> I spørjeundersøkinga var det lagt inn ei forklaring av omgrepa personopplysningar og sensitive personopplysningar i samband med dette spørsmålet.

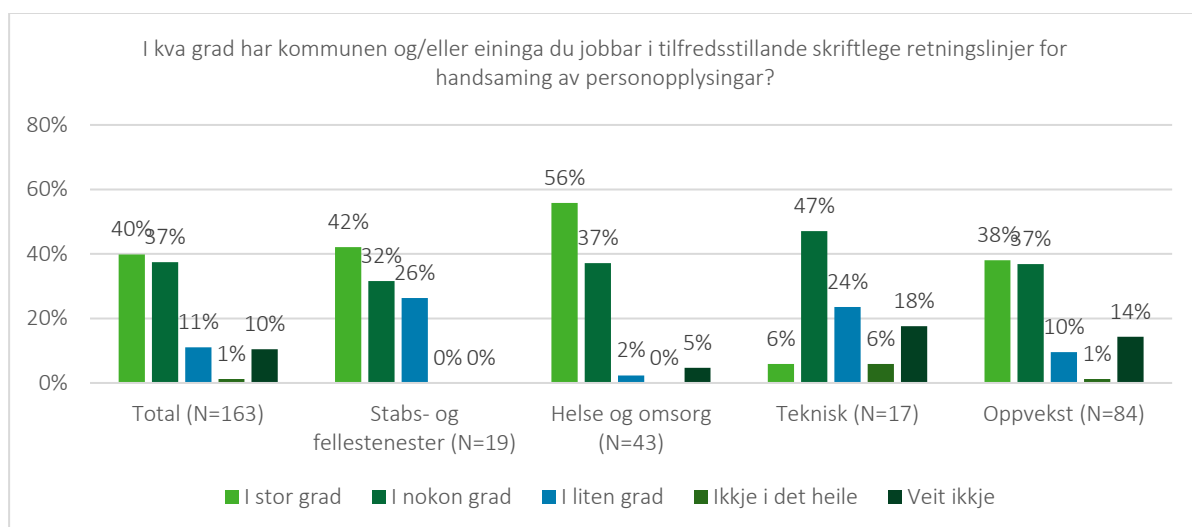
<sup>40</sup> I spørjeundersøkinga var det lagt inn ei forklaring på kva som er meint med fortruleg informasjon. Sjå elles ordliste på side 3 i rapporten

Figur 7: Har kommunen og/eller eininga tilfredsstillande skriftlege retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og anna fortruleg informasjon?



Nærare analyse viser at det er skilnader på svar frå respondentane fordelt på sektorar i kommunen når det gjeld spørsmålet om tilfredsstillande skriftlege retningslinjer som framstilt i figuren over. Over halvparten av respondentane frå helse og omsorg (56 prosent) svarar at det «i stor grad» er tilfredsstillande skriftlege retningslinjer for handsaming av personopplysningar, medan 38 prosent av respondentane frå oppvekstsektoren og 6 prosent av respondentane frå teknisk sektor svarer det same. 26 prosent av respondentane frå stabs- og fellestenester og 24 prosent frå teknisk sektor svarer at det «i liten grad» er tilfredsstillande skriftlege retningslinjer på dette området, medan 10 prosent frå oppvekstsektoren svarer det same.

Figur 8: Tilfredsstillande retningslinjer for handsaming av personopplysningar delt på sektorane i kommunen



Svar frå respondentane per sektor på spørsmålet framstilt i figuren over er i hovudsak likt fordelt som i spørsmåla om retningslinjer for handsaming av sensitive opplysningar og anna fortruleg informasjon.

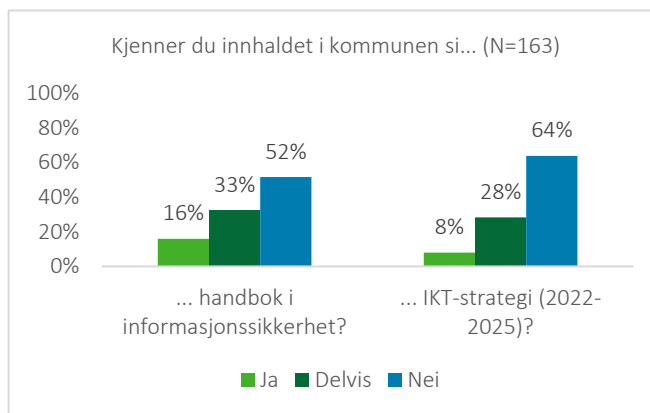
Respondentane som svarta at kommunen og/eller eininga «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer på områda som nemnt over, fekk eit oppfølgingsspørsmål om dei veit kvar dei finn rutinar og retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon som gjeld kommunen og/eller eininga.<sup>41</sup> På dette spørsmålet svarta total 70 prosent «ja» og 30 prosent «nei». Også på dette spørsmålet er det noko skilnad på svar frå respondentar frå dei ulike sektorane. Medan høvesvis 87 prosent og 85 prosent av respondentane frå stabs- og fellestenestene og helse- og omsorg svarar «ja» på dette spørsmålet, er det 62 prosent frå oppvekst og 40 prosent frå teknisk som svarer det same.

Som nemnt tidlegare i rapporten har Tysnes kommune i 2022 etablert *handbok i informasjonssikkerhet* og *IKT-strategi for Tysnes kommune 2022-2025*. Det blir vist til at dette er kommunen sine styrande dokument i arbeidet med informasjonstryggleik.

<sup>41</sup> N=130

I spørjeundersøkinga fekk respondentane spørsmål om dei kjenner innhaldet i desse to dokumenta. Som framstilt i figur 9 svarar over halvparten av respondentane (52 prosent) at dei ikkje kjenner til innhaldet i handboka og litt under to av tre respondentar (64 prosent) svarer at dei ikkje kjenner til innhaldet i IKT-strategien til kommunen.

Figur 9: Kjennskap til innhald i styrande dokument om informasjonstryggleik og personvern

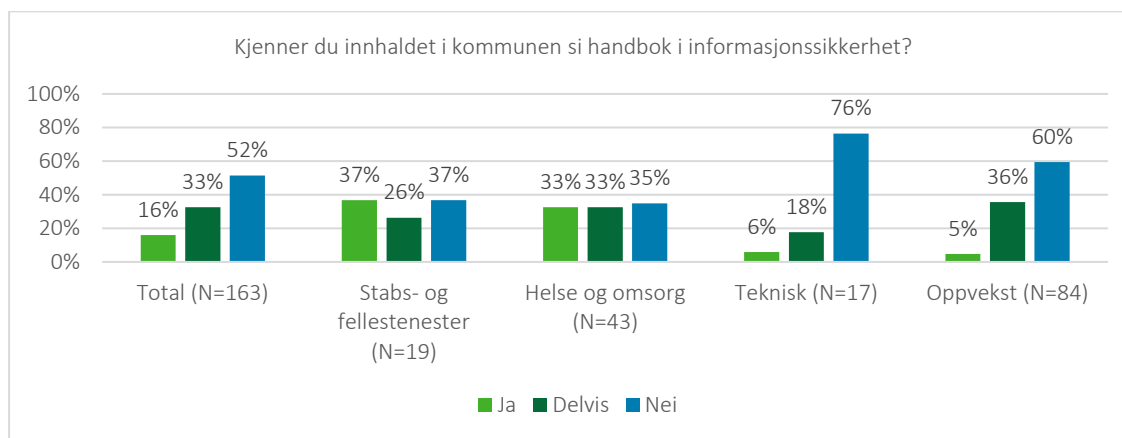


Ved nærare analyse går det fram at det er skilnad på svara frå respondentane på dette spørsmålet på bakgrunn av både kva sektor dei jobbar innan og om dei er tilsett med leiaransvar eller ikkje. Medan om lag ein av tre (34 prosent) tilsette med leiaransvar svarar at dei *ikkje* kjenner til innhaldet i handbok i informasjonssikkerhet, er det over halvparten (56 prosent) av tilsette utan leiaransvar som svarer det same. 31 prosent av leiarane svarar «ja» på spørsmålet om dei kjenner innhaldet i handboka og 12 prosent av tilsette svarar det same.

Når det gjeld IKT-strategien svarar 69 prosent av tilsette utan leiaransvar at dei *ikkje* kjenner innhaldet i denne, medan 46 prosent av leiarane svarer det same. Berre 5 prosent av tilsette utan leiaransvar svarer at dei kjenner innhaldet i strategien, medan 17 prosent av leiarane oppgjev at dei kjenner dette innhaldet.

Om lag tre av fire respondentar frå teknisk sektor (76 prosent) svarar at dei ikkje kjenner til innhaldet i nokre av dei to dokumenta. Innan oppvekstsektoren svarar 60 prosent at dei ikkje kjenner til innhaldet i handboka og 74 prosent svarar at dei ikkje kjenner til innhaldet i IKT-strategien. I tabellen under er fordelinga per sektor når det gjeld kjennskap til handbok i informasjonssikkerhet.

Figur 10: Kjennskap til handbok i informasjonssikkerhet delt på sektortilhørslse



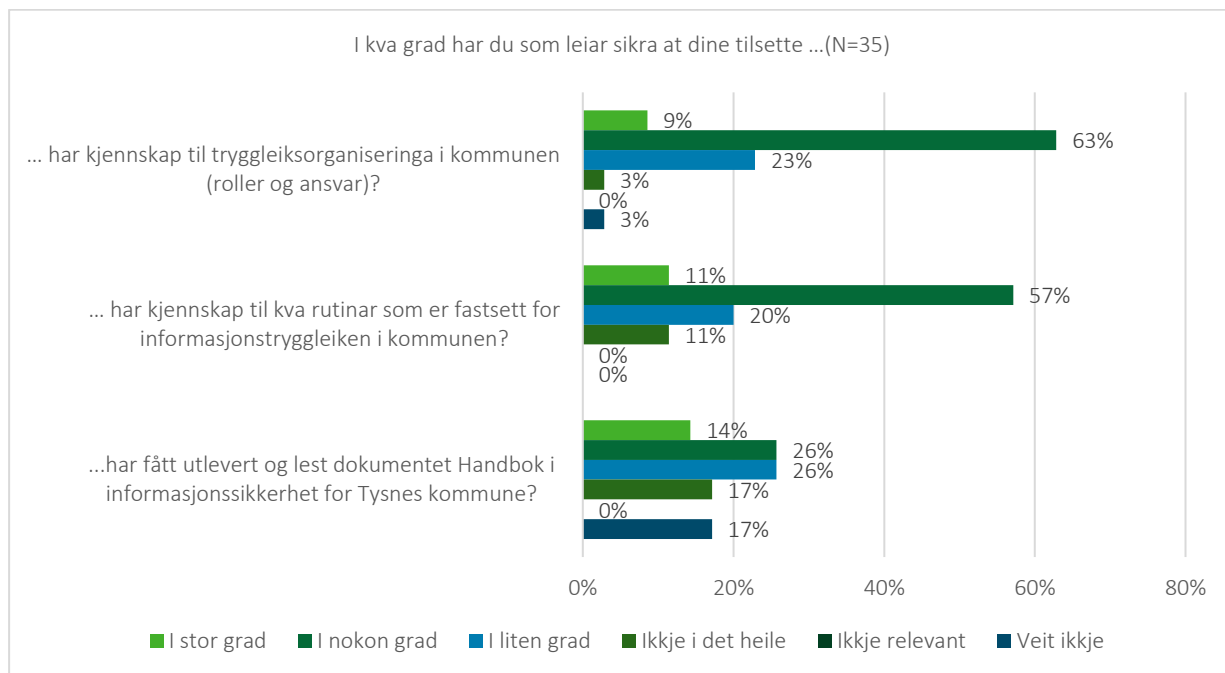
I spørjeundersøkinga svarar 17 prosent<sup>42</sup> av respondentane med leiaransvar at dei «ikkje i det heile» har sikra at dei tilsette har fått utlevert og lest handbok i informasjonssikkerhet, medan 26 prosent svarar at dei høvesvis «i liten grad» eller «i nokon grad» har sikra dette. 14 prosent av leiarane svarar at dei «i stor grad» har sikra dette.

Respondentane med leiaransvar fekk også spørsmål om i kva grad dei har sikra at dei tilsette kjenner til tryggleiksorganiseringa i kommunen og rutinar som er fastsett for informasjonstryggleiken. Som vist i figuren under svarar over halvparten av leiarane at dei «i nokon grad» har sikra at tilsette har kjennskap til rollar og ansvar knytt til informasjonstryggleik i kommunen og kva rutinar som gjeld for å sikre informasjonstryggleiken. Om lag ein av fem (høvesvis 23 og 20 prosent) svarar at dei «i liten grad» har sikra at dei tilsette har kjennskap til dette, medan 11 prosent av respondentane<sup>43</sup> svarer at dei «ikkje i det heile» har sikra at deira tilsette har kjennskap til kva rutinar som er fastsett for informasjonstryggleiken i kommunen.

<sup>42</sup> 5 respondentar

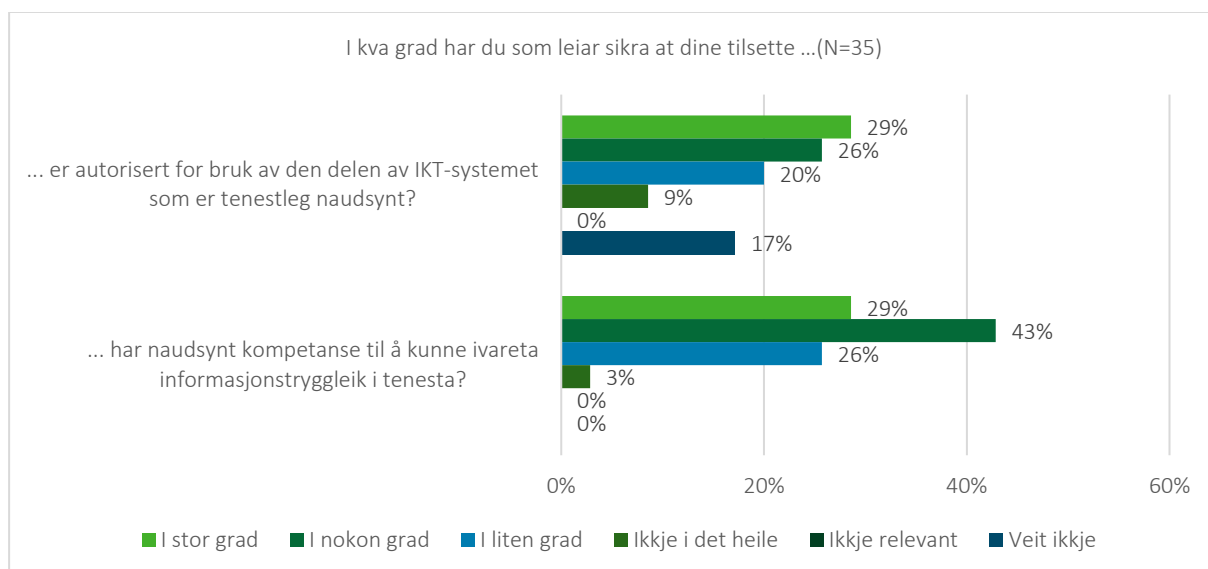
<sup>43</sup> 4 respondentar

Figur 11: Informasjon frå leiar om retningslinjer, tryggleiksorganisering og informasjonstryggleiksrutinar



Leiarane blei vidare spurt om dei har sikra at deira tilsette har nødvendig kompetanse til å kunne ivareta informasjonstryggleik i tenesta.<sup>44</sup> 29 prosent svara at dei «i stor grad» har sikra dette, medan om lag ein av fire svarar at dei «i liten grad» har sikra dette. 43 prosent svarar «i nokon grad» på dette spørsmålet. Vidare svarar 17 prosent «veit ikkje» på spørsmålet om det har sikra at deira tilsette er autorisert for bruk av den delen av IKT-systemet som er tenestleg nødvendig, medan 9 prosent svarar «ikkje i det heile» og 20 prosent oppgjev at dei «i liten grad» har sikra dette.

Figur 12: Nødvendig autorisering og kompetanse for å ivareta informasjonstryggleik



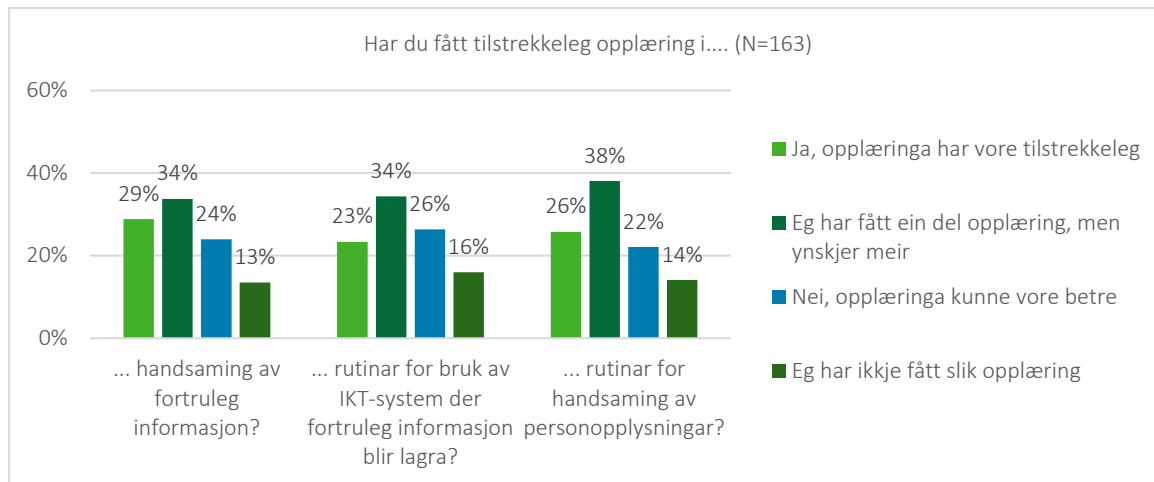
Alle respondentane fekk vidare spørsmål om dei har fått tilstrekkeleg opplæring i 1) handsaming av fortruleg informasjon, 2) rutinar for bruk av IKT-system der fortruleg informasjon blir lagra og 3) rutinar for handsaming av personopplysningar. Som framstilt i figuren under svarar om lag ein av fire at opplæringa innan desse tre områda kunne ha vore betre<sup>45</sup> medan rundt 15 prosent av respondentane svarar at dei ikkje har fått slik opplæring. Om lag ein av tre respondentar viser til at dei har fått ein del opplæring innan handsaming av fortrulege opplysningar og rutinar for bruk av IKT-system der fortruleg informasjon blir lagra, men at dei ynskjer meir opplæring. Når det

<sup>44</sup> N=35

<sup>45</sup> høvesvis 24 %, 26 % og 22 %

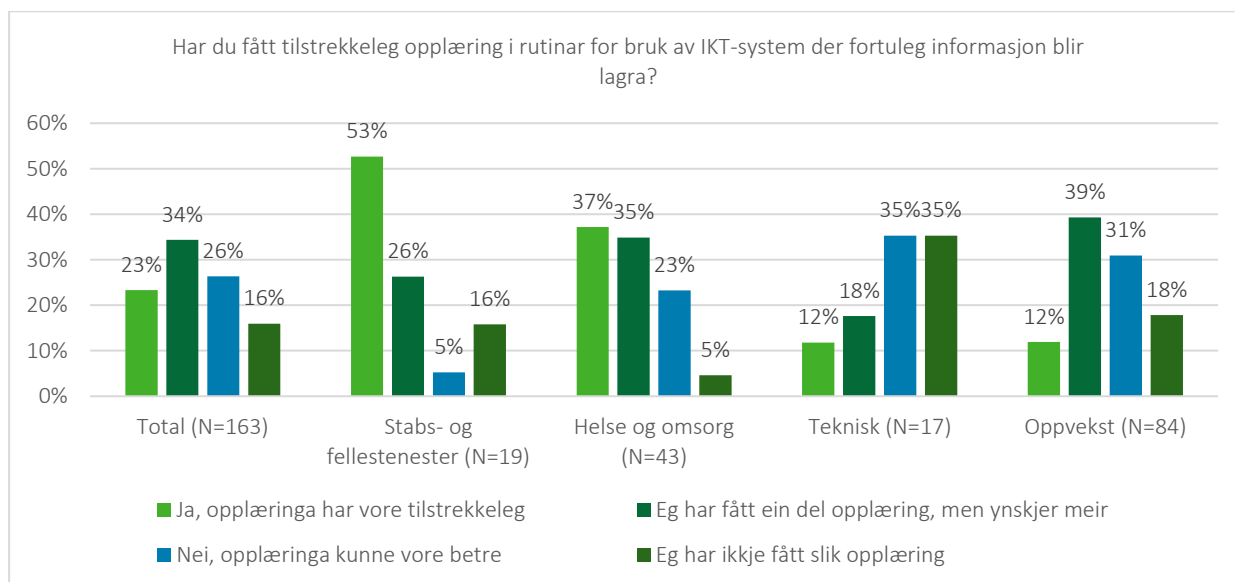
gjeld opplæring i rutinar for handsaming av personopplysningar, så svarar 38 prosent av respondentane at dei har fått ein del opplæring men ønsker meir.

Figur 13: Tilstreккеleg opplæring



Når vi fordeler svar på frå respondentane på kva sektor i kommunen dei er tilsett i (helse og omsorg, teknisk, oppvekst og stabs- og fellestenester), så ser vi at det er skilnad på kva tilsette innan dei fire sektorane svarar på spørsmåla om tilstrekkeleg opplæring. Tabellen under viser fordelinga på sektorane for spørsmålet «har du fått tilstrekkeleg opplæring i rutinar for bruk av IKT-system der fortruleg informasjon blir lagra?». Som framstilt er det lang færre innan teknisk sektor og oppvekstsektoren (12 prosent) som svarer at opplæringa har vore tilstrekkeleg enn i dei to andre sektorane, der høvesvis 53 prosent og 37 prosent svarer at opplæringa har vore tilstrekkeleg. 35 prosent av respondentane frå teknisk, 18 prosent av respondentane frå oppvekst og 16 prosent av respondentane frå stabs- og fellestenester svarer at dei ikkje har fått slik opplæring, medan 5 prosent frå helse og omsorg svarer det same. Svarfordelinga per sektor er relativt lik også for dei to andre spørsmåla om opplæring vist i figur 13 over.

Figur 14: Svar på tilstrekkeleg opplæring fordelt på sektorar i kommunen



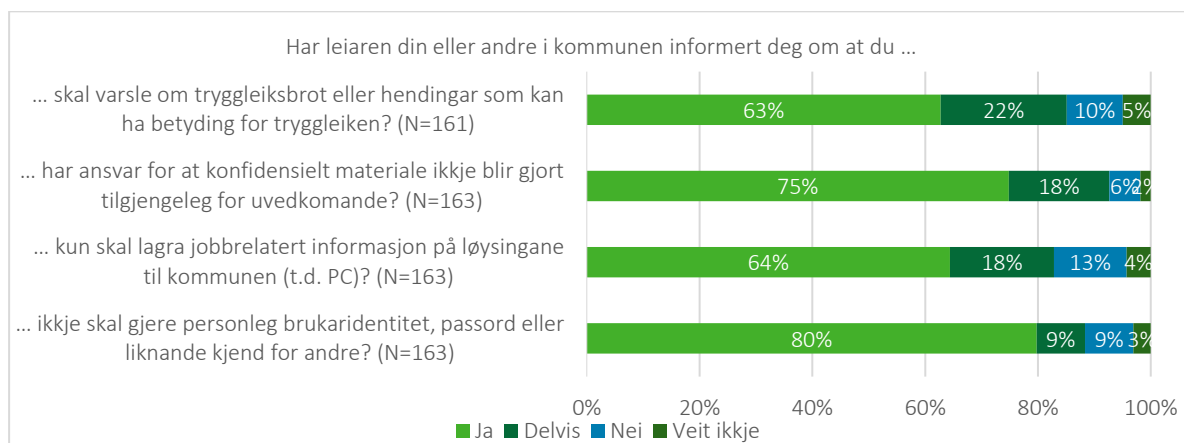
Dei respondentane som *ikkje* svarta «ja, opplæringa har vore tilstrekkeleg» på dei tre spørsmåla om opplæring framstilt i figur 13 over, fekk eit ope oppfølgingsspørsmål der dei fekk svare på kva opplæring knytt til informasjonstryggleik og/eller bruk av IKT-system dei saknar. 57 av respondentane har svart på dette spørsmålet og om lag halvparten av dei peiker på at dei har behov for generell opplæring, og fleire av dei påpeiker på at dei ikkje har fått noko opplæring knytt til dette i kommunen. 7 respondentar påpeiker at det er behov for retningslinjer og rutinar innan dette området og/eller ein repetisjon av kvar ein finn retningslinjer for informasjonstryggleik i kommunen. Fleire respondentantar etterlyser konkret opplæring i korleis ein skal handsame personopplysningar

sikkert i systema dei brukar i arbeidet, og nokre påpeikar at det er behov for opplæring også i informasjonstryggleik utanfor elektroniske system (sikker lagring av papirdokument, brevpost mv.)

Respondentane blei i spørjeundersøkinga bedt om å svare på i kva grad deira næraste leiar har framheva viktigheita av informasjonstryggleik. Totalt svarar 43 prosent at deira næraste leiar «i stor grad» har framheva dette, medan 13 prosent svarer «i liten grad» og 5 prosent svarer «ikkje i det heile». 40 prosent oppgjev at deira næraste leiar «i nokon grad» har framheva viktigheita av informasjonstryggleik.

Det blei vidare stilt spørsmål om leiar eller andre i kommunen har informert om nokre spesifiserte informasjonstryggleikstiltak. Totalt svarar 80 prosent at dei har fått informasjon frå sin leiar eller andre i kommunen om å ikkje dele passord, brukaridentitet og liknande, 75 prosent svarer at dei har fått informasjon om at dei har ansvar for å sikre at konfidensielt materiale ikkje blir gjort tilgjengeleg for uvedkomande. 63 prosent har fått informasjon om å varsle om tryggleiksbrot og 64 prosent svarer at dei har fått informasjon om at dei kun skal lagre jobbrelatert informasjon på kommunen sine PC-ar og liknande. Samtidig er det 22 prosent som viser til at dei «delvis» har fått informasjon om å varsle om tryggleiksbrot, og 10 prosent som svarer at dei ikkje har fått denne informasjonen. Det er vidare 18 prosent av respondentane som svarar «delvis» og 13 prosent som svarar «nei» på spørsmålet om leiar har formidla informasjon om at ein berre skal lagre jobbrelatert informasjon på kommunen sine PC-ar. Det er vidare 9 prosent som svarer at dei ikkje har fått informasjon om å ikkje dele brukaridentitet, passord og liknande.

Figur 15: Informasjon om ulike informasjonstryggleikstiltak



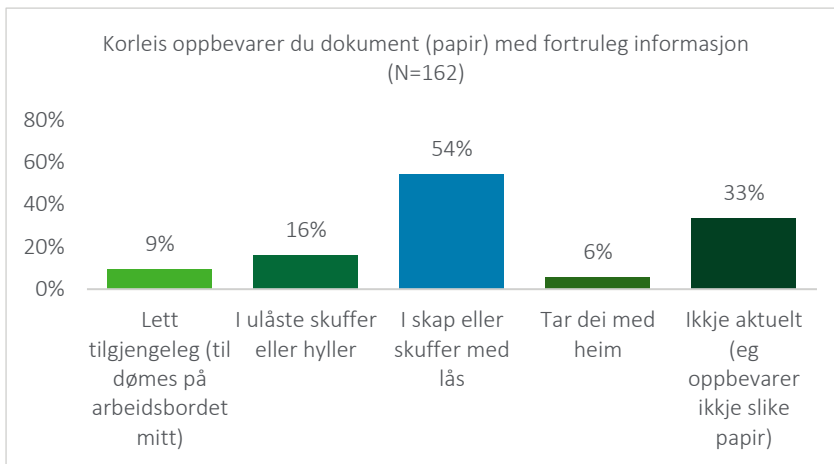
### Etterleving av retningslinjer og rutinar for informasjonstryggleik

I *handbok i informasjonssikkerhet* er tilgang og brukarkontroll et eige punkt for alle tilsette og for leiarar. For tilsette er det skildra fleire tiltak som skal sikre informasjonstryggleik. Dette inneber mellom anna policy for passord, underteikning av teiepliktsskjema, tilgang til IT-system og at dei tilsette er plikta til å låse teknisk utstyr som PC, nettbrett og mobiltelefon når dei forlèt dei.

Respondentane fekk spørsmål om dei har underteikna kommunen si erklæring om teieplikt. Totalt svarar 86 prosent av respondentane «ja» på dette spørsmålet, 6 prosent svarar «nei» og 8 prosent svarar «veit ikkje».

Respondentane i spørjeundersøking blei også stilt ulike spørsmål knytt til eige og andre tilsette si etterleving av retningslinjer og rutinar for informasjonstryggleik. Respondentane blei mellom anna bedt om å svare på korleis dei oppbevarer dokument med fortruleg informasjon. Som det går fram av figuren under, oppgjev over halvparten av respondentane at dei oppbevarer dokument med fortruleg informasjon i skap eller skuffer med lås. Samtidig er det ni prosent som svarar at dei oppbevarer dokument med fortruleg informasjon lett tilgjengeleg, 16 prosent svarar at slike dokument blir oppbevart i ulåste skuffer eller hyller og 6 prosent viser til at dei tar med dokument med fortruleg informasjon heim.

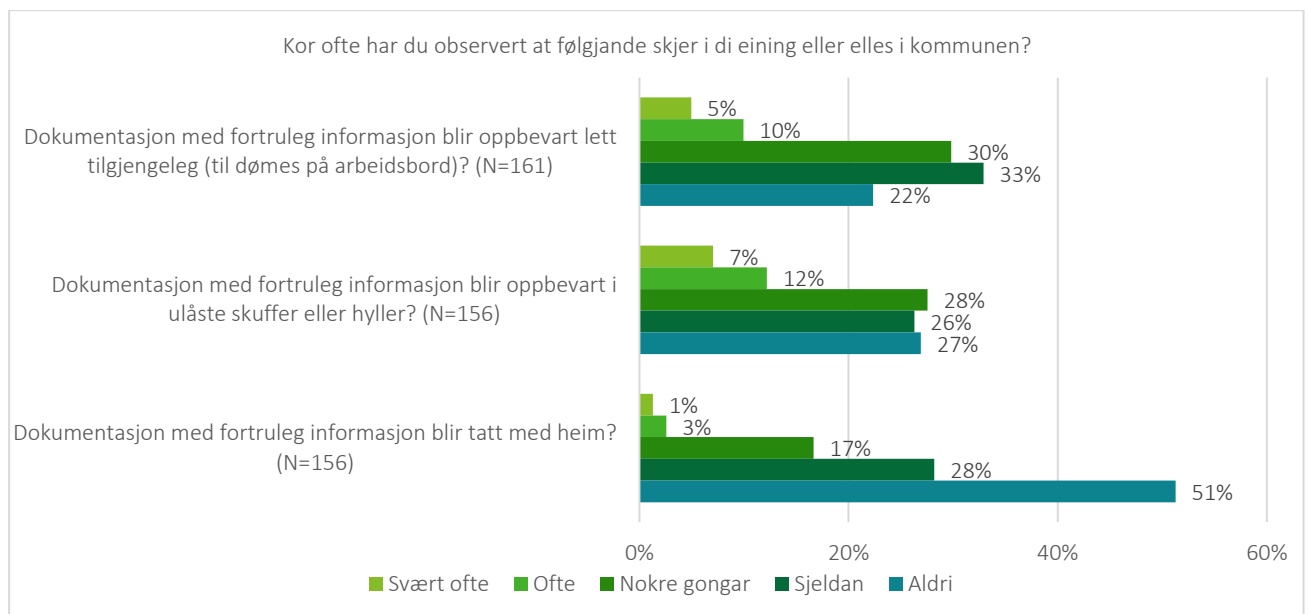
Figur 16: Oppbevaring av dokument med fortruleg informasjon



Som vist i figur 17 blei respondentane mellom anna også spurt om kor ofte dei observerer at dokumentasjon blir oppbevart lett tilgjengeleg eller i ulåste skuffer eller hyller og kor ofte dei observerer at slik dokumentasjon blir tatt med heim. Totalt svarar 10 prosent av respondentane at dei «ofte» observerer at dokumentasjon blir oppbevart lett tilgjengeleg, medan 5 prosent svarer at dei observerer dette «svært ofte».

30 prosent oppgjev å observerer dette «nokre gongar». Det er vidare 12 prosent av respondentane som viser til at dei «ofte» observerer at dokumentasjon med fortruleg informasjon blir oppbevart i ulåste skap eller hyller. 28 prosent svarer at dei ser dette «nokre gonger» og 7 prosent svarer at dei «ofte» observerer dette. Det er færre respondentar som observerer at dokumentasjon med fortruleg informasjon blir tatt med heim; her svarar over halvparten (51 prosent) at dei «aldri» observerer dette, medan 17 prosent oppgjev at dette skjer «nokre gonger», og 3 prosent peiker på at dette skjer «ofte».

Figur 17: Observasjon av informasjonstryggleiksbrøt



Respondentane fekk vidare spørsmål om kor ofte dei observerer at fortruleg informasjon frå møterom eller liknande (dokument, informasjon på tavle/flipover, osv.) blir fjerna før romma blir forlate.<sup>46</sup> Her svarar over halvparten av respondentane at dette «svært ofte» blir fjerna, medan 16 prosent svarer at slik informasjon «aldri» blir fjerna. 20 prosent svarar at denne typen informasjon «ofte» blir fjerna og 7 prosent svarar «sjeldan» på dette spørsmålet. Det er flest respondentar frå stabs- og fellestenester og teknisk sektor som svarar at denne typen informasjon «aldri» blir fjerna (høvesvis 33 prosent og 38 prosent).

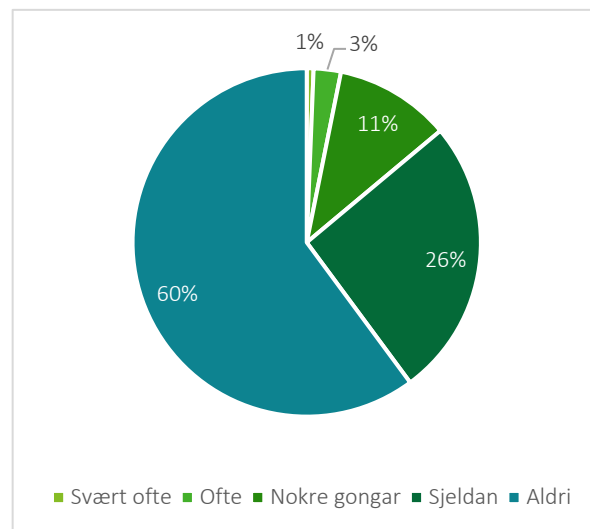
<sup>46</sup> N=154

I spørjeundersøkinga var det også spørsmål om kor ofte ein observerer at brukarnamn og passord blir gitt til andre, som til dømes IT-leiar. På dette spørsmålet svarar totalt 60 prosent at dei «aldri» observerer dette, medan 26 prosent oppgjev at dei «sjeldan» erfarer dette, og 11 prosent peiker på at dette «nokre gonger» førekjem. 3 prosent svarer at dei «ofte» observerer at brukarnamn og passord blir delt.

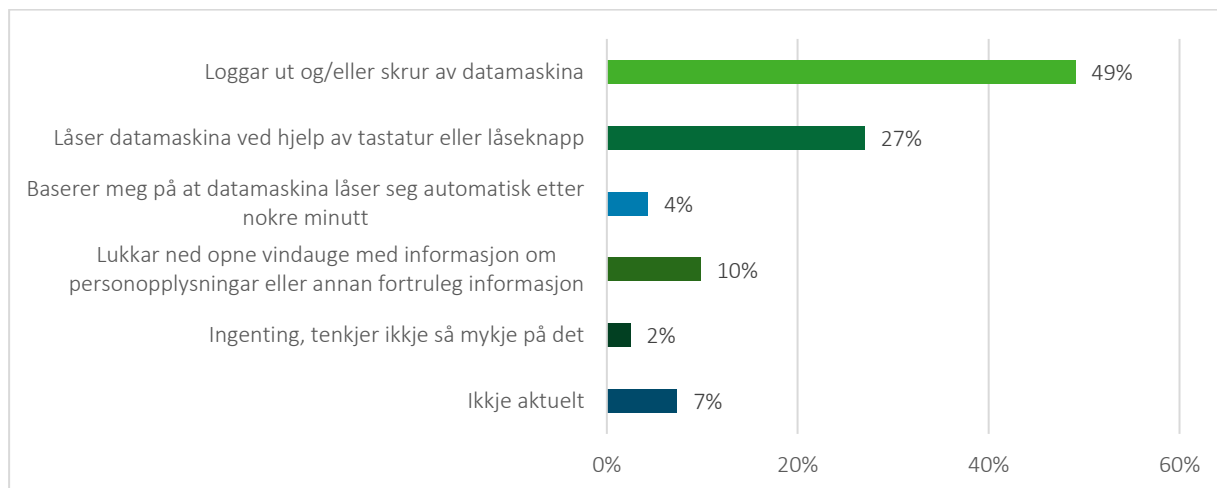
Respondentane blei også spurt om eigne vanar på dette området. Hovuddelen av respondentane svarar «nei» på spørsmålet om dei nokon gong har lånt ut brukarnamn og passord til andre (88 prosent), men 12 prosent svarar at dei har gjort dette. 7 prosent av dei som svarar at dei har lånt ut brukarnamn og passord svarar at dei har lånt dette ut til IT-leiar eller tilsvarande.

Respondentane blei vidare spurt om kva dei vanlegvis gjer når dei i løpet av arbeidsdagen går frå PC-en dei nyttar. Som framstilt i figuren under oppgjev halvparten av respondentane at dei i desse tilfella loggar ut eller skrur av PC-en, og over ein av fire svarar at dei låser datamaskina ved hjelp av tastatur eller låsetast. 4 prosent svarar at dei baserer seg på at PC automatisk låser seg etter nokre minutt og 2 prosent svarer at dei ikkje gjer noko

Figur 18: Kor ofte har du observert at brukarnamn og passord blir gitt til andre, som t.d. IT-leiar? (N=158)



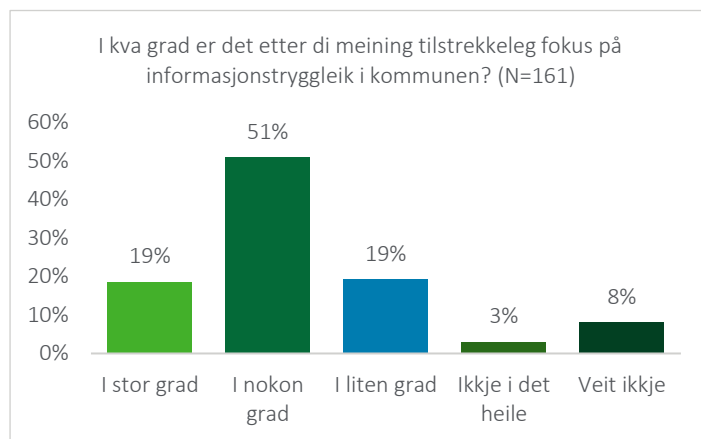
Figur 19: Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du nyttar? (N=163)



Avslutningsvis blei respondentane stilt spørsmål om i kva grad dei opplever at det er tilstrekkeleg fokus på informasjonstryggleik i kommunen. Som vist i figur 20 svara om lag halvparten av respondentane (51 prosent) at det «i nokon grad» er tilstrekkeleg fokus på informasjonstryggleik i kommunen. Om lag ein av fem respondentar (19 prosent) svarar at det «i liten grad» er tilstrekkeleg fokus på dette området, medan 3 prosent oppgjev at det «ikkje i det heile» er tilstrekkeleg fokus på informasjonstryggleik i kommunen.



Figur 20: Fokus på informasjonstryggleik i Tysnes kommune



Respondentane fekk vidare eit opent spørsmål der dei mellom anna kunne komme med innspel til område knytt til informasjonstryggleik eller handsaming av personopplysningar der kommunen har betringspotensiale. Mange av respondentane som har lagt inn kommentar her, peiker på at det er behov for meir opplæring, informasjon og påminningar om korleis ein skal sikre informasjonstryggleik og personvern i kommunen. Fleire peiker også konkret på at det er behov for å sikre større medvit om teieplikta blant tilsette.

Det er også ein del som peiker på at det må leggjast betre til rette for at tilsette kan jobbe godt med å sikre informasjonstryggleik. Fleire peiker her konkret på moglegheit for å låse inn dokument med sensitiv informasjon, samt at det er ei utfordring at fleire område i kommunen deler kopimaskin og at det her ofte kan ligge dokumentasjon som ikkje er henta og som ikkje burde sjåast av uvedkomande.

#### 5.4.2 Vurdering

Basert på funna i spørjeundersøkinga, vurderer revisjonen at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Til dømes svarar om lag halvparten av alle respondentane, og om lag ein av tre respondentar med leiaransvar, at dei *ikkje* kjenner innhaldet i kommunen si handbok i informasjonssikkerhet. Svar i spørjeundersøkinga indikerer vidare at det relativt store skilnadar mellom sektorane i kommunen når det gjeld kjennskap til styrande dokument for informasjonstryggleik. Til dømes går det fram at 93 prosent av respondentane frå oppvekstsektoren oppgjev å handsame både personopplysningar og sensitive personopplysningar, men 60 prosent av respondentane frå denne sektoren kjenner ikkje til innhaldet i kommunen si handbok i informasjonstryggleik. Det er vidare 14 prosent av respondentane frå oppvekstsektoren som ikkje veit om kommunen eller eininga har tilstrekkeleg skriftlege retningslinjer for handsaming av personopplysningar og 10 prosent svarar at det «i liten grad» er tilfredsstillande retningslinjer for dette. Vidare svarar 30 prosent av respondentane som oppgjev at kommunen og/eller eininga «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer for handsaming av personopplysningar, at dei ikkje kjenner til kvar dei finn desse retningslinjene og rutinane. Revisjonen vil understreke at kommunen etter personvernforordninga er forplikta til å sette i verk eigna tiltak, både organisatoriske og tekniske, for å sikre og påvise at personopplysningar blir handsama i samsvar med krav til dette i regelverket (personvernforordninga artikkel 24). Som ein del av dette bør kommunen mellom anna sikre at kommunen sine styrande dokument for informasjonstryggleik er tilgjengeleg og kjend for dei tilsette i kommunen.

Revisjonen vurderer vidare at kommunen ikkje i tilstrekkeleg grad etterlever retningslinjer og rutinar for informasjonstryggleik. Undersøkinga indikerer at dokument med fortruleg informasjon ikkje alltid blir lagra på ein sikker måte og/eller blir oppbevart slik at uvedkomande kan få innsyn. Undersøkinga viser også at 16 prosent av respondentane ikkje følgjer ein praksis for avlogging av PC i samsvar med prinsipp om god informasjonstryggleik. Det er vidare 12 prosent av respondentane som svarar at dei har lånt ut brukarnamn og passord til andre, medan 11 prosent viser til at dei «nokre gonger» ser at dette blir gjort av andre og 3 prosent oppgjev at dei «ofte» observerer dette. Revisjonen vil i den samanheng understreke at det å dele passord med andre ikkje er i samsvar med grunnleggjande prinsipp for informasjonstryggleik, også i tilfella der det er IT-tenesta ein deler passordet med.

## 6 Konklusjon og tilrådingar

Tysnes kommune har nyleg starta arbeidet med å etablere system og rutinar for arbeidet med informasjonstryggleik og personvern. Kommunen etablerte mellom anna handbok i informasjonssikkerhet og IKT-strategi 2022-2025 i 2022, og det er planlagt å gjennomføre leiinga si årlege gjennomgang i 2023. Arbeidet med å implementere rutinar og system var framleis pågåande på revisjonstidspunktet. Det er etter revisjonen si vurdering ein god del arbeid som ikkje er sett i verk på revisjonstidspunktet og kommunen manglar framleis ein del for å kunne ha tilfredsstillande system og rutinar for informasjonstryggleik.

Revisjonen vurderer at Tysnes kommune sine styrande dokument på revisjonstidspunktet langt på veg er i samsvar med krav i regelverket. Kommunen har gjennom handbok for informasjonssikkerhet og IKT-strategi 2022-2025 etablert mål og strategi for arbeidet med informasjonstryggleik i kommunen og styrande dokument er vidare tilgjengeleg for dei tilsette i organisasjonen via intranett og kvalitetssystemet (Compilo). Dette er i samsvar med krav på området (jf. eForvaltningsforskrifta § 15). Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette. Revisjonen vil påpeike at Tysnes kommune, i samsvar med denne tilrådinga, bør synleggjere kva krav og /eller anerkjende standardar dei baserer sine styrande dokument på.

Digitaliseringsdirektoratet tilrår at verksemder utformar føringar for arbeidet med informasjonstryggleik, og at struktur og innhald i styringsaktivitetane blir dokumentert på ein føremålstenleg måte slik at det er tydeleg kven som skal gjere kva, og korleis det skal gjerast (slik at dokumenteringa t.d. kan nyttast som oppslagsverk for tilsette). Revisjonen vurderer at Tysnes kommune sine styrande dokument i større grad bør tydeleggjere struktur og innhald i alle styringsaktivitetar, til dømes når det gjeld gjennomføring av tryggleiksrevisjonar. Undersøkinga viser at styrande dokument ikkje gir informasjon om kva tryggleiksrevisjonar omfattar, når det skal gjennomførast eller kven som har ansvar for dette.

Revisjonen er merksam på at kommunen sine styringsdokument relativt nyleg er etablert, og at arbeidet med å implementere rutinar og system i samsvar med dette framleis var pågåande på revisjonstidspunktet.

Revisjonen vurderer at Tysnes kommune ikkje i tilstrekkeleg grad har etablert tydelege ansvarsforhold knytt til informasjonstryggleik. Undersøkinga viser at det i all hovudsak går fram av kommunen si handbok for informasjonssikkerhet kva ansvar og oppgåver som ligg til ulike rollar i kommunen når det gjeld informasjonstryggleiksarbeidet. Undersøkinga indikerer samtidig at det står att ein del arbeid med å sikre at rollar og ansvar i dette arbeidet er tilstrekkeleg tildelt, kommunisert og etterlevd. Revisjonen vil påpeike at det er øvste leiing sitt ansvar å sikre det er etablert tydelege ansvarsforhold.

Revisjonen vurderer at Tysnes kommune på revisjonstidspunktet ikkje har etablert tilstrekkeleg rutinar knytt til informasjonstryggleik. Undersøkinga viser at kommunen er i prosess med å utarbeide slike rutinar og prosedyrar, men at dette per august 2023 ikkje ennå er ferdigstilt. Revisjonen vil understreke at kommunen skal sikre at internkontrollen er systematisk og at det er etablert nødvendige rutinar og prosedyrar (kommunelova §25-1).

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik på alle område. I handbok for informasjonssikkerhet blir retningslinjer for leiinga sin gjennomgang skildra, og det blir vist til at det skal gjennomførast tryggleiksrevisjonar. Desse styringsaktivitetane var ikkje gjennomført på revisjonstidspunktet. For tryggleiksrevisjonane var det på revisjonstidspunktet heller ikkje etablert formelle system og rutinar der det går fram korleis å gjennomføre tryggleiksrevisjonar. Revisjonen merkar seg også at det er ein plan om å få på plass årleg rapportering om informasjonstryggleik og personvern men at dette ikkje var implementert på revisjonstidspunktet. Revisjonen påpeiker difor at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta som seier at kommunen skal ha ein internkontroll på området som baserer seg på anerkjente standardar for styringssystem for informasjonstryggleik (§ 15).

Undersøkinga viser at det er ulike system for registrering av brukartilgangar, og at det ikkje går fram av skjema for tinging av brukaridentitet kva type tilgang brukaren skal ha (til dømes lesartilgang, full tilgang). Det blir også vist til at det er behov for å etablere skjema og rutinar som sikrar at leiarar søker om endra tilgang dersom tilsette får endra arbeidsoppgåver og dermed skal ha andre tilgangar i systema. Manglande registrering av endringar fører til ein risiko for at brukarar har tilgangar dei ikkje har behov for, og følgeleg risiko for at krava knytt til konfidensialitet

i regelverket ikkje alltid blir etterlevd. Dette er forhold som revisjonen meiner at kommunen må utbetre for å ha eit tilstrekkeleg system som sikrar tilgjenge og konfidensialitet i informasjonssystema som blir nytta i kommunen.

Revisjonen merkar seg også det at finst enkeltvise rutinar med instruksar og skjema som gjeld tilgangsstyring for nokre system. Revisjonen meiner at kommunen med fordel burde samle og gjere tilgjengeleg felles retningslinjer og rutinar for tilgangsstyring for alle kommunen sine elektroniske system slik at det blir tydeleg for dei involverte kva ansvar dei har for å sikre oppdaterte og riktige tilgangar, kven ein skal kontakte og korleis ein skal gå fram ved endring eller avslutning av brukartilgang mv.

Tysnes kommune har utnemnt eit personvernombod, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Revisjonen vil påpeike at kommunen pliktar å stille til rådighet dei ressursar som er nødvendig for at personvernombodet skal kunne utføre lovpålagde oppgåver (2. punkt i artikkel 38).

Det går vidare fram at personvernombodet opplever å i liten grad bli involvert i prosessar eller spørsmål knytt til vern av personopplysningar. Revisjonen er merksam på at noverande personvernombod har vore tilsett i kommunen i ein relativt kort perioden, og at det er sett inn fleire gode tiltak i perioden for å sikre involvering av personvernombodet. Revisjonen vil samtidig påpeike at kommunen etter personvernforordninga pliktar å sikre at personvernombodet på riktig måte og i rett tid blir involvert i alle spørsmål som gjeld vern av personopplysningar (1. punkt i artikkel 38).

Tysnes kommune har etablert personvernerklæring. Revisjonen vurderer samtidig at kommunen ikkje har sikra at denne erklæringa har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane. Datatilsynet skriv mellom anna i si rettleiing om verksemdene sine pliktar etter personvernregelverket<sup>47</sup> at verksemdene ikkje kan bruke juridisk eller teknisk sjargong når dei kommuniserer om personopplysningar, informasjonen skal vere forståeleg for målgruppa og informasjonen skal vere konkret (unngå formuleringar som «vi kan bruke personopplysningar til...»). Undersøkinga viser, etter revisjonen si vurdering, at Tysnes kommune i si fråsegn om personvern ikkje er tilstrekkeleg konkret og at det er nytta ein del omgrep og formuleringar som gjer fråsegna utfordrande å forstå for målgruppa.

Revisjonen vurderer vidare at kommunen si personvernerklæring ikkje er tilstrekkeleg lett tilgjengeleg, i samsvar med krav om dette i regelverket (artikkel 12 i personvernforordninga). Svar på spørjeundersøkinga indikerer at personvernerklæringa også er relativt ukjend for dei tilsette i kommunen; berre 12 prosent oppgjev å vere kjend med denne. Det skal ikkje vere nødvendig for brukarar å måtte leite etter informasjon om handsaming av personopplysningar, og revisjonen meiner derfor at kommunen bør plassere lenke til personvernerklæringa lett tilgjengeleg for ålmenta, til dømes på framsida for kommunen sine nettsider.

Tysnes kommune fører ikkje i tilstrekkeleg grad protokoll over behandlingsaktivitetar av personopplysningar. Undersøkinga viser at kommunen har sett i gang eit arbeid for å sikre at det framover skal førast protokoll over behandlinga av personopplysningar; det er mellom anna etablert mal for dette arbeidet og det er gjennomført workshops med nokre av leiarane i kommunen for å rette merksemd mot protokollføring. Revisjonen merkar seg likevel at kommunen på revisjonspunktet har utarbeidd få protokollar for behandling av personopplysningar og at dette heller ikkje blir gjort systematisk. Det er heller ikkje tilstrekkeleg tydeleggjort kven som skal ha dette ansvaret for dei ulike systema. Dette er ikkje i samsvar med krav om utarbeiding av behandlingsprotokollar (artikkel 30 i personvernforordninga).

Revisjonen vurderer at Tysnes kommune ikkje i tilstrekkeleg grad gjennomfører risikovurderingar av handsaming av personopplysningar, og at det heller ikkje i samband med risikovurderingar systematisk blir gjort vurderingar av personvernrisikoar (DPIA). Manglande risikovurderingar og rutinar for gjennomføring av slike gjer at kommunen ikkje har oversikt over kvar det er personvernrisikoar, og kommunen veit derfor heller ikkje kva eventuelle tryggleikstiltak som fungerer og ikkje. Kommunen manglar med dette grunnlag for å gjere eventuelle justeringar og slik kontinuerleg forbetre informasjonstryggleiken. Manglande risikovurderingar betyr vidare at kommunen heller ikkje veit kva personopplysningar dei handsamar med høg risiko, og har difor heller ikkje grunnlag for å gjennomføre vurdering av personvernkonskvensar ved behandling av personopplysningar med høg risiko, jf. personvernforordninga artikkel 35.

<sup>47</sup> Datatilsynet. Virksomhetenes plikter. Informasjon og åpenhet. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-åpenhet/>

Tysnes kommune har ved innføring av elektronisk avviksmeldesystem sikra oversikt over avvik som blir meldt knytt til personvern. Revisjonen vurderer samtidig at kommunen ikkje i tilstrekkeleg grad har etablert retningslinjer som sikrar tilfredsstillande rutinar for kven som har hovudansvar for å melde frå til Datatilsynet dersom det blir meldt om alvorlege brot på personopplysningstryggleiken, og det går heller ikkje fram kva som er frist for å melde slike avvik vidare til tilsynsmyndigheita. Revisjonen vil understreke at personvernforordninga er tydeleg på at den behandlingsansvarlege (dvs. rådmann) utan ugrunna opphald og seinast 72 timar etter å ha fått kjennskap til brot på personopplysningstryggleiken, skal melde brotet til Datatilsynet (jf. Artikkel 33). Datatilsynet peiker i si rettleiing på at den behandlingsansvarlege ikkje treng å melde frå om brot til Datatilsynet dersom brotet truleg ikkje vil medføre risiko for fysiske personar sine rettigheter og friheiter, men peiker vidare på at dersom behandlingsansvarleg er usikker på om unntaket er oppfylt bør melde frå til Datatilsynet for sikkerheits skuld.<sup>48</sup>

Undersøkinga viser at det er meldt avvik i desember 2022 om at helsepersonell frå både legekontor, helsestasjon og psykisk helseteneste har hatt tilgang til mapper med personsensitiv informasjon utan at dei har hatt tenestleg behov for dette. Dette skuldast at det blei oppretta ei mappe innan sikker sone, men likevel på eit område der tilsette frå fleire tenester hadde tilgang. Dette syner viktigeita av å gjennomføre kontrollar og å sikre at tilsette har tilstrekkeleg kompetanse knytt til handtering av personsensitiv informasjon.

Svara i spørjeundersøkinga tyder på at ikkje alle tilsette i kommunen veit at dei skal melde avvik knytt til informasjonstryggleik når dei opplever eller observerer slike tilfelle. Ein relativt stor del av respondentane som oppgjev at dei har opplevd slike avvik svarer at dei ikkje har meldt frå om dette. Kommunen si oversikt over registrerte avvik indikerer også at det er få avvik som blir meldt. Revisjonen vil peike på at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta.

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg rutinar for å sikre at tilsette får opplæring i informasjonstryggleik. Undersøkinga viser at kommunen har etablert nokre målsettingar om at opplæring knytt til informasjonstryggleik er viktig, og det går vidare fram av handbok i informasjonssikkerhet at leiarar og superbrukarar/fagsystemansvarlege har eit ansvar for å sikre at tilsette får denne opplæringa. Det går samtidig fram at kommunen ikkje har etablert system eller rutinar som sikrar tilsette får denne opplæringa. Kommunen har heller ikkje oversikt over kva opplæring eller kurs tilsette eventuelt har fått på dette området. Revisjonen vil påpeike at dette ikkje er i samsvar med krav og anbefalingar om kommunen sitt ansvar for å sikre tilstrekkeleg informasjonstryggleikskompetanse blant dei tilsette gjennom opplæringstiltak. Dette gjer at det er høgare sannsyn for at dei tilsette ikkje har tilstrekkeleg kompetanse innan informasjonstryggleik, noko som igjen aukar risiko for brot på regelverket som gjeld for behandling av personopplysningar og for informasjonstryggleiken generelt.

Revisjonen merkar seg at kommunen kjenner til behovet for opplæring av tilsette, og at det mellom anna blir vurdert å ta i bruk e-læring for å etablere opplæringsmodular og kurs innan mellom anna informasjonstryggleik på kommunen sine intranettsider.

Basert på funna i spørjeundersøkinga, vurderer revisjonen at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Til dømes svarar om lag halvparten av alle respondentane, og om lag ein av tre respondentar med leiaransvar, at dei *ikkje* kjenner innhaldet i kommunen si handbok i informasjonssikkerhet. Svar i spørjeundersøkinga indikerer vidare at det relativt store skilnadar mellom sektorane i kommunen når det gjeld kjennskap til styrande dokument for informasjonstryggleik. Til dømes går det fram at 93 prosent av respondentane frå oppvekstsektoren oppgjev å handsame både personopplysningar og sensitive personopplysningar, men 60 prosent av respondentane frå denne sektoren kjenner ikkje til innhaldet i kommunen si handbok i informasjonstryggleik. Det er vidare 14 prosent av respondentane frå oppvekstsektoren som ikkje veit om kommunen eller eininga har tilstrekkeleg skriftlege retningslinjer for handsaming av personopplysningar og 10 prosent svarar at det «i liten grad» er tilfredsstillande retningslinjer for dette. Vidare svarar 30 prosent av respondentane som oppgjev at kommunen og/eller eininga «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer for handsaming av personopplysningar, at dei ikkje kjenner til kvar dei finn desse retningslinjene og rutinane. Revisjonen vil understreke at kommunen etter personvernforordninga er forplikta til å sette i verk eigna tiltak, både organisatoriske og tekniske, for å sikre og påvise at personopplysningar blir handsama i samsvar med krav til dette i regelverket (personvernforordninga artikkel 24). Som ein del av dette bør kommunen mellom anna sikre at kommunen sine styrande dokument for informasjonstryggleik er tilgjengeleg og kjend for dei tilsette i kommunen.

---

<sup>48</sup> Datatilsynet. Hvilke brudd skal meldes til Datatilsynet? Publisert 24.03.2023. <https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hvilke-brudd-skal-meldes-til-datatilsynet/>

Revisjonen vurderer vidare at kommunen ikkje i tilstrekkeleg grad etterlever retningslinjer og rutinar for informasjonstryggleik. Undersøkinga indikerer at dokument med fortruleg informasjon ikkje alltid blir lagra på ein sikker måte og/eller blir oppbevart slik at uvedkomande kan få innsyn. Undersøkinga viser også at 16 prosent av respondentane ikkje følgjer ein praksis for avlogging av PC i samsvar med prinsipp om god informasjonstryggleik. Det er vidare 12 prosent av respondentane som svarer at dei har lånt ut brukarnamn og passord til andre, medan 11 prosent viser til at dei «nokre gonger» ser at dette blir gjort av andre og 3 prosent oppgjev at dei «ofte» observerer dette. Revisjonen vil i den samanheng understreke at det å dele passord med andre ikkje er i samsvar med grunnleggjande prinsipp for informasjonstryggleik, også i tilfella der det er IT-tenesta ein deler passordet med.

**Basert på det som kjem fram i undersøkinga vil revisjonen tilrå at Tysnes kommune set i verk følgjande tiltak:**

1. Etablerer styringssystem for informasjonstryggleik som tilfredsstillir krav i regelverket og som er basert på anerkjend standard på området. Under dette mellom anna:
  - a. sikrar at det er tydelege rollar og ansvar i arbeidet med informasjonstryggleik, og vidare at rollar og ansvar er tydeleg tildelt og kommunisert både til dei tilsette det gjeld og relevante tilsette i kommunen elles.
  - b. sikrar at det er etablert nødvendige rutinar og retningslinjer knytt til arbeidet med informasjonstryggleik i kommunen.
  - c. etablerer system for kontroll og etterprøving av informasjonstryggleik i kommunen, og sikrar at dette blir gjennomført jamleg (t.d. leiinga sin årlege gjennomgang og tryggleiksrevisjonar).
2. Gjennomfører eigna tekniske og organisatoriske tiltak for å sikre vedvarande konfidensialitet og integritet i behandlingssystema og -tenestene. Under dette mellom anna:
  - a. etablerer tilstrekkeleg system og rutinar som sikrar riktig nivå av tilgjenge og konfidensialitet i alle informasjonssystema som blir nytta i kommunen (både ved oppstart, endra arbeidsoppgåver og avslutting av arbeidsforhold),
  - b. sikrar at etablerte rutinar og retningslinjer for tilgangsstyring er tilgjengelege for alle relevante tilsette.
3. Sikrar at kommunen si personvernerklæring er lett tilgjengeleg og har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane, i samsvar med krav om dette i regelverket (artikkel 12 i personvernforordninga).
4. Sikrar at det blir utarbeidd protokoll over behandlingsaktivitetar av personopplysningar som blir utført i kommunen.
5. Sikrar at det blir gjennomført risikovurderingar av handsaming av personopplysningar, og at det i samband med gjennomføring av risikovurderingar også systematisk blir gjort vurderingar av personvernrisikoar (DPIA).
6. Ser til at retningslinjer for informasjonstryggleik tydeleg skildrar melding av avvik til Datatilsynet (ansvar og frist for å melde avvik vidare til tilsynsmyndigheita)
7. Får oversikt over kva kompetanse det er behov for hos leiarar og tilsette i arbeidet med informasjonstryggleiksarbeidet i kommunen.
8. Etablerer system og rutinar som sikrar at tilsette får tilstrekkeleg opplæring i informasjonstryggleik og personvern, under dette mellom anna:
  - a. sikre at tilsette har kjennskap til etablerte retningslinjer for informasjonstryggleik i kommunen
  - b. sikre at tilsette har kjennskap til at ein skal melde informasjonstryggleiksavvik, og korleis ein skal gå fram for å melde slike avvik

# Vedlegg 1: Høyringsuttale



Rådmannen

Sakshandsamar:  
Steinar Dalland  
Mobil: 970 46 500  
Vår ref: 2023/306- 4  
Dykkar ref:  
Dato: 27.09.2023

DELOITTE AS AVD BERGEN  
Postboks 6013  
5892 BERGEN

## Uttale til rapport - forvaltningsrevisjon informasjonstryggleik og personvern

Det vert vist til oversendt rapport til uttale.

Rådmannen si overordna vurdering av rapporten er at den på nokre område teiknar eit rett bilete av eksisterande praksis og system, på nokre område meiner rådmannen at rapporten trekk sine konklusjonar for langt.

Det grunnleggjande spørsmålet rådmannen stiller seg i samband med ein slik rapport er om det er eit godt utgangspunkt for vidare arbeid. Rådmannen meiner at rapporten gjev eit godt utgangspunkt for både å forbetra og endra eksisterande praksis på mange områder, på nokre områder kan den vera nyttig også for å synleggjera eksisterande praksis på ein litt meir nyansert måte. Dette gir såleis eit godt utgangspunkt for vidare arbeid både politisk og administrativt.

Rådmannen si samla vurdering er at Deloitte har gjort ein god gjennomgang av saksområde og rådmannen ser fram til å arbeida vidare ut frå dette utgangspunktet!

Med helsing

Steinar Dalland  
rådmann

*Brevet er elektronisk godkjent.*

Kopi til:  
Kjersti Gjuvsland  
Birte Bjørkelo

Tysnes kommune  
Uggdalsvegen 301

Telefon: 53 43 70 00

Bankgiro: 3525.07.00340

5685 UGGDAL

Org.nr: 959412340

e-post: post@tysnes.kommune.no

# Vedlegg 2: Utvida høyringsuttale



Kjersti Gjuvslund

Sentraladministrasjonen  
- stab

Sakshandsamar:  
Steinar Dalland  
Mobil: 95284301  
Vår ref: 2023/306- 7  
Dykkar ref:  
Dato: 21.12.2023

## Utvida uttale til rapport - forvaltningsrevisjon informasjonstryggleik og personvern

Det vert vist til epost av 13. desember d.å., her følgjer endeleg uttale.

I sitt opphavlege skriv dagsett 29. september d.å. der rådmannen skriv:

«Rådmannen si overordna vurdering av rapporten er at den på nokre område teiknar eit rett bilete av eksisterande praksis og system, på nokre område meiner rådmannen at rapporten trekk sine konklusjonar for langt.»

Tilbakemeldinga byggjer grunnleggjande på at me tar dei tilbakemeldingar me får, trekk ut det me kan av læring og bryr oss mindre om dei tilbakemeldingane der rapporten bommer.

Innanfor forskingsmetode er «bias» eit grunnleggjande omgrep. Omgrepet vert nytta om skeivheiter i utval eller data, bevisst eller ubevisst predisposisjon eller partiskheit opp mot einskilde konklusjonar. Rådmannen si vurdering er at rapporten har ein viss bias, truleg er dette ikkje medvite, men kan vera knytt til forståinga revisor har av eige oppdrag. Ein slik predisposisjon kan føra til at datagrunnlaget i rapporten i einskilde tilfelle vert trekt lenger enn det kanskje er grunnlag for, dette vil igjen føra til at rapporten gir eit svakare grunnlag for forbedring og endring enn den elles ville gjort. I ein del tilfelle kan rapporten trekka konklusjonar så langt at det også gjev grunnlag for å skapa utryggleik hjå publikum, det er i første rekkje dette punktet som gjer at rådmannen ser trong for å nyansera litt meir enn det rapporten i utgangspunktet har lagt opp til.

Når rådmannen no har lese gjennom rapporten på nytt så er det kanskje spesielt i kap. 6 at det kan synast som at konklusjonar vert malt opp med ein breiare pensel enn det rapporten elles legg opp til. Dette kan bli ytterlegare forsterka gjennom måten rapporten blir presentert på. I konklusjon og presentasjon vert nyansar fjerna og rapporten sine konklusjonar fjernar seg frå sitt eige datagrunnlag. Ein betre nyansering på dette punktet vil også gjera det enklare å gjera seg nytte av rapporten vidare.

Tysnes kommune  
Uggdalsvegen 301

Telefon: 53437000

Bankgiro: 3525.07.00340

5685 UGGDAL

Org.nr: 959412340

e-post: post@tysnes.kommune.no



I det følgjande vil me gå kort inn på ein skilde punkt i sjølve rapporten, men vil i hovudsak kommentera konklusjonar slik desse vert framstilt under kap. 6.

#### Styringssystem og informasjonstryggleik

##### 3.3.1 Omsynet til ISO/IEC 27001

På revisjonstidspunktet skriv Digdir i sin gjennomgang av standarden at det ikkje er krav til at offentlege verksemdar skal sertifiserast etter denne standarden. Det heitte vidare under Digdir si rettleiing punkt 2.4:

«Merk at offentlege verksemdar i Noreg ikkje er pålagd eller tilrådd å vera i samsvar med standarden.»

Dette er ikkje eit viktig punkt då KS sine læringsmateriell om GDPR og personvern mellom anna viser til denne ISO standarden, men har noko med valøren å gjera når revisjonen under punkt 3.3.1 skriv at:

«Ingen av dei intervjuja kjenner til den tilrådde standarden ved utarbeiding av styringssystem (ISO/IEC 27001) eller i kva grad kommunen etterlever denne.»

Revisjonen skriv på s. 10 i rapporten at:

«Digdir tilrår at offentlege verksemdar baserer seg på ISO/IEC 27001...»

Det vert her vist til note 5 der revisjonen skriv:

«Digdir påpeiker i eigen rettleiar om ISO/IEC 27001 at pålegget er å basera seg på anerkjente standardar og at tilrådinga er å basere seg på gjeldande versjon av ISO/IEC 27001. Offentlege verksemdar er dermed ikkje pålagt å vere i samsvar med standarden»

Noten er feil då det etter Digdir sin rettleiar heiter at offentlege verksemdar «..ikkje er pålagd eller tilrådd å vera i samsvar med standarden.» Rådmannen er kjent med at revisjonen etter verifikasjon har vore i kontakt med Digdir som då har uttrykt at dei meiner at offentlege verksemdar bør vera i samsvar med standarden. Det er også eit faktum at Digdir har utarbeidd nytt skrifleg rettleiingsmateriell etter at revisjonen vart fullført der dette vert tilrådd. Det framstår som likevel som unøyaktig at revisjonen ikkje kommenterer at standarden på revisjonstidspunktet ikkje var tilrådd i Digdir sitt skriftelege rettleiingsmateriell.

##### 3.3.2 Vurdering

Under vurdering skriv revisjonen mellom anna:

«Kommunen har gjennom handbok for informasjonstryggleik og IKT strategi 2022-2025 etablert mål og strategi for arbeidet med informasjonstryggleik i kommunen og styrande dokument er vidare tilgjengeleg for dei tilsette via intranett og kvalitetssystemet (Compilo). Dette er i samsvar med krav på området (jf. eForvaltningsforskriften § 15). Revisjonen vil samtidig påpeike at dei styrkande dokumenta ikkje i tilstrekkeleg grad skildrar system for kontinuerleg forbetring av leiing si styring av informasjonstryggleiken (til dømes gjennomføring av tryggleiksrevisjonar) og undersøkinga indikerer også at leiinga si styring av



informasjonstryggleik ikkje er tilstrekkeleg integrert i kommunen sine internkontrollprosessar. Det blir til dømes peikt på at informasjonstryggleik ikkje er fast tema på agenda i møta til strategisk leiing. Dette er ikkje i samsvar med krav til internkontroll på informasjonstryggleiksområdet (jf. § 15 i eForvaltningsforskrifta, andre ledd).

Det går fram av undersøkinga at dokument ikkje viser til standardar eller konkrete krav til regelverk på området. Regelverket set krav til at tryggleiksstrategi skal inkludere relevante krav som er fastsett i lov, forskrift eller instruks og at internkontroll skal basere seg på anerkjente standardar for styringssystem og informasjonstryggleik (eForvaltningsforskrifta § 15).»

eForvaltningsforskrifta § 15 har slik ordlyd:

#### **§ 15. Internkontroll på informasjonssikkerhetsområdet**

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

Omfang og innretning på internkontrollen skal være tilpasset risiko.

Konklusjonen om at Tysnes kommune sine styrande dokument ikkje er fullt ut i samsvar med krav i eForvaltningsforskrifta § 15 kan gjerne vera rett, men neppe på det grunnlaget som revisjonen viser til. For det første er internkontrollsystem for informasjonstryggleik fullt ut integrert i kommunen sitt overordna styringssystem for internkontroll og kvalitet. For det andre er ikkje det eit krav i forskrifta eller kommunelova sine reglar om internkontroll at alle kontrollområder skal ha eit eige punkt på strategisk leiarmøte. Per i dag er det slik at alle avvik innanfor område personvern og informasjonstryggleik går direkte til PVO og ansvarleg linjeleiar. Dersom det er avvik med høg alvorsgrad skal desse også gå direkte til kommunalsjef og rådmann. Kontrollaktivitetar, avvik og prosessar som kan føra til endringar i risikobilete innanfor informasjonstryggleik vert handsama i eige møtepunkt mellom IT leiar, rådmann og PVO kvar tredje veke. Per i dag, men ikkje på revisjonstidspunktet, vert alle avvik innanfor dette område gjennomgått på strategisk leiarmøte som 2. punkt på den faste agendaen.

Når det gjeld tryggleiksrevisjonar så skjer det i dag innanfor eit breidt spekter, nokre av revisjonane er knytt til teknisk løysing. Tysnes kommune har til dømes avtale med HelseCert som gjennomfører systematisk penetrasjonstestar av kommunen sin elektroniske system. Tilsvarande har kommunen avtale med Blackstone som gjennomfører systematisk skanning av moglege hol i system og nettverksoppsett. Det vert gjennomført kontinuerlege Phising testar for å vurdere og styrka brukarane sin kompetanse innanfor IT tryggleik. Forutan dette gjennomfører IT leiar revisjonar knytt til etterleving av rutiner for bruk av lagring på felles diskområder.

Det er vidare vist til at punkt 4.4 i Handbok om informasjonstryggleik:

«Gjennomgangen til leiinga skal haldast årleg for leiargruppa til rådmannen.

I møte skal det samanfattast status for informasjonstryggleiksarbeidet i kommunen, og dessutan avdekkast om tryggleiken blir vareteken i høve mål, strategiar og prosedyrar og vedtakast tiltak for det vidare sikkerhetsarbeidet. Tiltak skal sikra at sikkerhetsmål, strategi og organisering av informasjonstryggleikssystemet er oppdaterte og i samsvar med behovet til kommunen.

I gjennomgangen til leiinga skal m.a. følgjande punkt gåast gjennom og bli vurderte:

- Resultat og hovudkonklusjonar frå informasjonstryggleiksrevisjonar
- Registrerte avvik
- Rapportar frå offentlege og interne tilsyn
- Endringar i lover, forskrifter og offentlege sikkerhetskrav
- Endringar i dei personopplysningane som verksemda skal behandla
- Endringar i trusselbiletet som kjem fram i gjennomførte risikovurderingar
- Status på hendingar rundt teknisk informasjonstryggleik
- Organisatoriske endringar
- Bygningsmessige endringar
- Planar og framdrift for å ivareta intern kontroll og informasjonstryggleik.»

Tilsvarande har verksemda krav knytt til andre særskilte områder innanfor den samla styringssystem, det gjeld mellom anna oppfølging av ARP, årsrapport for HMT og vernearbeid med vidare.

Det er rett at Tysnes kommune i sitt IK system ikkje har vist eksplisitt til ein anerkjent standard, her har det vore naturleg å nytta dei tilrådingar som KS har gitt kommunane. Desse tilrådingane byggjer igjen på anerkjente standardar.

Det vert i rapporten kommentert at styrande dokument ikkje viser til standardar eller konkrete regelverk på området, men det er det er vanskeleg å sjå at det er ein mangel. Forskrifta stiller ikkje opp krav om at alle relevante regelverk skal listast opp, me kan ikkje sjå at revisjonen peiker på at reglar i lov, forskrift m.v. ikkje faktisk er ivareteke gjennom styrande dokument.

Rådmannen si vurdering er at det på dette punktet ikkje er grunnlag for å konkludera med at kommunen sitt internkontrollsystem ikkje er i samsvar med eForvaltningsforskrifta § 15 jf. kommuneloven § 25-1. I den grad revisjonen opprettheld sin konklusjon må i så tilfelle konklusjonen konkretiserast.

### 3.5.2

Revisjonen skriv under dette punktet:

«Revisjonen påpeiker likevel at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta § 15 eller tilrådingar i ISO/IEC 27001 knytt til oppfølging og kontroll.»

Etter rådmannen si vurdering kan det gjerne vere grunnlag for denne konklusjonen, men det må i så fall klargjerast kva konkrete krav i eForvaltningsforskrifta § 15 som ikkje er etterlevd. Når det gjeld ISO/IEC 27001 var ikkje dette ein tilrådd standard på revisjonstidspunktet. Me ber såleis om at revisjonen konkretiserer avvik opp mot standarden med presise tilvisingar, det er også ein føremon om standarden kan gå inn som vedlegg til rapporten.

#### Konklusjon og tilrådingar

Det er kanskje i dette kapittelet at det er vanskeleg å sjå samanhangen mellom datagrunnlaget, vurderingar undervegs og dei overordna konklusjonane.

#### **Tysnes kommune har ikkje etablert styringssystem for tilfredsstillar krav i sentrale føresegner:**

- Kulepunkt 1: Her er det eit spørsmål om tolking av eForvaltningsforskriften § 15. Er problemstillinga her at styrande dokument ikkje eksplisitt viser til standard, eller er avviket at styrande dokument ikkje tar opp i seg innhaldet av etablerte standardar. Ein meir nøytral konklusjon vil her vera:
  - Kommunen sine styrande dokument må vise til kva standard dei byggjer på.
- Kulepunkt 2: Ein konklusjon som er langt meir i tråd med rapporten er at Tysnes kommune langt på veg har skildra ansvarsforhold knytt til informasjonstryggleik. Undersøkinga viser tilsvarande at ansvarsforhold ennå ikkje er fullt ut implementert og forstått i alle deler av organisasjonen.
  - Det må presiserast i ansvarsskildringa at rådmannen er behandlingsansvarleg, dei funksjonar som er lagt til rådmannen særskilt må skildrast nærare.
  - Det må sikrast at rollefordelinga vert forstått og etterlevd på alle nivå i organisasjonen.
  - Det bør særskilt gjerast ei vurdering knytt til det som ser ut til å vera avvikande praksis innanfor oppvekst.

- Kulepunkt 3: Ok
- Kulepunkt 4: Her er konklusjonen vanskeleg å forstå, rådmannen kan ikkje sjå at det er grunnlag for å sei at det ikkje er etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik etter eForvaltningsforskrifta § 15. Når det gjeld ISO/IEC 27001 var den, som revisjonen kjenner til ikkje ein tilrådd standard, på revisjonstidspunktet. Dersom revisjonen ønskjer å halde på denne formulering må i alle fall konklusjonen underbyggjast. Når det gjeld verksemda sin årlege gjennomgang så er det ganske detaljert skildra kva den skal innehalde. Når det gjeld tryggleiksrevisjonar er dette tiltak for å sikre etterleving av rutiner, men også revisjonar som tar utgangspunkt i spesifikke risikoområder. Det vert per i dag gjennomført faste og systematiske sikkerhetsrevisjonar opp mot teknisk infrastruktur, det vert tilsvarande gjennomført systematiske revisjonar knytt til brukaratferd mellom anna gjennom phishing testar. Det vert også gjennomført einskild revisjonar knytt til etterleving av rutinar for lagring av sensitiv informasjon på strukturerte lagringsområdet.

Det kan vere naturleg å stille spørsmål om korvidt systemet er tilstrekkeleg implementert. Ein meir balansert konklusjon vil vera:

Tysnes kommune har langt på veg skildra system for kontroll og etterprøving av informasjonstryggleik, på revisjonstidspunktet var ennå ikkje leiinga sin årsgjennomgang gjennomført noko som gjer at revisjonen ikkje kan konkludere med at systemet er tilstrekkeleg etablert.

- Revisjonen tilrår at rapport knytt til leiinga sin årlege gjennomgang også vert sendt til kommunestyre for informasjon.
- 
- Kulepunkt 5: Konklusjonen er kanskje grei nok, men den er veldig vid, så vid at den etter underteiknande sitt syn ikkje gjev eit rett bilete av situasjonen. Slik konklusjonen står no gjeld dette alle kommunen sine informasjonssystem. Realiteten er at for dei aller fleste av systema våre er tilgjenge og rettar veldig finmaska i høve til kva tilgangar som vert gitt opp mot kva rolle den tilsette har. I underlaget viser de til to problemstillingar: 1) Tilsette på NAV der tilgangen er gitt ut «flatt», men her er det gjort ut frå at alle dei tre tilsette arbeider med same saksfelt. Dei har såleis tenestleg behov for dei tilgangar dei er tildelt. Det blir samstundes ført logg over oppslag og det er mogleg å skjerme einskilde saker der einskilde tilsette er inhabile. Når dette er sagt så vil det vera naturleg å vurdere systematiske revisjonar knytt til oppslag for å vurdere om einskilde tilsette tileignar seg informasjon utover tenestleg behov. 2) Tinging og avslutning av tilgangar skjer på ein anna måte innanfor oppvekst enn i resten av verksemda.

Når det gjeld avslutning av brukartilgangar så er det ei felles rutine for heile verksemda, jf. Handbok for informasjonstryggleik punkt 3.6, men også rutine for avslutning av arbeidsforhold. For tilsette i skular og barnehagar så skal avslutning meldast til IT leiar for skule, for andre skal det meldast til IT leiar for øvrig verksemd. Innanfor skule og barnehage er det også slik at AD er

automatisk knytt til lønssystemet slik at brukarar vert automatisk sletta når løn vert avslutta. Når det gjeld tilgang og brukarkontroll følgjer det punkt 3.1, men det er også ein del av kommunen si rutine for mottak av nyttilsette.

Trass i at det er etablert system og klare ansvarslinjer kan avvik førekomme, i desse tilfella er avvikssystemet grunnlag for å evaluere og følge opp svikt.

### **Tysnes kommune etterlever ikkje alle sentrale krav i personvernlovgivinga som er undersøkt**

- Kulepunkt 1: I denne konklusjonen vert det vist til at PVO har ein redusert stilling, her vil me visa til Datatilsynet sin gjennomgang av ordninga med PVO i norske kommunar som viser at over 50 % av kommunane har PVO tilsett i mindre enn 20 % stilling. Det er elles heilt rett at kommunen pliktar å sikre at PVO på rett måte og til rett tid vert involvert i alle spørsmål som gjeld vern av personopplysingar. Rådmannen anerkjenner PVO si oppleving at det kan opplevast vanskeleg å setja av tilstrekkeleg tid til oppgåva, men her må det også sjås opp mot iverksette tiltak for å sikra at PVO får tilstrekkeleg tid: 1) Faste møtepunkt mellom PVO, IT leiar og rådmann for å samordna prioriteringar og gå gjennom oppgåver og endringar som kan føra til risiko og trong for tiltak, 2) fast involvering på alle møter i utvida leiarteam for å sikra informasjonsflyt til PVO og frå PVO, 3) fast møtepunkt med strategisk leiing der alle avvik innanfor personvern og informasjonstryggleik vert gjennomgått. Kommunen har også sikra at PVO får tilgang til tilstrekkeleg opplæring. Rådmannen meiner at det ikkje er grunnlag for å sei at kommunen ikkje fyller sine plikter i forhold til PVO etter personopplysingsloven art. 38, men ser at oppleving av å ha tilstrekkeleg tid alltid vil vera krevjande.
- Kulepunkt 2: Den er ok
- Kulepunkt 3: Den er ok
- Kulepunkt 7: Den er ok
- Kulepunkt 8: Konklusjonen om at kommunen ikkje i tilstrekkeleg grad har etablert rutinar for sikrar tilfredsstillande oppfølging av meldte avvik knytt til informasjonstryggleik er for vid. Det er etablert rutinar for å sikra tilfredsstillande oppfølging av meldte avvik i det store og heile. I dag er avvik innanfor personvern og GDPR omfatta i kommunen sitt samla system for avviksmeldingar. Oppfølging av avvik innanfor dette område vert gjort i minst fire ledd: 1) linja, 2) avdelingsnivå, 3) strategisk leiing og 4) i felles møte mellom PVO, rådmann og IT leiar. For sistnemnde så vert det no også avvik kommentert slik at også meldar får melding om at avviket er vurdert på dette nivået. Det er vidare skildra oppsett på eskalering og handsaming av avvik med ulike alvorsgrad og alle avvik, uavhengig av alvorsgrad, går også i samtidig kopi til PVO.

Når det er sagt så er det heilt rett at melding til Datatilsynet ikkje er tilstrekkeleg skildra i handboka. Her er det naturleg at det vert ført inn som eit punkt under rolleskildringa slik at det går klart fram at det er rådmann som

skal melda avviket og at fristen snarast mogleg, men seinast innan 72 timar. Dette følgjer lovkravet, rådmannen er kjent med både fristen, vilkåra og ansvaret for å melda inn. Når det vert lagt opp til at dette vert vurdert særskilt også i møtepunkt mellom rådmann, IT leiar og PVO så er ikkje det for at dette er beslutningar som skal tas kollektivt, men fordi det er viktig at vurderingar som rådmannen gjer er mogleg å etterprøva og at dei også bør kunne kritiserast/utfordrast av PVO og kommunen sin fagansvarlege på IT.

- Kulepunkt 9: Her bør nok dette punktet nyanserast litt, bruk av uttrykket «uvedkomande» er etter rådmannen sitt syn for vidt og skaper eit inntrykk av at opplysingar mest er fritt tilgjengeleg for alle som er innom Rådhuset. Dette er sjølvsagt ikkje tilfelle og det er heller ikkje noko i dykkar datagrunnlag som understøttar ein slik konklusjon. Dette er kanskje det mest problematiske punktet i dykkar konklusjon og eit punkt som svekka innbyggjarane si oppleving av tryggleik noko som gjer det vanskeleg å la dette punktet stå slik det er.

Kommunen gjennomfører tekniske og organisatoriske tiltak i samsvar med artikkel 32, første ledd bokstav b. Dei tekniske tiltaka er knytt til brukar- og tilgangsstyring gjennom fagsystem, i tillegg er det eit finmaska system for datalagring der moglegheit for å lagre data er avgrensa og delt inn etter fag og avdeling. I tillegg er det eigne skilje mellom sikker sone og adm. sone. Ulike avdelingar har ulike oppsett for print og skanning, dette er avgrensa både gjennom fysiske og IT tekniske verkemiddel. Tilgangen til fysiske lokale er sikra gjennom elektroniske tilgangssystem, tilgangssystema gjev også grunnlag for å hente ut data om det skulle vera mistanke om at det har vore uautorisert tilgang. Organisatorisk er det gjeve ulike instruksar knytt til bruk av felles område innanfor einskilde avdelingar, kva skal kunne lagrast, korleis skal mappestruktur med vidare vera. Det er også gjort tilpassingar mellom anna til at kommunen ikkje publiserer fulltekstdokument på nettsida under innsynsløysinga. Ved førespurnad om dokumentinnsyn er det alltid sidemannskontroll før dokument vert sendt ut. Denne gjennomgangen er ikkje uttømmende. På dette punktet er det vanskeleg å sjå at Tysnes kommune ikkje opptre i samsvar med artikkel 32, første ledd, bokstav b.

Dette kan likevel ikkje heilt eliminere risiko for at det kan oppstå avvik, den største risiko for slike avvik vil vera at tilsette innfor same avdeling får tilgang til informasjon utover tenestleg behov. I desse tilfella skal det følgjast opp gjennom avvikssystemet.

- Kulepunkt 10: Rådmannen er samd i at svara i spørjeundersøkinga tyder på at det framleis er ein veg å gå for å sikra at alle avvik vert meldt. Dette er eit kontinuerleg fokusområde, og det styringsmessige fokuset på personvern avvik er ekstra tungt ut frå at me ser at det er færre avvik på dette området. Det er fram til no i år meldt 31 avvik innanfor personvern, 81 % av desse er lukka, det vert ført og fylgt opp kor avvika er registrert, kor lang tid det går før dei blir lest, kor lang tid det går før dei blir lukka, kva avvik som vert fylgt opp med vidare tiltak. I tillegg til dette vert kvart avvik særskilt vurdert i samband med møteplass personvern der rådmann, IT leiar og PVO deltek. Det kunne vore interessant om det vart gjort ein empirisk vurdering på om

talet på avvik innanfor dette fagområdet er høgt eller lågt opp mot kommunar av tilsvarande storleik.

Rådmannen er samd i revisjonen sine vurdering om at manglande avviksmeldingar aukar risiko for at svakheiter systema ikkje vert retta. Rådmannen meiner likevel at kommunen sin avvikspraksis og vurderingar knytt til generelle prinsipp for god internkontroll må vurderast i ljøs av det kunnskapsgrunnlaget og tiltaka kommunen set i verk for å sikra at avvikssystemet faktisk vert etterlevd. Ein konklusjon på dette grunnlaget om at kommunen ikkje etterlever generelle prinsipp for god internkontroll er å tolka det datagrunnlaget revisjonen har for langt.

### **Kommunen har betringspotensiale når det gjeld å sikre at tilsette har tilstrekkeleg kompetanse om informasjonstryggleik**

Generelt: Denne konklusjonen kunne nok vore strekt lenger, dette er ut frå rådmannen si vurdering det mest vesentlege avviket og konklusjonen her kunne nok vore skjerpa.

- Kulepunkt 1: Konklusjonen her er ok. Det kan nemnast at me i haust har skaffa oss tilgang til KS lærings om både har gode læringsmodular, men som også gjev oss moglegheit til å sjå kven som har gjennomført og kven som ikkje har gjennomført den pålagde opplæringa.
- Kulepunkt 2: Ok.
- Kulepunkt 3: Ok. Dei styrande dokumenta er lett tilgjengeleg for alle tilsette, det er også vorte gjennomført eigne gjennomgangar for leiarar utan at det synes å ha hatt synleg effekt. Rutina for tinging av IT tilgangar er skjerpa inn ved at leiar no må stadfesta at den tilsette faktisk har lese handbok for IT tryggleik før tilgang vert oppretta.
- Kulepunkt 4: Her viser me til kommentar under kulepunkt 9 under førre hovudoverskrift. Kommunen gjennomfører tiltak etter personvernforordninga art. 32, men dette er ikkje tilstrekkeleg til å eliminera ein kvar risiko. Betre opplæring og vedvarande fokus på avvik vil medverka til å redusera risikoen vidare.

Når dette er sagt bør revisjonen vurdere nærare validiteten i einskilde data som kjem fram i spørjeundesøkinga. Til dømes går det fram at 38 % av tilsette innanfor teknisk sektor opplever at sensitive data aldri blir fjerna frå møterommet når møtet er avslutta. Underteiknande tolka det som eit uttrykk for at data blir liggjande att på møteromma, men truleg er det eit uttrykk for at det ikkje finnes slike data etter møte.

### **Revisjonen sine tilrådingar:**

Eg vil ikkje gå gjennom alle punkta og tilrådingane, men generelt heng det litt saman med vurderingane ovanfor. Tilrådingane kan stå slik dei gjer, men det er ikkje alle punkta der me ser at det faktisk er grunnlag for endring og på nokre punkt er det trong for mindre justeringar. På andre punkt igjen slik som punkt 4 og 5 står det igjen eit omfattande arbeid.

**Avslutning:**

Til slutt ber me om at spørjeskjema som er nytta og den ISO standarden de har nytta som revisjonskriterie vert lagt ved den endelege rapporten.

Med helsing

Steinar Dalland  
rådmann

*Brevet er elektronisk godkjent.*

Kopi til:



# Vedlegg 3: Kommentar til utvida høyringsuttale

## Innleiing

Forvaltningsrevisjonar er underlagt strenge krav til prosess og kvalitetssikring for å sikre at informasjon som kjem fram i rapporten er riktig. Ein viktig del av dette arbeidet er at alle som er intervjuet får sine referat til godkjenning. Deretter får rådmannen rapporten til faktasjekk og står fritt til å kome med innspel om noko framstår uklart, om ein ikkje er einig i revisjonskriteria som er nytta eller ønskjer å supplere med informasjon. Då kan ein også kome med innspel dersom ein meiner at det er eit «bias» i rapporten. Deretter får rådmannen rapporten på høyring. Dette er eit nytt høve til å kommentere dersom ein meiner det er forhold som trengst å justerast. Alle desse prosessane blei gjennomført i samsvar med krava. Revisjonen tok omsyn til verifiseringsvaret ved å justere delar av rapporten, og følgde opp med Digitaliseringsdirektoratet om vi hadde lagt rett kriterium til grunn. Når vi mottok høyringsvaret frå rådmann sendte vi dette ilag med rapporten til kontrollutvalet.

Likevel fekk revisjonen ved framlegging av rapport for kontrollutvalet, informasjon om at rådmannen hadde innvendingar til rapporten som ikkje blei formidla verken i verifiseringsprosessen eller gjennom høyringsvaret.

På bakgrunn av dette fekk rådmannen høve til å kome med ein utvida høyringsuttale med ei skriftleg utgreiing av punkta som rådmannen meinte ikkje var rett vurdert eller der det eventuelt mangla informasjon. Revisjonen har på bakgrunn av den utvida høyringsuttalen justert noko av teksten i rapporten.

## Under vil revisjonen kommentere eit par moment i kommunen sin utvida høyringsuttale.

I den utvida høyringsuttalen skriv rådmann at det ikkje er eit krav at offentlege verksemder skal sertifiserast etter ISO/IEC 27001, og at det mellom anna framstår som unøyaktig at revisjonen ikkje har kommentert at standarden (ISO/IEC 27001) ikkje var tilrådd i delar av Digdir sitt tidlegare skriftlege rettleiingsmaterieil.<sup>49</sup> Revisjonen vil påpeike at vi ikkje har lagt til grunn at kommunen skal sertifiserast etter ISO-standard. Det er riktig at det i ein rettleiar frå Digdir på revisjonstidspunktet gjekk fram at offentlege verksemder verken var pålagt *eller tilrådd* å vere i samsvar med standarden. Som rådmannen påpeiker er det no utarbeidd ein ny versjon av denne rettleiaren der teksten er noko endra for å ta inn endringar i ny versjon av standarden. I oppdatert versjon av rettleiaren går det også fram at offentlege verksemder i Noreg ikkje er pålagde å vere i samsvar med ISO-standard, men at pålegget er å basere seg på anerkjende standardar og at tilrådinga er å basere seg på gjeldande versjon av NS-ISO/IEC 27001.

Revisjonen er samd i at det er eit viktig poeng at offentlege verksemder ikkje er påkravd å etterleve standarden ISO/IEC 27001, men at ein er påkravd å ha internkontroll på informasjonstryggleiksområdet som *baserer seg på* anerkjente styringssystem for informasjonstryggleik. Uttrykket «baserer seg på» gir eit viktig handlingsrom til det enkelte forvaltningsorgan til å tilpasse bruk av anerkjente standardar på informasjonstryggleiksområdet til egne behov og eigen heilskapleg verksemdsstyring.<sup>50</sup> Revisjonen har på bakgrunn av tilbakemeldinga frå rådmannen tatt ut kriteria i kapittel 3 som viser konkret til ISO-standard og erstatta dette med rettleiing frå Digitaliseringsdirektoratet. Rettleiingsmaterieilet frå Digitaliseringsdirektoratet baserer seg på eForvaltningsforskrifta og ISO/IEC 27001 og er Digitaliseringsdirektoratet sine offisielle tilrådingar for korleis verksemder kan etablere og vedlikehalde systematisk internkontroll på informasjonstryggleiksområdet. Krav og tilrådingar på området er såleis stort sett dei same uavhengig av om ein legg rettleiingsmaterieil eller ISO-standard til grunn. På bakgrunn av denne endringa har vi vidare tatt ut ein setning frå datagrunnlaget i avsnitt 3.3.1 (tatt ut setning om kjennskap til standard) og justert delar av vurderingane i avsnitt 3.3.2. og i avsnitt 5.3.2.

<sup>49</sup> Digitaliseringsdirektoratet. *Kva seier NS-ISO/IEC 27001*. Denne rettleiinga er revidert etter revisjonsperioden for denne forvaltningsrevisjonen. <https://www.digdir.no/informasjonsikkerhet/kva-seier-ns-isoiec-27001/3060>

<sup>50</sup> Regjeringa.no: Veileder til eForvaltningsforskriften. Første del: *eForvaltningsforskriften: Elektronisk samhandling med og i forvaltningen* av Rolf Riisnæs, advokat dr. juris.: <https://www.regjeringen.no/no/dokumenter/veileder-til-eforvaltningsforskriften/id2425012/>

Revisjonen vil presisere at vi ikkje har henta inn ny eller oppdatert data frå kommunen etter at undersøkingsperioden var ferdigstilt i september 2023, og at endringane som er gjort i vurderinga dermed ikkje inkluderer eventuelle endringar som er gjort i kommunen sine styrande dokument, rutinar mv. etter revisjonsperioden.

Rådmann peiker på at det i rapporten blir vist til at styrande dokument ikkje viser til standardar eller konkrete regelverk på området, og at det er vanskeleg å sjå at dette er ein mangel. Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette.<sup>51</sup> Revisjonen er samtidig samd i at det viktigaste ikkje er at styrande dokument skal vise til konkrete regelverk og standardar, men at dei styrande dokumenta er basert på dette. Vi har difor tatt omsyn til dette i avsnitt 3.3.2.

Revisjonen anerkjenner at teksten i vurdering 4.3.2. om utnemnt personvernombod var formulert slik at det kunne oppfattast som at vi peika på stillingsprosenten til personvern som ei utfordring. Revisjonen vil påpeike at det er kapasiteten til å utføre oppgåvene som personvernombod som blir vist til som ei utfordring, og har tatt ut delen av setninga som omtala stillingsprosent i vurderinga då dette kunne mistolkast. Revisjonen oppfattar utifrå rådmann sine kommentarar på dette punktet at han er samd i at kommunen pliktar å sikre at personvernombodet på rett måte og til rett tid blir involvert i alle spørsmål som gjeld vern av personopplysninga, og at han anerkjenner at personvernombodet på revisjonstidspunktet har hatt ei oppleving av at det er utfordrande å sette av tid til denne oppgåva. Rådmannen påpeiker i sin utvida høyringsuttale at det er iverksett tiltak på dette området for å involvere personvernombodet, noko også revisjonen påpeiker i vurdering 4.3.2.

Rådmannen peiker i utvida høyringsuttale på at det skjer tryggleiksrevisjonar innan eit breitt spekter i kommunen. Revisjonen er merksam på at kommunen mellom anna har avtale med ein ekstern leverandør på IKT-tenester, og at kommunen har avtale med HelseCert. Dette er viktige tiltak for å sikre IKT-tryggleiken i kommunen (beskytte maskin- og programvare), og er dermed ein viktig del av tiltaka som samla skal sikre tilstrekkeleg informasjonstryggleik i kommunen. Denne forvaltningsrevisjonen har i hovudsak undersøkt i kva grad kommunen har tilstrekkeleg internkontroll på informasjonstryggleiksområdet (styringssystem for informasjonstryggleik), og då særskilt leiingsaktivitetar på området. Vi har ikkje i denne forvaltningsrevisjonen gått inn på tekniske tiltak for å sikre informasjonstryggleiken.

Revisjonen merkar seg at rådmann er samd i revisjonen si vurdering 4.6.2. om at det ikkje framgår av styrande dokument kven som har hovudansvar for å melde frå til Datatilsynet dersom det blir meldt om alvorlege brot på personopplysningstryggleiken, og at det heller ikkje går fram kva som er frist for å melde slike avvik vidare til tilsynsmyndigheita. Revisjonen meiner at rådmann sitt innspel om å føre inn ansvar og tidsfrist for melding av avvik i handbok for informasjonssikkerheit er føremålstenleg.

Rådmannen påpeiker at han opplever at bruken av omgrepet «uvedkomande» er problematisk. Vi har presisert kven det vi spesifikt viser til i teksten.

Revisjonen oppfattar vidare utifrå rådmannen sin utvida høyringsuttale at han er samd i at svara i spørjeundersøkinga tyder på at kommunen har rom for betring når det gjeld å sikre at avvik blir meldt, og at manglande avviksmeldingar aukar risiko for at svakheiter i systema ikkje blir retta. Revisjonen har tatt ut tilvisinga til ISO/IEC 27001 i denne vurderinga, jf. første avsnitt i revisjonen sine kommentarar til den utvida høyringsuttalen.

Rådmann peiker også på at revisjonen burde vurdere validiteten nærare i data som kjem fram av spørjeundersøkinga. Rådmannen viser til at tilsette innanfor eit av tenestoområda i kommunen i samband med eit av spørsmåla truleg har lagt noko anna i svara sine enn det som var meint med spørsmålet. Revisjonen vurderer både reliabilitet og validitet i alt arbeid med forvaltningsrevisjonen. Revisjonen meiner det ikkje er sannsynleggjort at det er ei anna tolking enn det som er lagt til grunn i rapporten som er den rette. Dette er likevel ikkje til hinder for at rådmannen kan følgje opp og sikre at tiltaka som blir sett i verk er best mogleg tilpassa behova i organisasjonen.

Rådmannen viser også i utvida høyringsuttale til at det i kapittel 6 (konklusjon og tilrådingar) blir opplevd som vanskeleg å sjå samanheng mellom datagrunnlaget, vurderingane undervegs og konklusjonane. Revisjonen har utvida punkta i konklusjonen slik at all informasjon frå vurderingane i rapporten blir tatt med.

Rådmannen ber i utvida høyringsuttale om at spørjeskjema som er nytta blir lagt ved endeleg rapport. Revisjonen har lagt inn figurar frå gjennomført spørjeundersøking i rapporten, og det går fram spørsmålsformulering og

<sup>51</sup> Digitaliseringsdirektoratet. Informasjonssikkerhet. Internkontroll i praksis. Etableringsaktiviteter. Utforme føringer. <https://www.digdir.no/informasjonssikkerhet/utforme-foringer/3159>

svarfordeling per svaralternativ for alle spørsmåla. Utover dette kan ikkje revisjonen dele resultat frå spørjeundersøkinga av omsyn til konfidensialitet.

Rådmannen peiker også på at det vil vere eit føremon om revisjonen kan legge inn ISO/IEC 27001 som vedlegg til rapporten. Revisjonen vil her påpeike at det er Standard Norge som fastset Norsk Standard og Standard Online og som forvaltar rettigheter på opphavsmanns- og utgjevarsida ([standard.no](http://standard.no)). Standardar er litterære verk som er opphavsrettsleg beskytta i henhold til Lov om opphavsrett til åndsverk m.v. (åndsverkloven).

# Vedlegg 4: Revisjonskriterier

## Informasjonstryggleik

Informasjonstryggleik handlar om trygging av informasjon med omsyn til *konfidensialitet*, *integritet* og *tilgjengelegheit*.

Å sørge for *konfidensialitet* inneber å hindre ikkje-autorisert innsyn i informasjon som ikkje skal vere tilgjengeleg for alle; å sørge for *integritet* inneber å hindre ikkje-autorisert endring og sletting av informasjon; å sørge for *tilgjengelegheit* inneber å sikre tilgang til informasjon ved behov for tilgang.

## Krav i lov og forskrift

Regelverket knytt til informasjonstryggleik omfattar mellom anna personopplysningslova.<sup>52</sup> Denne tredde i kraft 20. juli 2018, og gjennomfører EU si personvernforordning – kjend som GDPR<sup>53</sup> – i norsk lov.

Artikkel 4 i personvernforordninga definerer omgrepa brukt i forordninga i 26 punkt. Under er nokre relevante punkt presentert:

1) «personopplysninger» enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»); en identifiserbar fysisk person er en person som direkte eller indirekte kan identifiseres, særlig ved hjelp av en identifikator, f.eks. et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidetifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet,

2) «behandling» enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring

...

7) «behandlingsansvarlig» en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes ...

8) «databehandler» en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlige

...

12) «brudd på personopplysningssikkerheten» et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet

I kommunen er det rådmannen som er behandlingsansvarleg.<sup>54</sup> Databehandlarar er eventuelle tenesteleverandørar til kommunen som behandlar personopplysningar, som til dømes leverandør av løn- og personalsystem. Forordninga artikkel 28 nr. 3 stiller krav om at behandling av personopplysningar utført av ein databehandlar skal vere underlagt ein avtale med nærare spesifisert innhald (bokstav a til h).

## Internkontroll og styringssystem for informasjonstryggleik

Artikkel 24 og 28 i personvernforordninga omhandlar den behandlingsansvarlege og databehandlaren sitt ansvar for å etablere internkontroll; nr. 1 i artikkel 24 seier mellom anna at den behandlingsansvarlege skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov», medan artikkel 28 nr. 1 stiller krav om at databehandlarar skal gi tilstrekkeleg med garantiar «for at de vil gjennomføre egnede tekniske og organisatoriske tiltak som sikrer at behandlingen oppfyller kravene i denne forordningen og vern av den registrertes rettigheter.»

<sup>52</sup> Lov om behandling av personopplysninger (personopplysningsloven)

<sup>53</sup> General Data Protection Regulation

<sup>54</sup> Jf. *En veiledning om internkontroll og informasjonssikkerhet* (Datatilsynet 2009, s. 11).

Personvernforordninga artikkel 32 nr. 1 stiller vidare krav om informasjonstryggleik ved behandling av personopplysningar. Krava som blir stilt er at informasjonstryggleiken skal vere tilfredsstillande med omsyn til personopplysningane sin konfidensialitet, integritet, tilgjengelegheit og robustheit gjennom at det blir sett i verk eigna tekniske og organisatoriske tiltak basert på risikovurderingar. Artikkelen inneheld føresegn som omhandlar kva risikovurderingane skal leggje vekt på.

I tillegg til føresegna i personvernforordninga knytt til internkontroll og informasjonstryggleik, er kommunen gjennom eForvaltningsforskrifta § 15 forplikta til å ha eit internkontrollsystem basert på anerkjende standardar for styringssystem for informasjonstryggleik:

Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.

Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

I rettleiar til e-forvaltningsforskrifta går det fram følgjande når det gjeld § 15 andre ledd:

Internkontrollen (styring og kontroll) på informasjonssikkerhetsområdet skal være basert på anerkjente standarder for styringssystem for informasjonssikkerhet. I det ligger en klar føring om at det ikke er tilstrekkelig å basere seg på generelle rammeverk eller standarder for virksomhetsstyring alene. Når det gjelder informasjonssikkerhetsområdet må forvaltningsorganet baserer seg på de standarder som er utviklet innenfor informasjonssikkerhetsområdet spesielt og som oftest omtales som styringssystem for informasjonssikkerhet. De må i tillegg være anerkjente. Samtidig gir eForvaltningsforskriften gjennom nøkkelordene "basere seg på" et viktig handlingsrom til det enkelte forvaltningsorgan for å tilpasse anvendelsen av anerkjente standarder på informasjonssikkerhetsområdet til egne behov og egen helhetlig virksomhetsstyring. Selv om den anerkjente standarden en velger å basere seg på stiller spesifikke krav, må forvaltningsorganet selv beslutte ut fra egen risikovurdering om det enkelte kravet i standarden er noe forvaltningsorganet faktisk skal følge eller ikke. Alle kravstandarder om internkontroll/styringssystem blir derfor i eForvaltningsforskriftens forstand veiledende. Vesentlige avvik fra valgt kravstandard bør imidlertid begrunnes, da de er ment å representere god praksis "for de fleste".<sup>55</sup>

Digitaliseringsdirektoratet (Digdir) er peika ut som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttas. Digdir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001, som er ein internasjonal standard for styringssystem for informasjonstryggleik.

### Ytterlegare krav i personvernforordninga

Personvernforordninga stiller krav om kommunen skal informere registrerte personar om at kommunen handsamar personopplysningar om dei, jf. artikkel 12-14. Artikkel 12 nr. 1 pålegg kommunen at slik informasjon skal vere «kortfattet, åpen, forståelig, lett tilgjengelig og på et klart og enkelt språk.» Datatilsynet skriv i sitt rettleingsmateriell at ein behandlingsansvarleg t.d. kan etterkome deler av informasjonskrava ved å ha ei personvernerklæring.

Personvernforordninga pålegg kommunen å utpeike eit personvernombod, jf. artikkel 37 nr.1. Artikkel 38 regulerer stillingstilhøva for personvernombodet, og det går mellom anna fram der at kommunen skal sikre at personvernombodet blir involvert i rett tid i alle spørsmål som gjeld vern av personopplysningar (nr. 1), at kommunen skal stille tilstrekkeleg ressursar til rådighet for at personvernombodet kan gjennomføre oppgåvene pålagt stillinga i personvernforordninga artikkel 38 (nr. 2), at personvernombodet skal vere uavhengig og rapportere direkte til rådmannen (nr. 3), og at personvernombodet er bunde av teieplikt (nr. 5).

Personvernombodet sine lovpålagte oppgåver går fram av artikkel 39. Her går det fram at personvernombodet mellom anna skal kontrollere at personvernforordninga blir overholdt (bokstav b), gi råd om vurdering av personvernkonsensar (bokstav c), og samarbeide med Datatilsynet (bokstav d).

<sup>55</sup> Regjeringa.no: Veileder til eForvaltningsforskriften. Første del: eForvaltningsforskriften: Elektronisk samhandling med og i forvaltningen av Rolf Riisnæs, advokat dr. juris.: <https://www.regjeringen.no/no/dokumenter/veileder-til-eforvaltningsforskriften/id2425012/>

Forordninga stiller vidare krav til kva avvik som skal meldast til Datatilsynet. Hovudregelen slik denne går fram i artikkel 33 er at alle avvik som skuldast brot på personopplysningstryggleiken (utilsikta sletting, tap, endring, ulovleg spreiding av eller tilgang til personopplysningar som er overført, lagra eller på anna måte handsama, jf. artikkel 4 punkt 12), skal meldast til Datatilsynet innan 72 timar. Artikkel 33 nr. 3 stiller krav til kva avviksmeldingane skal innehalde. Artikkel 34 stiller nærare krav om kva vilkår som må vere oppfylt for at kommunen ikkje skal melde i frå om personopplysningstryggleiksbrotet til den eller dei registrerte som avviket gjeld. Jf. artikkel 33 punkt 5, skal kommunen dokumentere alle avvik, og kva tiltak som er sett i verk.

Artikkel 30 nr. 1 i personvernforordninga stiller krav om at kommunen skal føre ein protokoll over behandlingsaktivitetane av personopplysningar som blir utført. Forordninga stiller nærare krav til innhaldet i denne protokollen, som t.d. namn og kontaktopplysning på den behandlingsansvarlege (bokstav a), føremålet med behandlinga (bokstav b), ei skildring av kategoriane av registrerte og kategoriane av personopplysningar (bokstav c). Nr. 3 i artikkelen stiller krav om at protokollen skal vere skriftleg og nr. 4 seier at protokollen skal gjerast tilgjengeleg for Datatilsynet dersom dei ber om det.

Forordninga stiller i tillegg krav om at det i nokre situasjonar skal gjerast risikovurderingar av behandlinga av personopplysningar. I artikkel 35 nr. 1, står det at:

Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for personopplysningsvernet.

Dette er eit krav om at kommunen skal gjennomføre ei vurdering av personvernkonsekvensane av behandling av personopplysningar der slik behandling medfører høg risiko for rettar og fridom for fysiske personar. Jf. artikkel 39 om personvernombodet sine oppgåver, skal vedkomande gi råd om vurdering av personvernkonsekvensar og kontrollere gjennomføringa av denne dersom kommunen ber om det.

### Kompetanse

Som nemnd er kommunen gjennom eForvaltningsforskrifta § 15 forplikta til å ha ein internkontroll basert på anerkjende standardar for styringssystem for informasjonstryggleik. Departementet har peika ut Digitaliseringsdirektoratet (Digdir) som ansvarleg for å gje tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast, og Digdir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001. Kapittel 7.2 i standarden seier at kommunen skal:

- a) fastslå hvilken kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonens styring, og som påvirker dens informasjonssikkerhetsprestasjon;
- b) sikre at disse personene har kompetanse tilegnet gjennom passende utdanning, opplæring eller erfaring;
- c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere virkningen av tiltakene som er truffet; og
- d) oppbevare relevant dokumentert informasjon som bevis på kompetanse.

I merknaden til punkt 7.2, står det at «Aktuelle tiltak kan for eksempel omfatte å sørge for opplæring, veiledning eller omplassering av nåværende ansatte eller innleie av eller kontraktinngåelse med kompetente personer.»

Datatilsynet sin rettleiar Internkontroll og informasjonssikkerhet<sup>56</sup> omhandlar mellom anna oppfølging og opplæring. Her går det fram at målet med brukaropplæring er å syte for at brukarane er merksame på trugslar mot personvernet og informasjonstryggleiken generelt, og at dei er gitt høve til å etterleve dette i sitt daglege arbeid. Opplæringa bør vere tilpassa dei ulike målgruppene sitt behov for opplæring og fordelast over tid. Brukarane bør få opplæring i rutinar, tryggleiksprosedyrar og riktig bruk av informasjonssystem for å redusere potensielle risikoar.

I tillegg til tilrådinga om opplæring av tilsette som følgjer av ISO-standarden, kan ein utleie eit krav om opplæring og kjennskap til system, rutinar og regelverk blant tilsette frå kommunelova § 25-1, som seier at kommunedirektøren skal «ha internkontroll med administrasjonens virksomhet for å sikre at lover og forskrifter følges» Dette inneber at kommunen må ha eit system for internkontroll på plass for å sikre forsvarleg saksbehandling. Eit sentralt tiltak i eitkvart internkontrollsystem vil vere at det er på plass tilstrekkeleg opplæring til at dei tilsette er i stand til å gjennomføre sine arbeidsoppgåver i samsvar med lover, krav og forventningar.

<sup>56</sup> Internkontroll og informasjonssikkerhet. Datatilsynet. Publisert 23.06.2018. Sist endra 30.10. 2018. <https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/>

### **Anna regelverk**

I tillegg til krava i personvernforordninga og eForvaltningsforskrifta er det også fleire andre reglar knytt til informasjonstryggleik som er relevant for kommunen. Krava i desse regelverka er i nokon grad overlappende med krava til eit styringssystem for informasjonstryggleik.

I helseregisterlova er det gitt konkrete føringar knytt til behandlinga av helseopplysningar, og her kjem det mellom anna fram konkrete krav knytt til informasjonstryggleik (§ 16). Det er utarbeidd ein norm for informasjonstryggleik i helse-, omsorgs- og sosialsektoren (Norma), som stiller krav med utgangspunkt i både personopplysningsforskrifta og helseregisterlova. I Norma er det også innarbeidd ulike krav knytt til teieplikt og informasjonsrett etter særlovgeving for kommunehelsetenester, sosialtenester, psykisk helsevern, samt forvaltnings- og offentlegheitslov.

Kommunen er også omfatta av sikkerheitslova, og har som følge av dette plikt til å ha forsvarleg informasjonstryggleik for informasjon som kan vere kritisk for å forhindre truslar som spionasje, sabotasje og terrorhandlingar. Desse krava kan vere relevante for kommunen for eksempel når det gjeld å beskytte vassforsyninga frå forureining av drikkevatt.

# Vedlegg 5: Sentrale dokument og litteratur

## Lov og forskrift

- Lov om behandling av personopplysninger (personopplysningsloven).
- Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften).

## Førearbeider, rundskriv, rettleiarar mv.

- Diverse rettleiingsmateriell frå Digitaliseringsdirektoratet
- Diverse rettleiingsmateriell frå Datatilsynet

## Dokument frå kommunen

- Tysnes kommune. *Handbok i informasjonssikkerhet*. 2022. Ikkje datert
- Tysnes kommune. *IKT-strategi i Tysnes kommune 2022-2025*. Ikkje datert
- Tysnes kommune. *Årsmelding 2021*. 31.03.2021.
- Tysnes kommune. *Agresso UBW – instruks for behandling av elektroniske document*. Ikkje datert.
- Tysnes kommune. *Cosdoc – instruks for behandling av elektroniske arkivdokument*. Ikkje datert.
- Tysnes kommune. *DIPS – Sosial – instruks for behandling av elektroniske system tysnes.arkivplan.no*. Ikkje datert.
- Tysnes kommune. *ESA – instruks for behandling av elektroniske dokument tysnes.arkivplan.no*. Ikkje datert.
- Tysnes kommune. *GIS – Line instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *HelseCERT – Avtale om deltakelse i HelseCERTs nasjonalt beskyttelsesprogram*. 20.01.2023.
- Tysnes kommune. *HelseCERT – Informasjon om Nasjonalt Beskyttelsesprogram*. Ikkje datert.
- Tysnes kommune. *HelseCERT – Skjema – Deltakelse i nasjonalt beskyttelsesprogram*. 20.01.2023.
- Tysnes kommune. *HelseCERT Sårbarhetsoversikt*. Ikkje datert.
- Tysnes kommune. *Infrastruktur – informasjonstryggleik*. Ikkje datert.
- Tysnes kommune. *Krisehandtering IT – eksterne ressursar – eksterne som kan yta akutt hjelp*. Ikkje datert.
- Tysnes kommune. *Medlemskap i HelseCERT*. 20.01.2023.
- Tysnes kommune. *Sjekklister forbehandling av personopplysningar*. 20.01.2023.
- Tysnes kommune. *Skjema for tildeling av brukarar i fagsystem*. Ikkje datert.
- Tysnes kommune. *Visma flyktning – instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *Visma Flyt Barnehage – Tysnesbarnehagane – instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *Visma Flyt skule – Tysnes skule – instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *Visma Flyt skule – Uggdal skule – instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *Visma Flyt skule – Onarheim skule – instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *ROS-analyse IKT*. Datert 27.01.2023.
- Tysnes kommune. *DPIA provesvar*. Datert 03.11.2020.
- Tysnes kommune. *DPIA klinikermelding*. Datert 20.09.2021.
- Tysnes kommune. *DPIA Vaksine*. Datert 03.11.2020.
- Tysnes kommune. *DPIA Digisos*. Datert 20.09.2021.
- Tysnes kommune. *DPIA Fiks min kommune*. Datert 10.12.2020
- Tysnes kommune. *DPIA Smittevern*. Datert 15.05.2020.
- Tysnes kommune. *DPIA analyse for fiks smittesporing*. Datert 15.05.2020.
- Tysnes kommune. *DPIA Innreiseoppfølging*. Datert 08.06.2021
- Tysnes kommune. *DPIA Fiks vaksinestatus*. Datert 21.09.2021



- Tysnes kommune. *DPIA Fiks del dokument*. Datert 09.03.2022
- Tysnes kommune. *GDPR kartlegging CosDoc*. Datert 2018.
- Tysnes kommune. *GDPR kartlegging Shiftmanager*. Datert 2018.
- Tysnes kommune. *GDPR kartlegging flyktning (VISMA)*. Datert 16.01.2023.
- Tysnes kommune. *GDPR kartlegging Infodoc.*. Datert 24.01.2023.
- Tysnes kommune. *GDPR kartlegging sosial*. Datert 16.01.2023.
- Tysnes kommune. *UNIT4 ERP Managed Cloud Sikkerhetsdokument*. Datert 21.11.2022.
- Tysnes kommune. *Databehandlaravtaler – tysnes.arkivplan.no*. Ikkje datert.
- Tysnes kommune. *Avtale om løpende tjenestekjøp over internett*. Ikkje datert.
- Tysnes kommune. *Databehandleravtale for PatientSky*. Ikkje datert.
- Tysnes kommune. *Databehandleravtale for EVA Admin*. Ikkje datert.
- Tysnes kommune. *Oppdatering av databehandleravtale Infodoc*. Datert 13.09.2022.
- Tysnes kommune. *Tinging av brukarident*. Ikkje datert.
- Tysnes kommune. *Introduksjonsprogram for nytilsette*. Datert 12.12.17.
- Tysnes kommune. *Atea: Antivirus og Wsus*. Ikkje datert.
- Tysnes kommune. *Atea si vurdering av IT-systemet i Tysnes kommune*. Ikkje datert.
- Tysnes kommune. *Overordna IT beredskapsplan – Tysnes kommune*. Datert 13.10.2010.



Deloitte AS and Deloitte Advokatfirma AS are the Norwegian affiliates of Deloitte NSE LLP, a member firm of Deloitte Touche Tohmatsu Limited ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see [www.deloitte.no](http://www.deloitte.no) for a more detailed description of DTTL and its member firms.

Deloitte Norway conducts business through two legally separate and independent limited liability companies; Deloitte AS, providing audit, consulting, financial advisory and risk management services, and Deloitte Advokatfirma AS, providing tax and legal services.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries and territories serves four out of five Fortune Global 500® companies. Learn how Deloitte's 330,000 people make an impact that matters at [www.deloitte.no](http://www.deloitte.no).

© 2024 Deloitte AS