



## Møteinnkalling

<b>Utval:</b>	Tysnes kommune, Kontrollutvalet
<b>Møtestad:</b>	Rådhuset, Onarheim
<b>Dato:</b>	05.10.2023
<b>Tid:</b>	10:00

Dersom nokon av medlemmene ikkje kan møte og må melde forfall, vert dei bedne om å gjere dette så tidleg som råd er ved **å ringa** til Helge Inge Johansen tlf. 402 03 664 eller til Hogne Haktorson, tlf. 911 05 982.

Til varamedlemar er denne innkallinga å sjå på som ei orientering.  
Dersom det vert aktuelt at varamedlemar må møta, vil det bli gjeve nærmare beskjed.

Lorentz Lunde  
kontrollutvalsleiar

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
seniorrådgjevar

*Dokumentet er godkjent elektronisk og har difor ingen handskriven underskrift*

Kopi: Vararepresentantar til kontrollutvalet  
Ordførar  
Revisor  
Rådmann

## Sakliste

Utvals-saknr	Innhald	Arkiv-saknr	U.Off
	Godkjenningssaker		
GK 5/23 GK 6/23	Godkjenning av innkalling og sakliste Godkjenning av møteprotokoll frå møte 11.05.2023 Politiske saker	2022/106	
PS 15/23	Forvaltningsrevisjon av informasjonstryggleik og personvern - revisjonsrapport	2022/324	
PS 16/23	Forvaltningsrevisjon av Plan- og byggesakshandsaming - oppfølging av handlingsplan	2022/208	
PS 17/23	Rekneskapsrevisjon - oppfølging av revisjonsrapport nr.11 - orientering frå rådmann	2022/96	
PS 18/23	Rådmann orienterer om etikk og misleg framferd i Tysnes kommune	2022/100	
PS 19/23	Kontrollutvalet si rolle i varslingsaker	2023/413	
PS 20/23	Vurdering av om Deloitte er uavhengig i høve Tysnes kommune	2022/98	
PS 21/23	Revisjonsplan og risikovurdering i samband med etterlevingskontroll av økonomiforvaltninga i 2023	2022/96	
PS 22/23	Plan for forvaltningsrevisjon for perioden 2024-2028 - Bestilling av prosjektplan	2023/406	
PS 23/23	Plan for eigarskapskontroll for perioden 2024-2028 - Bestilling av prosjektplan	2023/407	
PS 24/23	Budsjett 2024 for kontrollutvalet	2022/101	
PS 25/23	Gjennomgang av møteprotokollar frå andre politiske utval	2022/102	
PS 26/23	Evaluering av arbeidet i kontrollutvalet i denne perioden	2022/108	
PS 27/23	Eventuelt	2022/95	
PS 28/23	Konkurransetsetting av revisjonstenester - forslag til konkurransgrunnlag Referat saker	2023/371	
RS 3/23	VS: FKT Medlemsinfo juni 2023	2022/109	
RS 4/23	VS: Reglement for kontrollutvalet for valperioden 2023 - 2027	2022/108	
RS 5/23	VS: Valg og opplæring av kontrollutvalg for perioden 2023– 2027	2022/109	



## **GK 5/23 Godkjenning av innkalling og sakliste**



Tysnes kommune

## Sekretariat for kontrollutvalet

---

Saksframlegg

---

**Saksnr:** 2022/106-13  
**Saksbehandlar:** Helge Inge Johansen

---

### Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	6/23	05.10.2023

### Godkjenning av møteprotokoll frå møte 11.05.2023

Møteprotokoll frå møte 11.05.2023 er vedlagt saka

**Møteprotokoll**

<b>Utval:</b>	Kontrollutvalet
<b>Møtestad:</b>	Rådhuset, Møterom Lunde
<b>Dato:</b>	11.05.2023
<b>Tid:</b>	10:00 - 11:30

**Følgjande faste medlemmer møte:**

Namn	Funksjon	Representerer
Lorentz Lunde	Leiar	KRF

**Følgjande medlemmer hadde meldt forfall:**

Namn	Funksjon	Representerer
Britt Ersvær	Nestleiar	AP
Lars Heine Kåsa	Medlem	SP
Kåre Haugland	Medlem	FRP
Sigvard Michael Madsen	Medlem	H

**Følgjande varamedlemmer møte:**

Namn	Møtte for	Representerer
Helge Hauge	Lars Heine Kåsa	SP
Egil Bjarne Berge	Sigvard Michael Madsen	H

**Andre som møte:**

Namn	Stilling
Steinar Dalland	Rådmann
Rolf Johan Lunde	Økonomisjef
Helena Winkel Hildershavn	Rekneskapsrevisor, Deloitte AS
Kjersti Gjuvsland	Forvaltningsrevisor, Deloitte AS
Helge Inge Johansen	Spesialrådgjevar, Vestland fylkeskommune

Lorentz Lunde  
utvalsleiar

Helge Inge Johansen  
utvalssekretær

*Dokumentet er godkjent elektronisk og har difor inga handskriven underskrift*

## Sakliste

<b>Utvals- saknr</b>	<b>Innhald</b>	<b>Arkiv- saknr</b>	<b>U.Off</b>
	<b>Godkjenningssaker</b>		
GK 3/23	Godkjenning av innkalling og sakliste		
GK 4/23	Godkjenning av møteprotokoll frå møte 09.02.2023	2022/106	
	<b>Politiske saker</b>		
PS 10/23	Årsmelding og årsrekneskap 2022 for Tysnes kommune - Uttale frå kontrollutvalet	2022/96	
PS 11/23	Forvaltningsrevisjon av informasjonstryggleik og personvern - statusrapportering	2022/324	
PS 12/23	Innkjøp av revisjonstenester - ny konkurranse - fullmakt til kontrollutvalet	2023/371	
PS 13/23	Gjennomgang av møteprotokollar frå andre politiske utval	2022/102	
PS 14/23	Eventuelt	2022/95	

## **Godkjenningsaker**

### **GK 3/23 Godkjenning av innkalling og sakliste**

#### **Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet**

##### **Behandling i møte**

Det kom ingen merknader til innkalling eller saklista.

##### **Vedtak**

Innkalling og sakliste vart samrøystes godkjent.

### **GK 4/23 Godkjenning av møteprotokoll frå møte 09.02.2023**

#### **Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet**

##### **Behandling i møte**

Det var ingen merknad til protokoll frå møte 09.02.2023.

##### **Vedtak**

Møteprotokoll frå møte 09.02.2023 vart samrøystes vedteke.

## **Politiske saker**

### **PS 10/23 Årsmelding og årsrekneskap 2022 for Tysnes kommune - Uttale frå kontrollutvalet**

#### **Forslag til vedtak**

1. Kontrollutvalet vedtek utkast til uttale om Tysnes kommune sin årsrekneskap og årsmelding for 2022.
2. På bakgrunn av det som kjem fram i revisjonsrapport nr. 11 frå Deloitte AS ber kontrollutvalet om at rådmann kjem i møte 05.10.2023 for å gjera greie for kva som vil bli gjort i høve tilrådingane i rapporten
3. Kontrollutvalet tek resultatet etter etterlevingskontrollen til orientering.

#### **Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet**

##### **Behandling i møte**

Rådmann og økonomisjef orienterte om årsrekneskapen 2022 og svarte på spørsmål frå kontrollutvalet.



Rekneskapsrevisor orienterte om revisjonsmelding, revisjonsrapport og rapport etter forenkla etterlevingskontroll.

Forslag til vedtak vart samrøystes vedteke.

### **Vedtak**

1. Kontrollutvalet vedtek utkast til uttale om Tysnes kommune sin årsrekneskap og årsmelding for 2022.
2. På bakgrunn av det som kjem fram i revisjonsrapport nr. 11 frå Deloitte AS ber kontrollutvalet om at rådmann kjem i møte 05.10.2023 for å gjera greie for kva som vil bli gjort i høve tilrådingane i rapporten
3. Kontrollutvalet tek resultatet etter etterlevingskontrollen til orientering.

### **PS 11/23 Forvaltningsrevisjon av informasjonstryggleik og personvern - statusrapportering**

#### **Forslag til vedtak**

Informasjonen vert teken til orientering.

### **Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet**

#### **Behandling i møte**

Forvaltningsrevisor orienterte om status i arbeid med forvaltningsrevisjonen.

- litt forseinka med intervjuprosessen
- har send ut spørjeundersøking men noko låg svarprosent - vil sende ut på ny med ny frist

Sekretær orienterte om at neste møte i kontrollutvalet er 05.10.2023. Deloitte har noko betre tid her ut i frå den opprinelege fristen for overlevering av rapport vart satt til 15.08.2023.

Forslag til vedtak var samrøystes.

### **Vedtak**

Informasjonen vert teken til orientering.

### **PS 12/23 Innkjøp av revisjonstenester - ny konkurranse - fullmakt til kontrollutvalet**

#### **Forslag til innstilling**

1. Kommunestyret gir kontrollutvalet fullmakt til å gjennomføra ny konkurranse om val av revisor for Tysnes kommune. Tidsramma må leggjast slik at den som vert vald ut frå konkurransen, er revisor f.o.m. 01.07.2024.
2. Fullmakta omfatter gjennomføring av heile prosessen, herunder:
  - Utarbeiding og godkjenning av tilbodsokument
  - Knytte til seg naudsynt hjelp.
  - Vurdere mottekne tilbod og innstilla overfor kommunestyret på val av revisor.

### **Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet**

#### **Behandling i møte**

Sekretær orienterte kort om saka.

Forslag til innstilling vart samrøystes vedteke.

#### **Innstilling**

1. Kommunestyret gir kontrollutvalet fullmakt til å gjennomføra ny konkurranse om val av revisor for Tysnes kommune. Tidsramma må leggjast slik at den som vert vald ut frå konkurransen, er revisor f.o.m. 01.07.2024.
2. Fullmakta omfatter gjennomføring av heile prosessen, herunder:
  - Utarbeiding og godkjenning av tilbodsokument
  - Knytte til seg naudsynt hjelp.
  - Vurdere mottekne tilbod og innstilla overfor kommunestyret på val av revisor.

### **PS 13/23 Gjennomgang av møteprotokollar frå andre politiske utval**

#### **Forslag til vedtak**

Kontrollutvalet tar møteprotokollane som går fram av saksutgreiinga til orientering.

### **Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet**

#### **Behandling i møte**

Møteprotokollane vart gjennomgått, det kom ikkje fram noko spesielt ved gjennomgang av møteprotokollane.

Forslag til vedtak vart samrøystes vedteke.

#### **Vedtak**

Kontrollutvalet tar møteprotokollane som går fram av saksutgreiinga til orientering.

## PS 14/23 Eventuelt

### Forslag til vedtak

Saka vert lagt fram utan forslag til vedtak.

## Saksprotokoll 11.05.2023 - Tysnes kommune, Kontrollutvalet

### Behandling i møte

#### Henvending - Ørjan Lavik - tomt i vågsmarka

Kontrollutvalet, sekretær og forvaltningsrevisor diskuterte saka slik det kjem fram av eposten som vart sendt frå utvalsleiar 10.05.2023.

Kontrollutvalet diskuterte saka ut i frå gjeldande retningslinjer for kontrollutvalet som vart vedteke av kontrollutvalet i møte 13.10.2022.

Henvendinga er ikkje ei sak for kontrollutvalet, då kontrollutvalet ikkje er eit klageorgan i forvaltningssaker. Kontrollutvalet avviser saka.

Vedtaket vart samrøystes vedteke

### Vedtak

Henvendinga gjeldande Ørjan Lavik - tomt i Vågsmarka er avvist grunna at dette ikkje er ei sak for kontrollutvalet.



---

Saksframlegg

---

**Saksnr:** 2022/324-8  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	15/23	05.10.2023

## Forvaltningsrevisjon av informasjonstryggleik og personvern - revisjonsrapport

### Forslag til innstilling

Kommunestyret ber rådmannen om å:

1. Sørge for å etablere styringssystem for informasjonstryggleik som tilfredsstiller krav i regelverket og som er basert på anerkjend standard på området. Under dette mellom anna:
  - a) Sikrar at tryggleiksstrategi og internkontroll inkluderer relevante krav fastsett i lov, forskrift eller instruks,
  - b) 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,
  - c) Sikrar at det er etablert nødvendige rutinar og retningslinjer knytt til arbeidet med informasjonstryggleik i kommunen,
  - d) Etablere system for kontroll og etterprøving av informasjonstryggleik i kommunen og sikrar at dette blir gjennomført jamleg
2. Sørge for at det vert gjennomført eigna tekniske og organisatoriske tiltak for å sikre vedvarande konfidensialitet og integritet i behandlingssystema som blir nytta i kommunen. Under dette mellom anna:
  - a) Etablere tilstrekkeleg system og rutinar som sikrar riktig nivå av tilgjenge og konfidensialitet i alle informasjonssystema som blir nytta i kommunen
  - b) Sikrar at etablerte rutinar og retningslinjer for tilgangsstyring er tilgjengelege for alle relevante tilsette
3. Sørge for at kommunen si personvernerklæring er lett tilgjengeleg og ha tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane, i samsvar med krav om dette i regelverket

4. Sørge for at det blir utarbeidd protokoll over behandlingsaktivitetar av personopplysningar, og at det er i samband med gjennomføring av risikovurderingar også systematisk blir gjort vurderingar av personvernrisikoar
5. Sørge for 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
6. Sørge for at retningslinjer for informasjonstryggleik tydeleg skildrar krav, oppfølging av meldte avvik på området, og særskilt krav når det gjeld melding av avvik til Datatilsynet
7. Sørge for å få oversikt over kva kompetanse det er behov for hos leiarar og tilsette i arbeid med informasjonstryggleiksarbeidet i kommunen
8. Sørge for at det vert etablert 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
9. Kontrollutvalet ber og om at det vert laga ein prioritert handlingsplan til første møte i 2024, som viser kva tiltak som skal setjast i verk for å følgja opp tilrådinga i rapporten, når tiltaka skal setjast i verk og kven som skal ha ansvaret for iverksettinga. Prioritert handlingsplan vert å senda sekretariatet innan 15.01.2024.

### Samandrag

Kontrollutvalet bestilte forvaltningsrevisjon av informasjonstryggleik og personvern i møte 24.11.2022, og kontrollutvalet skal handsama rapporten i dette møte. Kontrollutvalet skal gje innstilling til kommunestyret som skal fatte endeleg avgjerd i saka. Forslag til innstilling i saksframlegget byggjer på forslag i rapporten. På bakgrunn av dette vert det tilrådd at kontrollutvalet innstiller på at kommunestyret ber rådmannen om å koma med tilbakemelding på revisjonsrapporten.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

### Vedlegg

- 1 Rapport etter forvaltningsrevisjon av informasjonstryggleik og personvern i Tysnes kommune

## Saksutgreiing

### Bakgrunn for saka

Kontrollutvalet bestilte i møte 24.11.2022 (PS 22/22) ny forvaltningsrevisjon:

«Vedtak:

1. *Kontrollutvalet ber Deloitte AS gjennomføra forvaltningsrevisjon av informasjonstryggleik og personvern.*
2. *Kontrollutvalet godkjenner samla timetal, inkl. opsjon, i forslag til prosjektplan.*
3. *Kontrollutvalet ønskjer at revisjonsrapporten vert ferdig innan 15.08.2023 verifisert og inkludert rådmannen sin uttale.»*

### Av prosjektplanen går det fram at føremålet med forvaltningsrevisjonen er:

Føremålet med prosjektet vil vere å undersøke om kommunen har tilfredsstillande system og rutinar for informasjonstryggleik og om etablerte standardar og gjeldande lovar og reglar blir etterlevd innan dette området. Videre er det eit føremål å undersøke i kva grad Tysnes kommune etterlever sentrale krav i personvernlovgjevinga.

### Med bakgrunn i prosjektet sitt føremål har revisjonen formulert følgjande problemstillingar:

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 klåre 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 personvernlovgjevinga?
  - 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?

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse for å gjennomføre forvaltningsrevisjonen. Når revisjonsrapport er levert og behandla i kontrollutvalet, skal utvalet innstille til kommunestyret, som gjer vedtak, jf. kommunelova § 23-3.

### Vurderingar og verknader

Prosjektet er utført i samsvar med gjeldande standard for forvaltningsrevisjon (RSK 001). Deloitte har i revisjonen nytta dokumentanalyse, intervju, spørjeundersøking og verifiseringsprosessar. Revisjonen er gjennomført i tidsrommet januar 2023 til september 2023.

**I kapitel 6 Konklusjon og tilrådingar i rapporten (s. 40 – 42), kjem blant anna revisjonen med slik informasjon:**

Tysnes kommune har nyleg starta arbeidet med å etablere system og rutinar for arbeidet med informasjonstryggleik og personvern. Kommunen etablerte mellom anna handbok i informasjonssikkerheit og IKT-strategi 2022-2025 i 2022.

Arbeidet med å implementera rutinar og system var framleis 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.

Tysnes kommune har ikkje etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegrer:

- Styrande dokument er ikkje fullt ut i samsvar med krav i regelverket,
- Ikkje tilstrekkeleg grad etablert tydelege ansvarsforhold knytt til informasjonstryggleik,
- Ikkje etablert tilstrekkelege rutinar knytt til informasjonstryggleik,
- Ikkje etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik,
- Ikkje etablert tilstrekkeleg system eller kontrollar som sikrar tilgjenge og konfidensialitet i informasjonssystema,

Tysnes kommune etterlever ikkje alle sentrale krav i personvernlovgevinga som er undersøkt:

- Kommunen har utnemnt eit personvernombod, men berre i 15 % Stilling
- Kommunen har etablert personvernerklæring, men denne erklæringa er ikkje tilstrekkeleg klar og tydeleg, og heller ikkje lett tilgjengeleg.
- Kommunen gjennomfører ikkje i tilstrekkeleg grad protokoll over behandlingsaktivitetar av personopplysningar
- Kommunen gjennomfører ikkje i tilstrekkeleg grad risikovurderingar av handsaming av personopplysningar
- Kommunen har sikra oversikt over avvik knytt til personvern, men ikkje i tilstrekkeleg grad etablert retningslinjer som sikrar tilfredsstillande oppfølging av meldte avvik

Tysnes kommune har betringspotensiale når det gjeld å sikre at tilsette har tilstrekkeleg kompetanse om informasjonstryggleik:

- Kommunen har ikkje etablert tilstrekkeleg rutinar for å sikre at tilsette får opplæring i informasjonstryggleik
- Kommunen sine tilsette ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik
- Kommunen ikkje i tilstrekkeleg grad etterlever retningslinjer og rutinar for informasjonstryggleik

**Rådmannen har gjeve uttale til revisjonsrapporten på s. 43 i rapporten:**

*«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 det 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!»*

**Basert på det som kjem fram i undersøkinga tilrår revisjonen at kommunen set i verk følgjande tiltak:**

1. Etablerer styringssystem for informasjonstryggleik som tilfredsstillar krav i regelverket og som er basert på anerkjend standard på området. Under dette mellom anna:
  - a) sikrar at tryggleiksstrategi og internkontroll inkluderer relevante krav fastsett i lov, forskrift eller instruks.
  - b) 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.
  - c) sikrar at det er etablert nødvendige rutinar og retningslinjer knytt til arbeidet med informasjonstryggleik i kommunen.
  - d) 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 krav oppfølging av meldte avvik på området, og særskilt krav når det gjeld melding av avvik til Datatilsynet (t.d. når det gjeld 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

**Konklusjon**

Forslag til innstilling i saksframlegget, byggjer på forslag i rapporten. På bakgrunn av dette vert det tilrådd at kontrollutvalet innstiller på at kommunestyret ber rådmannen om å kome med tilbakemelding på revisjonsrapporten etter ei stund, i form av ein prioritert handlingsplan.





## Forvaltningsrevisjon | Tysnes kommune Informasjonstryggleik og personvern

September 2023

«Forvaltningsrevisjon av  
informasjonstryggleik og personvern»

September 2023

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.

**Tysnes kommune har ikkje etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner.**

- Kommune sine **styrande dokument er ikkje fullt ut i samsvar med krav i regelverket**. Det går vidare fram av undersøkinga at styrande dokument ikkje viser til anerkjende standardar eller konkret regelverk på området.<sup>1</sup> Dette er ikkje i samsvar med krav til internkontroll på informasjonstryggleiksområdet (jf. § 15 i eForvaltningsforskrifta).
- Tysnes kommune har **ikkje i tilstrekkeleg grad etablert tydelege ansvarsforhold knytt til informasjonstryggleik**. Undersøkinga indikerer at det står att ein del arbeid med å sikre at rollar og ansvar knytt til arbeidet med informasjonstryggleik og personvern er tilstrekkeleg tildelt og kommunisert. Revisjonen påpeiker at det er øvste leing sitt ansvar å sikre at ansvar og rollar er tildelt og kommunisert, og understrekar vidare at dette er viktig for å sikre at kommunen etterlever regelverket og anerkjende standardar på området.
- Tysnes kommune har **ikkje 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 er ferdigstilt. Revisjonen understrekar at kommunen skal sikre at internkontrollen er systematisk og at det er etablert nødvendige rutinar og prosedyrar.
- Tysnes kommune har **ikkje etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik**. Revisjonen merkar seg at kommunen er i prosess med å utarbeide prosedyrar mv. for gjennomføring av kontroll og etterprøving av informasjonstryggleik, men påpeiker likevel at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta § 15 eller tilrådingar i ISO/IEC 27001 knytt til oppfølging og kontroll.
- Tysnes kommune har **ikkje etablert tilstrekkeleg system eller kontrollar som sikrar tilgjenge og konfidensialitet i informasjonssystema** som blir nytta i kommunen. Revisjonen meiner at kommunen med fordel burde samle og gjere tilgjengeleg felles retningslinjer og rutinar for tilgangsstyring i 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. Undersøkinga indikerer at kommunen ikkje har tilstrekkeleg felles system og tilgjengelege retningslinjer for dette arbeidet i alle elektroniske system i kommunen, og det er dermed 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 ikkje i samsvar med krav for informasjons- og personopplysningstryggleik, jf. personvernforordninga artikkel 32 nr. 1.

**Tysnes kommunen etterlever ikkje alle sentrale krav i personvernlovgevinga som er undersøkt**

- **Kommunen har utnemnt eit personvernombod**, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at rolla som personvernombodet er ein redusert stilling (15 prosent), og at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Det går vidare fram at personvernombodet i liten grad opplever å 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.

<sup>1</sup> Digdir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001 ved utarbeiding av styringssystem for informasjonstryggleik.

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.** Samtidig har kommunen ikkje sikra at denne erklæringa har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane. Kommunen si personvernerklæring er vidare ikkje tilstrekkeleg lett tilgjengeleg, i samsvar med krav om dette i regelverket (artikkel 12 i personvernforordninga).
- **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, men 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).
- **Kommunen gjennomfører ikkje i tilstrekkeleg grad risikovurderingar av handsaming av personopplysningar,** og det blir heller ikkje i samband med risikovurderingar systematisk 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 personvernkonsvensar ved behandling av personopplysningar med høg risiko, jf. personvernforordninga artikkel 35.
- Tysnes kommune har ved innføring av elektronisk avviksmeldesystem **sikra oversikt over avvik knytt til personvern.** Kommunen har samtidig **ikkje i tilstrekkeleg grad etablert retningslinjer som sikrar tilfredsstillande oppfølging av meldte avvik** knytt til informasjonstryggleik. Undersøkinga viser at det ikkje går konkret fram av handbok i informasjonstryggleik eller andre rutinar kven som skal melde få 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 understrekar at personvernforordninga er tydeleg på at den behandlingansvarlege (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).
- Undersøkinga viser at det førekjem i kommunen at det blir lagra sensitiv informasjon om tilsette og innbyggjarar på område der uvedkommande har innsyn, og at det også har blitt meldt avvik på dette. Dette ikkje er i samsvar med krav i personvernforordninga som seier at kommunen skal gjennomføre eigna tekniske og organisatoriske tiltak for å mellom anna sikre vedvarande konfidensialitet og integritet i behandlingssystema og -tenestene (artikkel 32, første ledd, bokstav b).
- Svare 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 påpeiker at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta. Revisjonen vurderer at kommunen sin avvikspraksis ikkje er i samsvar med tilrådingane i ISO/IEC 27001 eller generelle prinsipp for god internkontroll.

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

- Tysnes kommune har **ikkje etablert tilstrekkeleg rutinar for å sikre at tilsette får opplæring i informasjonstryggleik..** Revisjonen påpeiker 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.
- Funna i spørjeundersøkinga viser at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Svar i spørjeundersøkinga indikerer vidare at det relativt store skilnadar mellom sektorane i kommunen når det gjeld kjennskap til styrande dokument for informasjonstryggleik. Revisjonen understrekar 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. 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 (ISO/IEC 27001, punkt 5.2).

- Kommunen etterlever ikkje i tilstrekkeleg grad retningslinjer og rutinar for informasjonstryggleik. Undersøkinga indikerer mellom anna at dokument med fortruleg informasjon ikkje alltid blir lagra på ein sikker måte og/eller blir oppbevart slik at uvedkomande kan få innsyn.

## 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>2</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 føresett.

**Behandlingsansvarleg:** Den behandlingsansvarlege er etter regelverket mellom anna ansvarleg for å behandle personopplysningar på en 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 identifikasjonsnummer, lokaliseringsopplysningar, ein nettidifikator 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, fagforeiningsmedlemskap, 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>3</sup>

<sup>2</sup> Digitaliseringsdirektoratet (Digdir): Informasjonssikkerhet – en forutsetning for å nå virksomhetens mål:

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

<sup>3</sup> Det store norske leksikon: Datasikkerhet: <https://snl.no/datasikkerhet>

# Innhald

1	Innleiing	7
2	Organisering av arbeidet med informasjonstryggleik	9
3	Styringssystem for informasjonstryggleik	10
4	Etterleving av krav i personvernlovgevinga	19
5	Kompetanse blant tilsette	29
6	Konklusjon og tilrådingar	40
	Vedlegg 1 : Høyringsuttale	43
	Vedlegg 2 : Revisjonskriterier	44
	Vedlegg 3 : Sentrale dokument og litteratur	47

# Detaljert innhald

1	Innleiing	7
1.1	Bakgrunn	7
1.2	Føremål og problemstillingar	7
1.3	Avgrensing	7
1.4	Metode	7
1.4.1	Dokumentanalyse	7
1.4.2	Intervju	7
1.4.3	Spørjeundersøking	8
1.4.4	Verifiseringsprosessar	8
1.5	Revisjonskriterier	8
2	Organisering av arbeidet med informasjonstryggleik	9
2.1	Organisering	9
3	Styringssystem for informasjonstryggleik	10
3.1	Problemstilling	10
3.2	Revisjonskriterier	10
3.3	Styrande dokument for informasjonstryggleik	11
3.3.1	Datagrunnlag	11
3.3.2	Vurdering	12
3.4	Rutinar og ansvarsforhold	13
3.4.1	Datagrunnlag	13
3.4.2	Vurdering	15
3.5	System for og gjennomføring av kontroll og etterprøving av informasjonstryggleik	16
3.5.1	Datagrunnlag	16
3.5.2	Vurdering	18
4	Etterleving av krav i personvernlovgjevinga	19
4.1	Problemstilling	19
4.2	Revisjonskriterier	19
4.3	Personvernombod og personvernerklæring	20
4.3.1	Datagrunnlag	20
4.3.2	Vurdering	22
4.4	Protokoll over behandlingsaktivitetar	22
4.4.1	Datagrunnlag	22
4.4.2	Vurdering	23
4.5	Risiko- og konsekvensvurderingar av behandling av personopplysingar	23
4.5.1	Datagrunnlag	23
4.5.2	Vurdering	24
4.6	Oversikt over avvik knytt til personvern	25
4.6.1	Datagrunnlag	25
4.6.2	Vurdering	27
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	43
	Vedlegg 2 : Revisjonskriterier	44
	Vedlegg 3 : Sentrale dokument og litteratur	47

## Figurar

Figur 1: Administrativ organisering av Tysnes kommune	9
Figur 2: Kjennskap til ansvar og oppgåver knytt til informasjonstryggleik i eiga rolle	15
Figur 3: Kjennskap til kommunen sitt personvernombod	21
Figur 4: Informasjonstryggleiksavvik meldt mellom juni 2022 og august 2023 (Kjelde: Tysnes kommune)	25
Figur 5: Melding om opplevde informasjonstryggleiksavvik	27
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	8
Tabell 2: Strategiar for innsatsområdet personvern og informasjonssikring (Kjelde: Tysnes kommune)	11
Tabell 3: Rolle- og ansvarsdeling knytt til informasjonstryggleik i Tysnes kommune	13



# 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 er innarbeidd i rapporten. Høyringsutkast av rapporten er sendt til rådmannen for uttale, og uttale frå rådmannen sin høyringsuttale er å finne i vedlegg 1 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 ISO/IEC 27001. Kriteria er summert opp innleiingsvis under kvart tema, og presentert utfyllande i vedlegg 2 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).

Jamfør punkt tre over, er Digitaliseringsdirektoratet (Digdir) peika ut som ansvarleg for å gi tilrådingar knytt til kva styringssystem for informasjonstryggleik som bør nyttast. Digdir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001<sup>4</sup>, som er ein internasjonal standard for styringssystem for informasjonstryggleik.<sup>5</sup> I denne standarden går det mellom anna fram følgjande tilrådingar:

- verksemda synleggjer leiinga si haldning til informasjonstryggleik, og med dette etablerer ein tydleg «tone på toppen».
- Leiinga sjølv deltar aktivt i styringsaktivitetane i leiinga si styring og oppfølging.
- leiinga peiker ut eller tilset nokre på verksemdsnivå som skal vere pådrivar og støtte til leiinga og organisasjonen elles i informasjonstryggleiksarbeidet. Det blir understreka at det viktigaste er at rollar og ansvar for informasjonstryggleik er godt definert og at nødvendige ressursar til reell innsats på informasjonstryggleiksområdet er avsett. Ressursbehovet vil vere avhengig av verksemda sin storleik, kompleksitet og tilgjengeleg kompetanse.
- verksemda bør i tillegg peike ut ein pådrivar i kvar avdeling eller på tilsvarende organisatorisk nivå, avhengig av verksemda sin storleik og organisering.

<sup>4</sup> ISO/IEC 27001 er utarbeidd for å stille krav til etablering, implementering, vedlikehald og kontinuerleg forbetring av eit leiingssystem for informasjonstryggleik.

<sup>5</sup> Digdir påpeiker i eigen rettleiar om ISO/IEC 27001 at *pålegget* er å basere seg på anerkjende standardar og at *tilrådinga* er å basere seg på gjeldande versjon av ISO/IEC 27001. Offentlege verksemder er dermed ikkje pålagd å vere i samsvar med standarden.

- Dei nemnte funksjonane på verksemdsnivå og avdelingsnivå kan med fordel utgjere ei samla pådrivargruppe for informasjonstryggleik i verksemda.

Sjå vedlegg 2 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>6</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 lydoptak 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. Handboka viser heller ikkje eksplisitt til krav i regelverk, og det er ikkje vist til anerkjende rammeverk på området. Ingen av dei intervjua kjenner til den tilrådde standarden ved utarbeiding av styringssystem (ISO/IEC 27001) eller i kva grad kommunen etterlever denne

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 leggast 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.
<b>Leggja til rette for å gje innbyggjaren 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 medføre 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.

<sup>6</sup> Tysnes kommune. *Handbok i informasjonssikkerhet for Tysnes kommune*. 2022.

<b>Syta for rett sikkerheitsnivå og oppdaterte sikkerheitsrutinar</b>	<p>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.</p> <p>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.</p> <p>Kommunen må til ei kvar tid ha gode nok tryggleiksrutinar og bruke sikringsløysingar som sikrar for at informasjonen berre når autoriserte personar.</p>
<b>Gjennomføra organisatoriske tiltak for å vareta personvern og informasjonssikkerhet</b>	<p>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.</p>
<b>Bevisstgjera og gje opplæring</b>	<p>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.</p>
<b>Sikra moderne og effektive løysingar for å vareta informasjonstryggleik</b>	<p>Kommunen må tilpassa seg kontinuerleg teknologisk utvikling ved å implementera moderne og effektive løysingar som kan handtere kommande tryggleiksutfordringar.</p>

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 eigne 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 ikkje fullt ut 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). Revisjonen vil samtidig påpeike at dei styrande dokumenta ikkje i tilstrekkeleg grad skildrar system for kontinuerleg forbetring av leiinga si styring av informasjonstryggleiken (til dømes gjennomføring av tryggleiksrevisjonar) og undersøkinga indikerer også at leiinga si styring av informasjonstryggleik ikkje i tilstrekkeleg grad er 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 styrande dokument ikkje viser til standardar eller konkret regelverk på området.<sup>7</sup> Regelverket set krav til at tryggleiksstrategi skal inkludere relevante krav som er fastsett i lov, forskrift eller instruks og at internkontroll på informasjonstryggleiksområdet skal basere seg på anerkjente standardar for styringsystem for informasjonstryggleik (eForvaltningsforskrifta § 15). 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 kommunen i det vidare arbeidet med

<sup>7</sup> Digidir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001 ved utarbeiding av styringsystem for informasjonstryggleik.

å implementere eit heilskapleg styringssystem for informasjonstryggleik, må sikre at systemet er i samsvar med anerkjende standardar på området, i samsvar med krav til dette i regelverket.

### 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 etablera 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</li> </ul>

		<p>utarbeidast ROS analysar ved nye system eller større endringar i eit fagsystem.</p> <ul style="list-style-type: none"> <li>• Ansvarleg for at tilsette har undertekna 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 forsvareleg forvaltning av informasjonen i fagsystema/IT-systema.</li> <li>• Ansvar å utarbeida risikoanalyse.</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 innføringa 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.

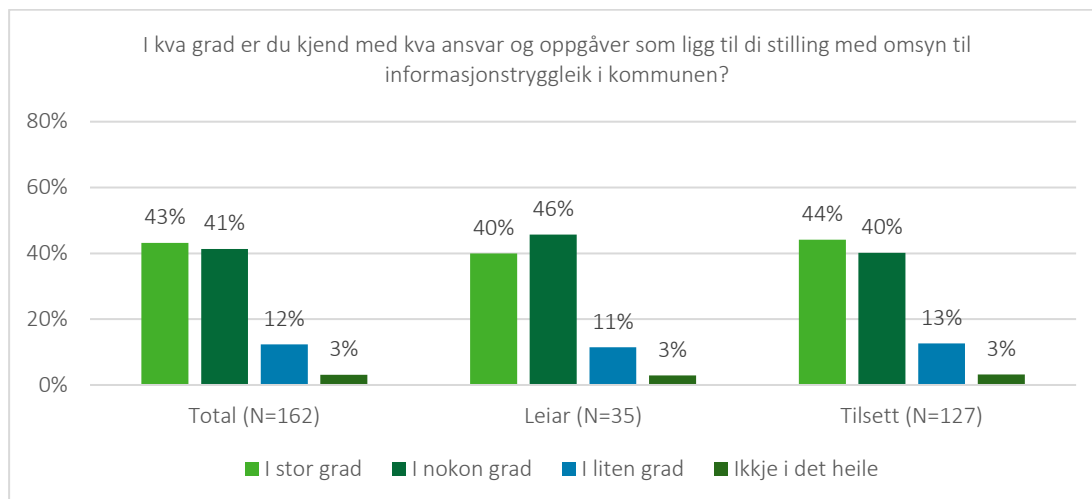
Det blir vist til at kommunen gjer vurderingar om internkontrollsystem innan personvern og informasjonstryggleik er tilstrekkeleg. Til dømes blir det vist til at kommunen har registrert at andre kommunar har meir omfattande rolleskildringar på dette området, og at kommunen med bakgrunn i dette vil vurdere 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 fellestenester 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>8</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>9</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 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

<sup>8</sup> Tysnes kommune. Compilo: Støtteprosessar. GDPR/personvern.

<sup>9</sup> Tysnes kommune. Tinging av brukarident. Ikkje datert.

informasjonstryggleiksarbeidet. Undersøkinga indikerer samtidig at det står att ein del arbeid med å sikre at rollar og ansvar i dette arbeidet er tilstrekkeleg tildelt og kommunisert. Revisjonen vil påpeike at det er øvste leiing sitt ansvar å sikre at ansvar og rollar er tildelt og kommunisert, og vidare understreke at dette er viktig for å sikre at kommunen etterlever regelverket og anerkjende standardar på området.<sup>10</sup>

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

<sup>10</sup> NS-ISO/IEC 27001. Informasjonsteknologi, sikringsteknikker, ledelsessystemer for informasjonssikkerhet, krav.

<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.

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 fellestene 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 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.

<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.

### 3.5.2 Vurdering

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik. Undersøkinga viser at kommunen har sett seg mål om at det skal gjennomførast kontrollar gjennom leiinga sin årlege gjennomgang og jamlege tryggleiksrevisjonar, men at dette ikkje ennå er gjennomført. Revisjonen merkar seg at kommunen er i prosess med å utarbeide prosedyrar mv. for gjennomføring av kontroll og etterprøving av informasjonstryggleik og at kommunen etter planen vil gjennomføre første runde med leiinga sin gjennomgang i 2023. 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.

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg system eller kontrollar som sikrar tilgjenge og konfidensialitet i informasjonssystema som blir nytta i kommunen. Undersøkinga viser at det er etablert system for at IT-leiar godkjenner bestilling av tilgang for brukarar av nokre, men ikkje alle, kommunen sine system. Revisjonen merkar seg vidare at det gjennom kommunen sin arkivplan er utarbeidd nokre instruksar og skjema som skal sikre at brukarar av nokre av systema kommunen nyttar har riktige og oppdaterte tilgangar. Revisjonen meiner at kommunen med fordel burde samle og gjere tilgjengeleg felles retningslinjer og rutinar for tilgangsstyring i 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. Undersøkinga indikerer at kommunen ikkje har tilstrekkeleg felles system og tilgjengelege retningslinjer for dette arbeidet i alle system i kommunen, og revisjonen vurderer at det derfor er 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 ikkje i samsvar med krav for informasjons- og personopplysningstryggleik, jf. personvernforordninga artikkel 32 nr. 1.

# 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 2 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

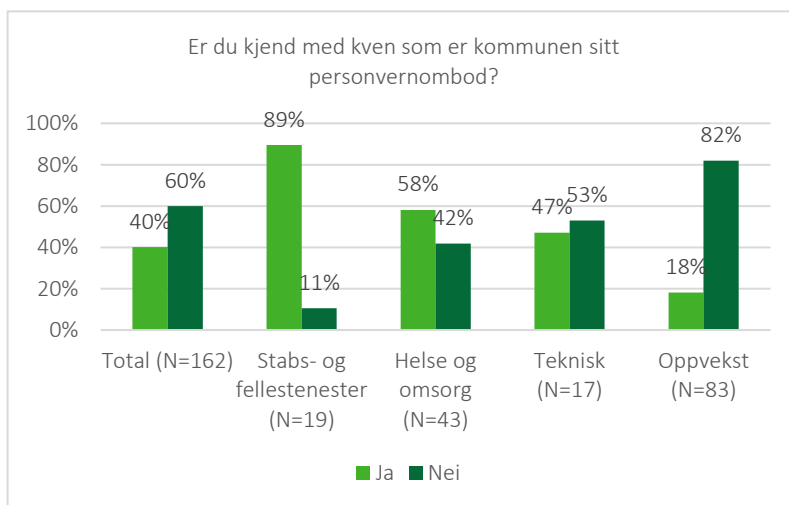
<sup>16</sup> Tysnes kommune. Personvernombod. Ikkje datert

<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 rolla som personvernombodet er ein redusert stilling (15 prosent), og 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 rådigheit 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 støttmateriell. 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.tplbbpjumwumi%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

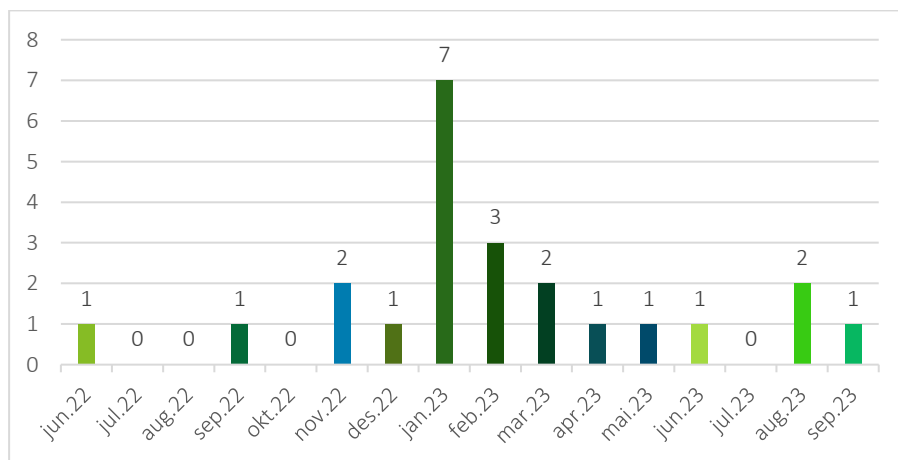
Tysnes kommune omtalar melding av avvik knytt til informasjonstryggleik og personvern i handbok i informasjonssikkerhet. I kapittel 3 om informasjonstryggleik for leiarar går det fram at alle tilsette skal ha kjennskap til korleis avvik skal registrerast i Compilo. Det går vidare fram i same kapittel 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 avviksmeldesystem, 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.

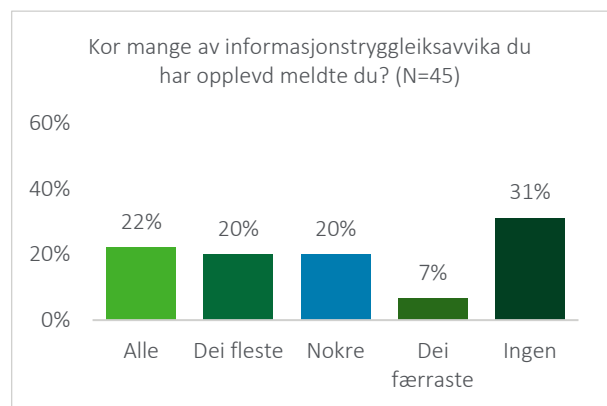
#### 4.6.2 Vurdering

Tysnes kommune har ved innføring av elektronisk avviksmeldesystem sikra oversikt over avvik knytt til personvern. Revisjonen vurderer samtidig at kommunen ikkje i tilstrekkeleg grad har etablert retningslinjer som sikrar tilfredsstillande oppfølging av meldte avvik knytt til informasjonstryggleik. Undersøkinga viser at det ikkje går konkret fram av handbok i informasjonstryggleik eller andre rutinar 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 førekjem i kommunen at det blir lagra sensitiv informasjon om tilsette og innbyggjarar på område der uvedkommande har innsyn, og at det også har blitt meldt avvik på dette. I avviket som er meldt var tilfelle at helsepersonell frå både legekontor, helsestasjon og psykisk helseteneste hadde tilgang til mapper med personsensitiv informasjon. Revisjonen vurderer at dette ikkje er i samsvar med krav i personvernforordninga som seier at kommunen skal gjennomføre eigna tekniske og organisatoriske tiltak for å mellom anna sikre vedvarande konfidensialitet og integritet i behandlingssystema og -tenestene (artikkel 32, første ledd, bokstav b). Revisjonen vil i samband med dette påpeike at verksemda også må tilgjengeleggjere helseopplysningar på ein måte som varetar krava til informasjonstryggleik. Tilgangsstyring skal også gi helsepersonell tilgang til *nødvendige* helseopplysningar ut frå eit tenestleg behov og samtidig hindre uautorisert bruk og ugrunna innsyn i opplysningar.<sup>34</sup>

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

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/>

<sup>34</sup> Direktoratet for e-helse. Veileder for tilgang til helse- og personopplysninger.

avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta. Revisjonen vurderer at kommunen sin avvikspraksis ikkje er i samsvar med tilrådingane i ISO/IEC 27001 eller generelle prinsipp for god internkontroll.

# 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 baserer styringssystem for informasjonstryggleik på ISO/IEC 27001.

Kommunen bør:

- a) fastslå kva kompetanse som er nødvendig for personen(e) som utfører arbeid under organisasjonen si styring, og som påverkar organisasjonen sin informasjonstryggleiksprestasjon;
- b) sikre at desse personane har kompetanse tileigna gjennom passande utdanning, opplæring eller erfaring;
- c) der det er relevant, treffe tiltak for å erverve nødvendig kompetanse og evaluere verknaden av tiltaka som er treft; og
- d) oppbevare relevant dokumentert informasjon som bevis på kompetanse (ISO/IEC 27001:2022, punkt 7.2).

Sjå vedlegg 2 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.

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

- o opplæring i aktuelle fagprogram og rutinar knytt til bruken av system
- o kunnskap om innhaldet i informasjonssikkerhetshandboka

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 grunnleggande 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 grunnleggande 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 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 (t.d. ISO/IEC 27001, punkt 7.2). Dette gjer at det er høgare sannsyn for at dei tilsette ikkje har tilstrekkeleg kompetanse innan

<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.



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

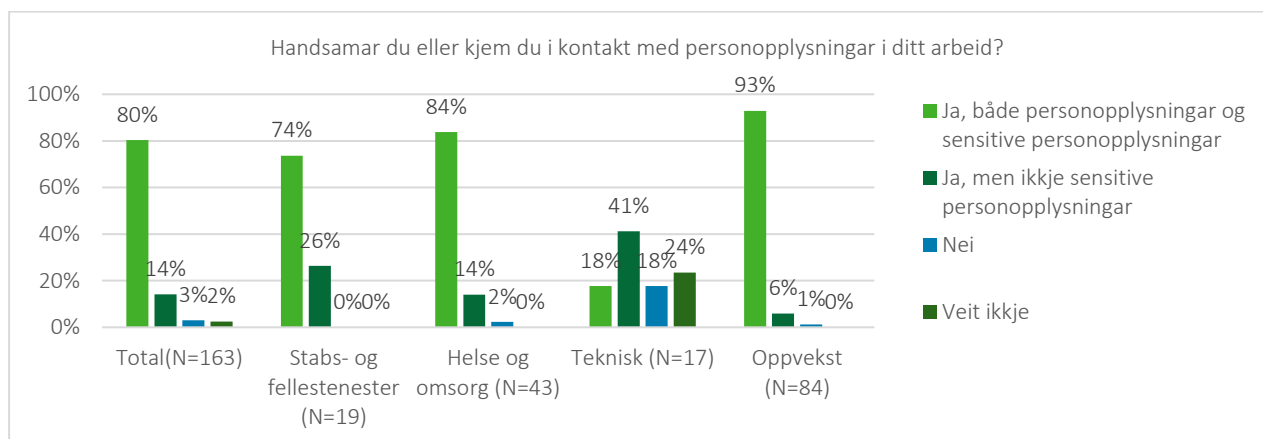
### 5.4.1 Datagrunnlag

#### 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



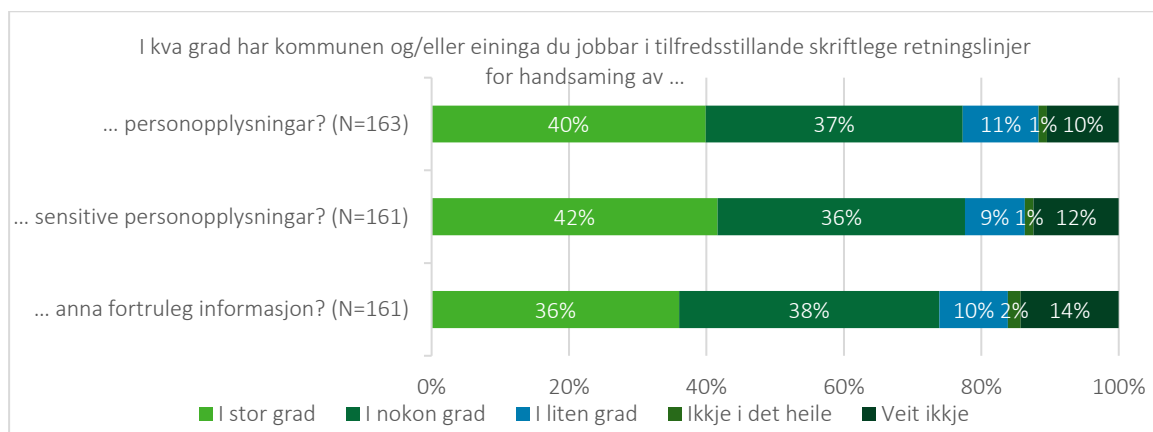
Respondentane blei også stilt spørsmål om dei handsamar anna *fortruleg informasjon*.<sup>40</sup> Her svara om lag 80 prosent *ja* og 11 prosent *nei*, medan 9 prosent svarar «veit ikkje». Fordelinga mellom sektorane er på dette spørsmålet relativt likt som svara framstilt i figuren over.

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.

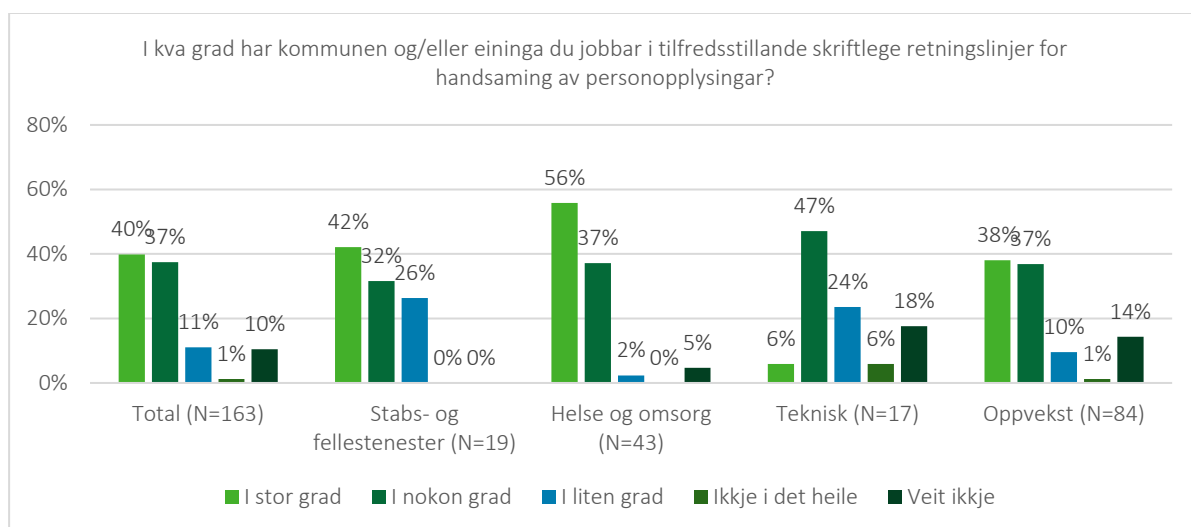
<sup>40</sup> I spørjeundersøkinga var det lagt inn ei forklaring på kva som er meint med fortruleg informasjon. Sjå elles ordliste på side 3 i rapporten

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.

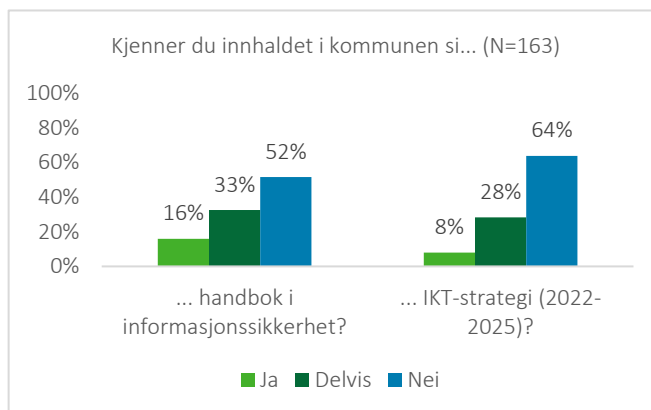
Respondentane som svarta at kommunen og/eller eininga «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer på områda som nemnt over, fekk eit oppfølgingsspørsmål om dei veit kvar dei finn rutinar og retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og/eller 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

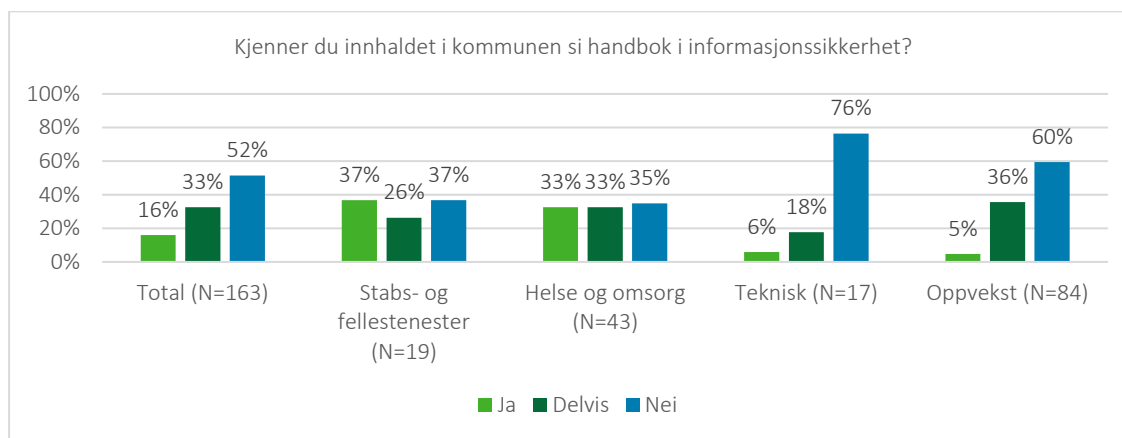


Ved nærare analyse går det fram at det er skilnad på svara frå respondentane på dette spørsmålet på bakgrunn av både kva sektor dei jobbar innan og om dei er tilsett med leiaransvar eller ikkje. Medan om lag ein av tre (34 prosent) tilsette med leiaransvar svarar at dei *ikkje* kjenner til innhaldet 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 sektortilhøyrse



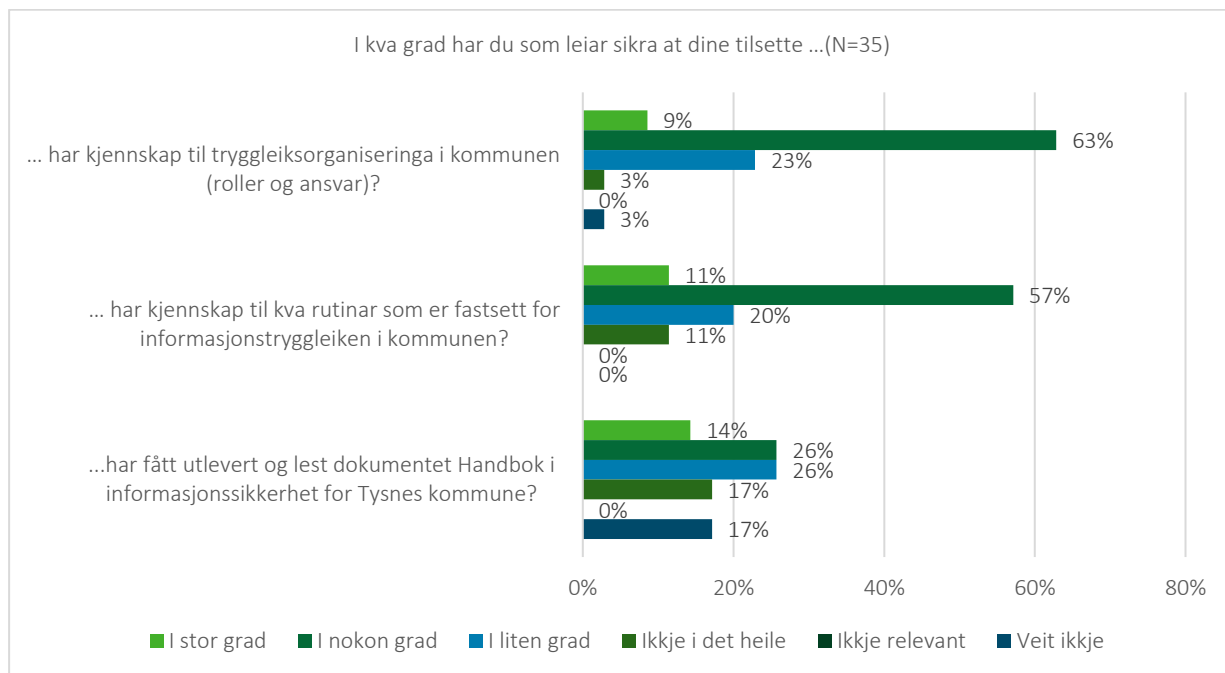
I spørjeundersøkinga svarar 17 prosent<sup>42</sup> av respondentane med leiaransvar at dei «ikkje i det heile» har sikra at dei tilsette har fått utlevert og lest handbok i informasjonssikkerhet, medan 26 prosent svarar at dei høvesvis «i liten grad» eller «i nokon grad» har sikra dette. 14 prosent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

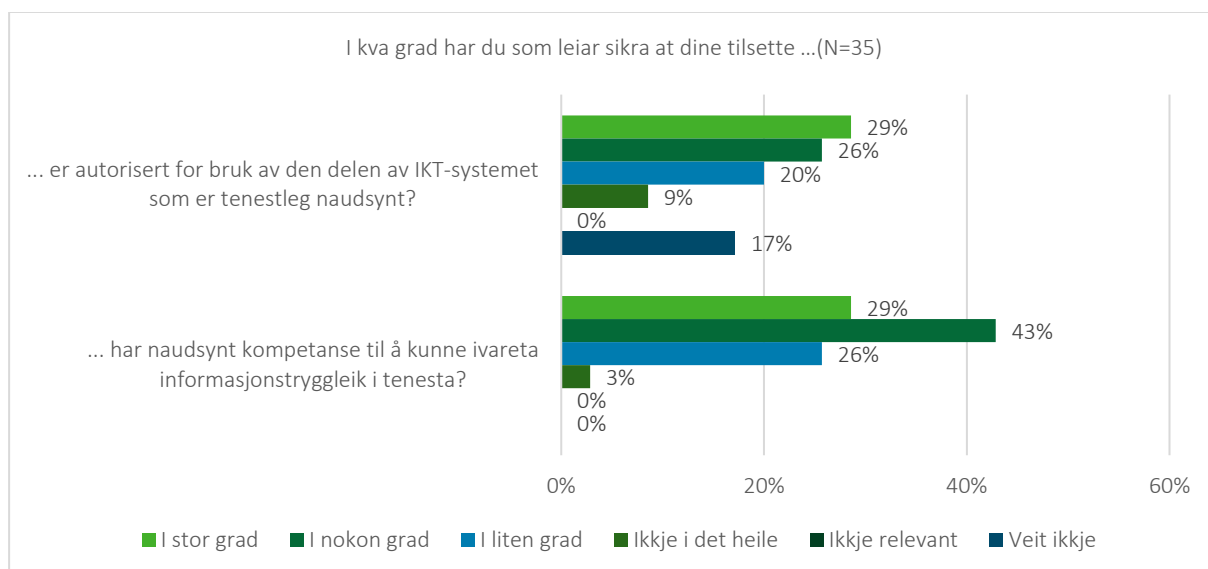
<sup>43</sup> 4 respondentar

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



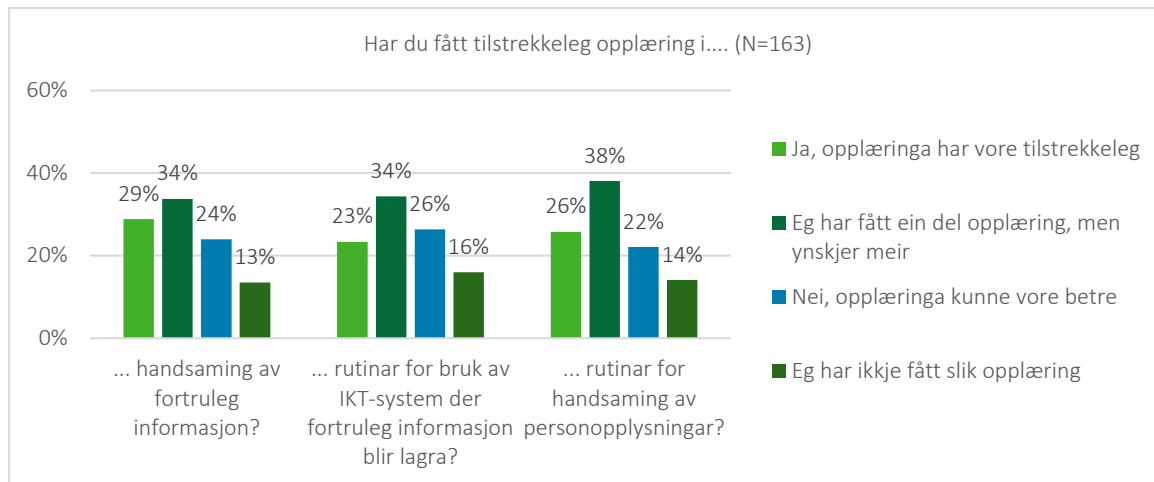
Alle respondentane fekk vidare spørsmål om dei har fått tilstrekkeleg opplæring i 1) handsaming av fortruleg informasjon, 2) rutinar for bruk av IKT-system der fortruleg informasjon blir lagra og 3) rutinar for handsaming av personopplysningar. Som framstilt i figuren under svarar om lag ein av fire 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 %

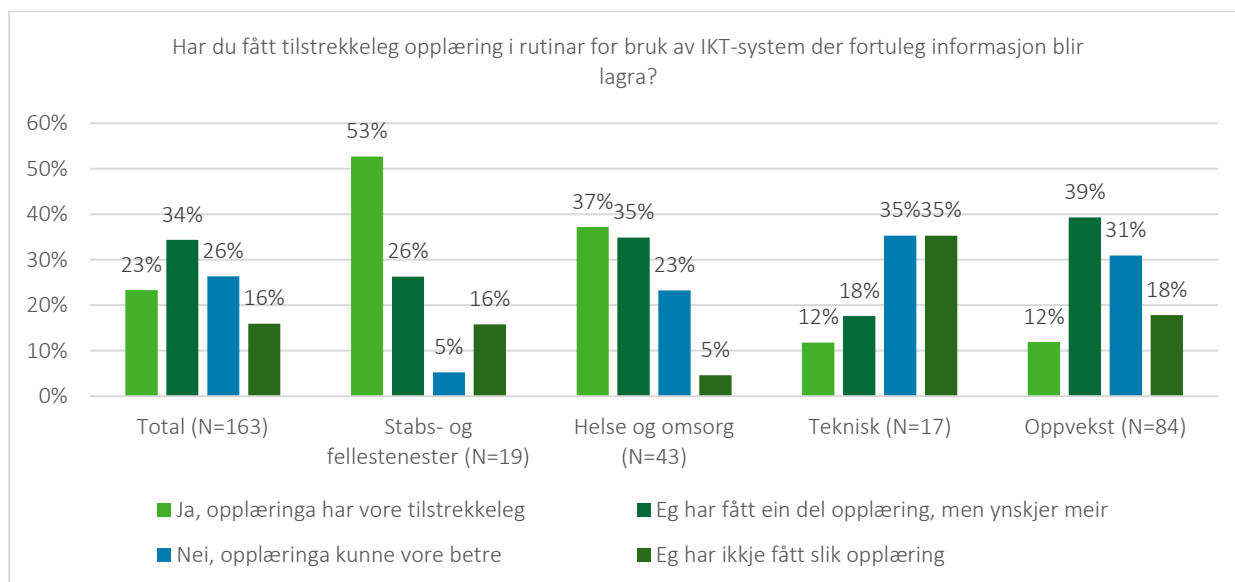
gjeld opplæring i rutinar for handsaming av personopplysningar, så svarar 38 prosent av respondentane at dei har fått ein del opplæring men ønsker meir.

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



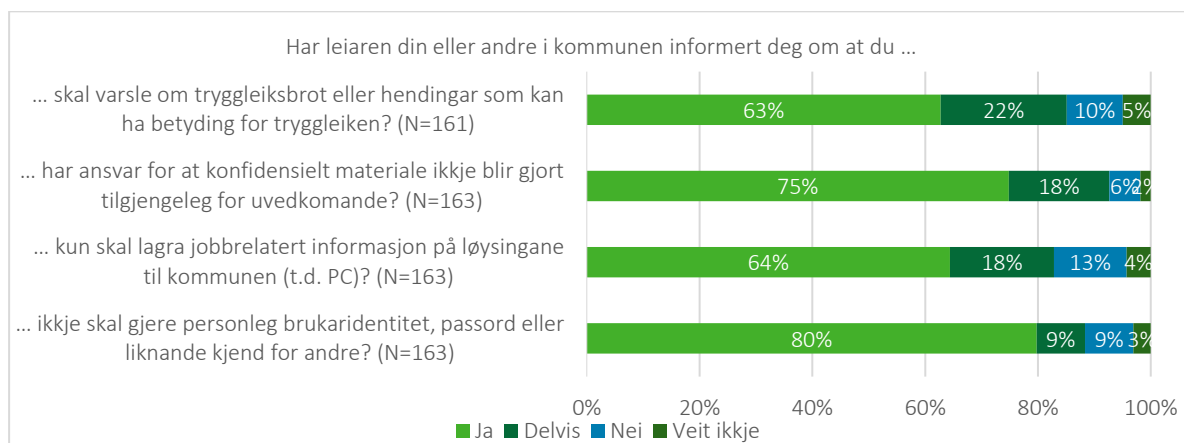
Dei respondentane som *ikkje* svarta «ja, opplæringa har vore tilstrekkeleg» på dei tre spørsmåla om opplæring framstilt i figur 13 over, fekk eit ope oppfølgingsspørsmål der dei fekk svare på kva opplæring knytt til informasjonstryggleik og/eller bruk av IKT-system dei saknar. 57 av respondentane har 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



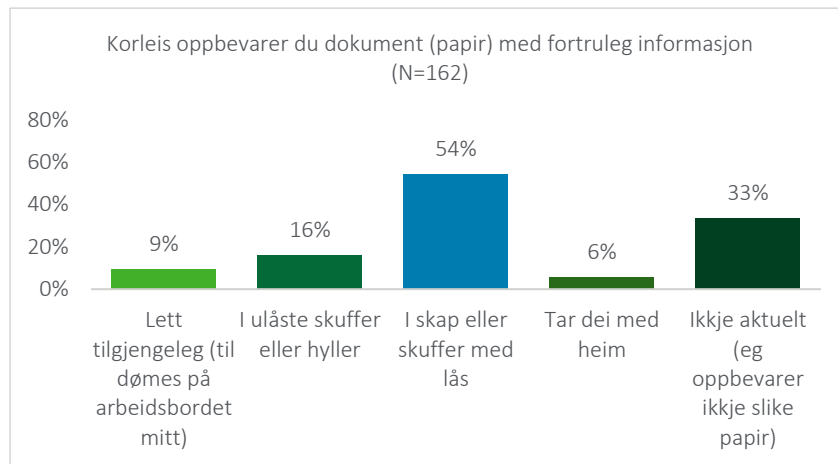
### Etterleving av retningslinjer og rutinar for informasjonstryggleik

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.

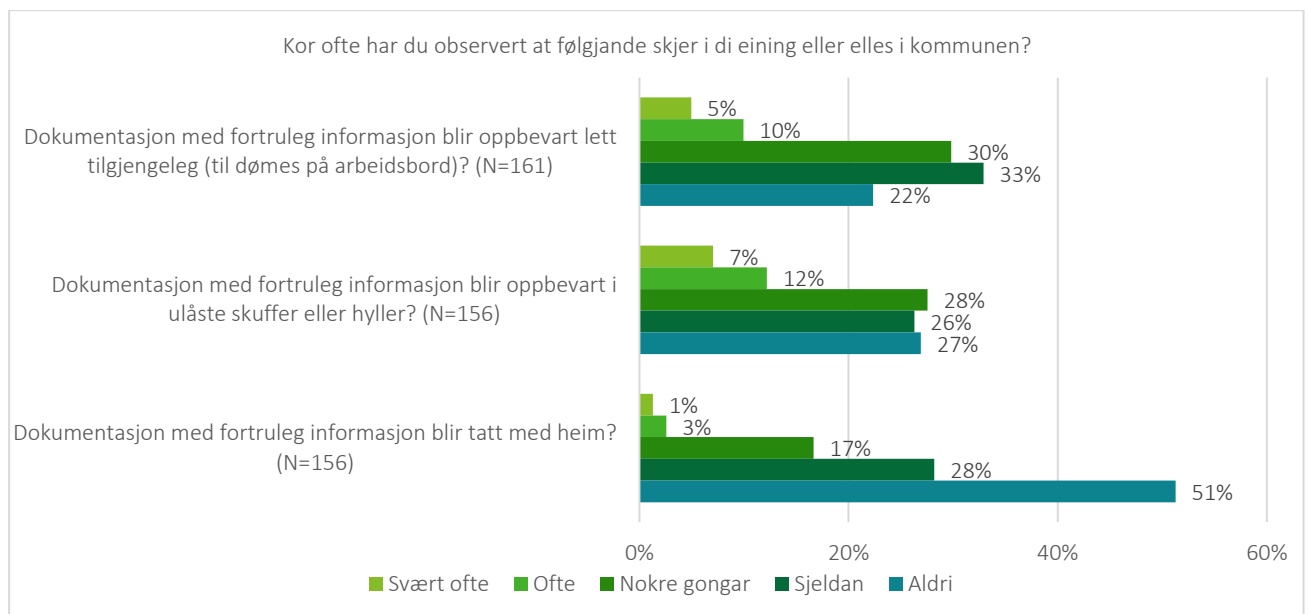
Figur 16: Oppbevaring av dokument med fortruleg informasjon



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 med fortruleg informasjon 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 informasjonstryggleiksbrot



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).

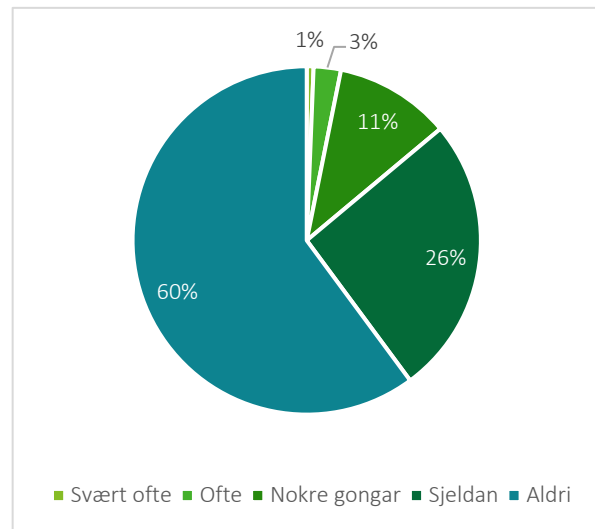
<sup>46</sup> N=154

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.

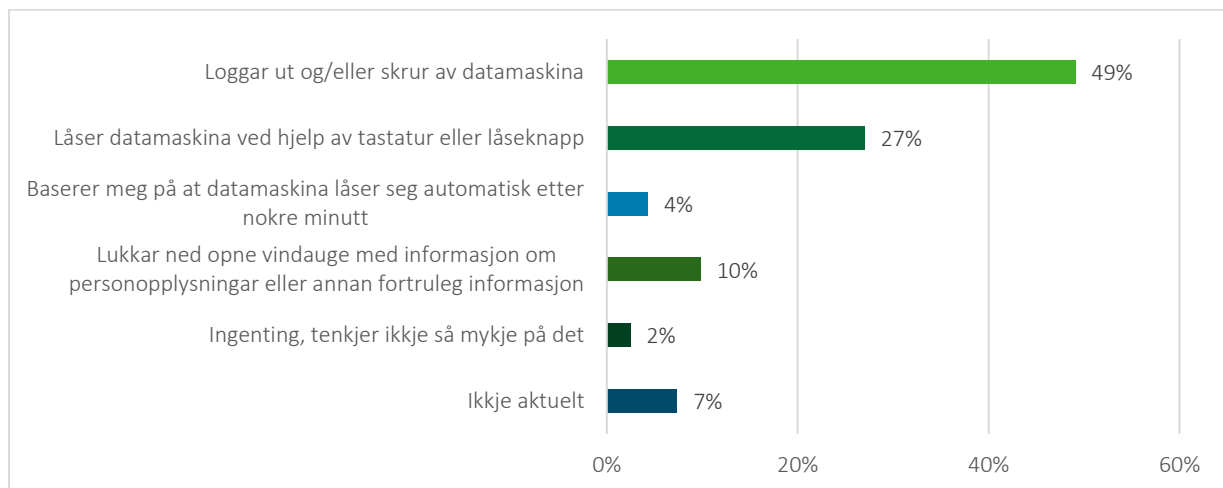
Respondentane blei også spurt om eigne vanar på dette området. Hovuddelen av respondentane svarar «nei» på spørsmålet om dei nokon gong har lånt ut brukarnamn og passord til andre (88 prosent), men 12 prosent svarar at dei har gjort dette. 7 prosent av dei som svarar at dei har lånt ut brukarnamn og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



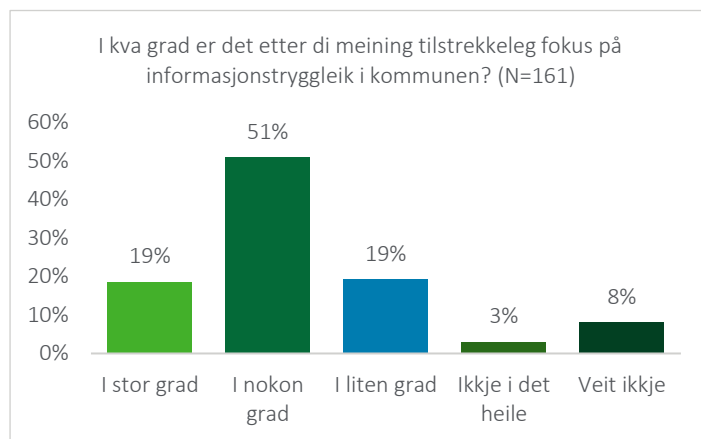
Figur 19: Kva gjer du vanlegvis når du i løpet av arbeidsdagen går frå PC-en du nyttar? (N=163)



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 leggast 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 (ISO/IEC 27001, punkt 5.2).

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 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:

**Tysnes kommune har ikkje etablert styringssystem for informasjonstryggleik som tilfredsstillar krav i sentrale føresegner.**

- Kommune sine **styrande dokument er ikkje fullt ut i samsvar med krav i regelverket**. Undersøkinga viser at styrande dokument ikkje viser til standardar eller konkret regelverk på området.<sup>47</sup> Dette er ikkje i samsvar med krav til internkontroll på informasjonstryggleiksområdet (jf. § 15 i eForvaltningsforskrifta).
- Tysnes kommune har **ikkje i tilstrekkeleg grad etablert tydelege ansvarsforhold knytt til informasjonstryggleik**. Undersøkinga indikerer at det står att ein del arbeid med å sikre at rollar og ansvar knytt til arbeidet med informasjonstryggleik og personvern er tilstrekkeleg tildelt og kommunisert. Revisjonen påpeiker at det er øvste leiing sitt ansvar å sikre at ansvar og rollar er tildelt og kommunisert, og understrekar vidare at dette er viktig for å sikre at kommunen etterlever regelverket og anerkjende standardar på området.
- Tysnes kommune har **ikkje 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 er ferdigstilt. Revisjonen understrekar at kommunen skal sikre at internkontrollen er systematisk og at det er etablert nødvendige rutinar og prosedyrar.
- Tysnes kommune har **ikkje etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik**. Revisjonen merkar seg at kommunen er i prosess med å utarbeide prosedyrar mv. for gjennomføring av kontroll og etterprøving av informasjonstryggleik, men påpeiker likevel at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta § 15 eller tilrådingar i ISO/IEC 27001 knytt til oppfølging og kontroll.
- Tysnes kommune har **ikkje etablert tilstrekkeleg system eller kontrollar som sikrar tilgjenge og konfidensialitet i informasjonssystema** som blir nytta i kommunen. Revisjonen meiner at kommunen med fordel burde samle og gjere tilgjengeleg felles retningslinjer og rutinar for tilgangsstyring i 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. Undersøkinga indikerer at kommunen ikkje har tilstrekkeleg felles system og tilgjengelege retningslinjer for dette arbeidet i alle elektroniske system i kommunen, og det er dermed 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 ikkje i samsvar med krav for informasjons- og personopplysningstryggleik, jf. personvernforordninga artikkel 32 nr. 1.

**Tysnes kommunen etterlever ikkje alle sentrale krav i personvernlovgevinga som er undersøkt.**

- **Kommunen har utnemnt eit personvernombod**, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at rolla som personvernombodet er ein redusert stilling (15 prosent), og at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Det går vidare fram at personvernombod i liten grad opplever å 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 (personvernforordninga, artikkel 38)

<sup>47</sup> Digidir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001 ved utarbeiding av styringssystem for informasjonstryggleik.

- **Tysnes kommune har etablert personvernerklæring.** Samtidig har kommunen ikkje sikra at denne erklæringa har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane. Kommunen si personvernerklæring er vidare ikkje tilstrekkeleg lett tilgjengeleg, i samsvar med krav om dette i regelverket (artikkel 12 i personvernforordninga).
- **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, men 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).
- **Kommunen gjennomfører ikkje i tilstrekkeleg grad risikovurderingar av handsaming av personopplysningar,** og det blir heller ikkje i samband med risikovurderingar systematisk gjort vurderingar av personvernisikoar (DPIA). Manglande risikovurderingar og rutinar for gjennomføring av slike gjer at kommunen ikkje har oversikt over kvar det er personvernisikoar, 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.
- Tysnes kommune har ved innføring av elektronisk avviksmeldesystem **sikra oversikt over avvik knytt til personvern.** Kommunen har samtidig **ikkje i tilstrekkeleg grad etablert retningslinjer som sikrar tilfredsstillande oppfølging av meldte avvik** knytt til informasjonstryggleik. Undersøkinga viser at det ikkje går konkret fram av handbok i informasjonstryggleik eller andre rutinar kven som skal melde få 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 understrekar 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).
- Undersøkinga viser at det førekjem i kommunen at det blir lagra sensitiv informasjon om tilsette og innbyggjarar på område der uvedkommande har innsyn, og at det også har blitt meldt avvik på dette. Revisjonen vurderer at dette ikkje er i samsvar med krav i personvernforordninga som seier at kommunen skal gjennomføre eigna tekniske og organisatoriske tiltak for å mellom anna sikre vedvarande konfidensialitet og integritet i behandlingssystema og -tenestene (artikkel 32, første ledd, bokstav b).
- 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 påpeiker at manglande avviksmeldingar aukar risikoen for at svakheiter i systema ikkje blir retta. Revisjonen vurderer at kommunen sin avvikspraksis ikkje er i samsvar med tilrådingane i ISO/IEC 27001 eller generelle prinsipp for god internkontroll.

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

- Tysnes kommune har **ikkje etablert tilstrekkeleg rutinar for å sikre at tilsette får opplæring i informasjonstryggleik.** Revisjonen påpeiker 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.
- Funna i spørjeundersøkinga viser at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Svar i spørjeundersøkinga indikerer vidare at det relativt store skilnadar

mellom sektorane i kommunen når det gjeld kjennskap til styrande dokument for informasjonstryggleik. Revisjonen understrekar 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. 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 (ISO/IEC 27001, punkt 5.2).

- Kommunen etterlever ikkje i tilstrekkeleg grad retningslinjer og rutinar for informasjonstryggleik. Undersøkinga indikerer mellom anna at dokument med fortruleg informasjon ikkje alltid blir lagra på ein sikker måte og/eller blir oppbevart slik at uvedkomande kan få innsyn.

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

1. Etablerer styringssystem for informasjonstryggleik som tilfredsstillar krav i regelverket og som er basert på anerkjend standard på området. Under dette mellom anna:
  - a. sikrar at tryggleiksstrategi og internkontroll inkluderer relevante krav fastsett i lov, forskrift eller instruks.
  - b. 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.
  - c. sikrar at det er etablert nødvendige rutinar og retningslinjer knytt til arbeidet med informasjonstryggleik i kommunen.
  - d. 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 krav oppfølging av meldte avvik på området, og særskilt krav når det gjeld melding av avvik til Datatilsynet (t.d. når det gjeld 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: 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>48</sup> Denne tredde i kraft 20. juli 2018, og gjennomfører EU si personvernforordning – kjend som GDPR<sup>49</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 nettidentifikator 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>50</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 databehandlarar 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>48</sup> Lov om behandling av personopplysninger (personopplysningsloven)

<sup>49</sup> General Data Protection Regulation

<sup>50</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.

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 rettleiingsmaterieill 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 overhaldt (bokstav b), gi råd om vurdering av personvernkonskvensar (bokstav c), og samarbeide med Datatilsynet (bokstav d).

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 (utslakta 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>51</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-standard, 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 eit kvart 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.

### 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 særlovgiving for kommunehelsetenester, sosialtenester, psykisk helsevern, samt forvaltnings- og offentlegheitslov.

Kommunen er også omfatta av sikkerheitslova, og har som følgje 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.

<sup>51</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/>



# Vedlegg 3: 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.

- ISO/IEC 27001: 2022. Information security, cybersecurity and privacy protection – Information security management systems – Requirements.
- 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. *Databehandlaravtale for PatientSky*. Ikkje datert.
- Tysnes kommune. *Databehandlaravtale for EVA Admin*. Ikkje datert.
- Tysnes kommune. *Oppdatering av databehandlaravtale 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.

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).

© 2023 Deloitte AS



---

Saksframlegg

---

**Saksnr:** 2022/208-12  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	16/23	05.10.2023

## Forvaltningsrevisjon av Plan- og byggesakshandsaming - oppfølging av handlingsplan

### Forslag til vedtak

1. Kontrollutvalet registrerer at kommunen har starta opp betringsarbeidet etter forvaltningsrevisjon av plan- og byggesakshandsaming
2. Kontrollutvalet ber om skriftleg tilbakemelding på handlingsplan til første møte i kontrollutvalet i 2024. Handlingsplan vert å senda sekretariatet innan 15.01.24

### Samandrag

Kommunestyret handsama revisjonsrapporten i møte 15.12.22, og vedtaket er i samsvar med innstillinga frå kontrollutvalet. Sekretariatet har motteke handlingsplanen og kommunen har starta opp betringsarbeidet etter forvaltningsrevisjonen. Sekretariatet tilrår at kontrollutvalet ber rådmann om ny skriftleg status til møte første møte i kontrollutvalet 2024.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

### Vedlegg

- 1 Forvaltningsrevisjon av plan og byggesak - handlingsplan
- 2 Forvaltningsrevisjon plan og byggesak - oppfølging av handlingsplan

## Saksutgreiing

### Bakgrunn for saka

Kommunestyret sitt vedtak frå møte 15.12.2022 (PS 34/2022) er i samsvar med innstillinga frå kontrollutvalet:

«På bakgrunn av gjennomført forvaltningsrevisjon innan plan- og byggesakshandsaming ber kommunestyret rådmannen syte for:

1. Å sikre at gjeldande fristar for sakshandsaming på tre og tolv veker i byggjesaker blir etterlevd
2. At det vert utarbeid system og rutinar som gjer det mogleg å halde felles oversikt over sakshandsamingstid og fristar i alle saker.
3. Å skriftleggjere og formalisere fordeling av roller, ansvar og oppgåver som gjeld plan- og byggesakshandsaming.
4. Å etablere rutinar for gjennomføring av jamlege risikovurderingar av arbeidsprosessar i plan- og byggesakshandsaming, som grunnlag for utforming av sakshandsamingsrutinar og kontrollar av kvalitet i sakshandsaming.
5. Å sikre at felles rutinar, sjekklister og vedtaksmalar for plan- og byggesakshandsaming, samt for gjennomføring av tilsyn og ulovlegheitsoppfølging, er tilstrekkeleg godt kjent og blir nytta av alle tilsette.
6. Iverksette kontroll av at rutinar/sjekklister/malar blir nytta og etterlevd.
7. At det vert utarbeid rutinar for som sikrar at det blir gjennomført kvalitetssikring av alle saker som blir handsama og vedtak som blir fatta.
8. Å sikre at det vert utarbeidd rutinar for å dokumentere habilitetsvurderingar som blir utført i samband med sakshandsaming av plan- og byggesaker
9. Å oppdatere strategi for gjennomføring av tilsyn med at byggetiltak blir gjennomført i samsvar med løyve og føresegn i regelverk.
10. At det vert etablert eit meir systematisk arbeid med kompetanse, læring og forbetring som sikrar at kommunen til ein kvar tid har tilgang på naudsynt kompetanse.
11. Å sikre at plan- og byggesaksavdelinga sine nettsider vert gjennomgått og utbetra, og sørge for å gjera det enklare for søkjarar å få oversikt over relevant informasjon om saksgang og kommunen sine krav til søknadar og planforslag.
12. Å sikre at arbeid med samanstilling og innrapportering av grunnlagsdata som skal inngå i sjølvkostkalkylar på plan- og byggesaksområdet, vert formalisert og rutinefesta.
13. Å lage ein prioritert handlingsplan til kontrollutvalet sitt første møte i 2023, med frist 15.01.2023, som viser kva tiltak som skal setjast i verk for å følgja opp tilrådingane i rapporten, når tiltaka skal setjast i verk og kven som skal ha ansvar for iverksettinga. «

Kontrollutvalet handsama handlingsplanen i møte 09.02.2023 (PS 3/23), dette vart protokollert:

*«Rådmannen orienterte om handlingsplanen slik den ligg føre i saka og svarte på spørsmål gjeldande denne.*

*Forslag til vedtak vart samrøystes vedteke.*

### Vedtak

1. *Kontrollutvalet registrerer at kommunen har starta opp betringsarbeidet etter forvaltningsrevisjon av plan- og byggesakshandsaming*
2. *Kontrollutvalet ber om skriftleg tilbakemelding på handlingsplan til møte i kontrollutvalet 05.10.23. Handlingsplan vert å senda sekretariatet innan 14.09.23»*

**Vedtakskompetanse**

Kontrollutvalet har vedtakskompetanse til å følge opp kommunestyret sine vedtak etter revisjonsrapportar, jf. kommunelova § 23-2, e.

**Vurderingar og verknader**

Sekretariatet har motteke handlingsplan frå rådmann og registrerer at kommunen er i gang med betringsarbeidet etter forvaltningsrevisjonen, men at det står att ein del arbeid med frist 01. november 2023. Rådmannen kjem til møtet og vil gje ei munnleg orientering om status punkt for punkt.

Handlingsplan og notat frå rådmann er vedlagt saka.

**Konklusjon**

Det vert tilrådd frå sekretariatet at kontrollutvalet ber rådmannen om skriftleg status på handlingsplanen til første møte i kontrollutvalet i 2024.

Rådmannen

Sakshandsamar:

Steinar Dalland

Mobil: 970 46 500

Vår ref: 2023/327- 2

Dykkar ref:

Dato: 31.01.2023

### Forvaltningsrevisjon av plan og byggesak - handlingsplan

Me viser til kommunestyre sitt vedtak i sak 34/22 i kommunestyre sitt møte 15. desember og sender med dette over handlingsplan i samsvar med kommunestyre sitt vedtak.

Målområde	Tiltak	Forventa effekt	Tidfrist	Frist for evaluering	Ansvar
<b>Å sikre at gjeldande fristar for sakshandsaming på tre og tolv veker i byggjesaker blir etterlevd</b>	Dette vert løyst ved innføring av e-byggesak	E-byggesak har gode løysingar for visuell framstilling av tidslinje, rapportering og kontroll.	01.mar	01.nov	Kommunalsjef
<b>At det vert utarbeid system og rutiner som gjer det mogeleg å halde felles oversikt over sakshandsamingstid og fristar i alle saker</b>	Dette vert løyst ved innføring av e-byggesak	E-byggsak har gode leiaroppfølgingssystem samanlikna med dagens system.	01.mar	01.nov	Kommunalsjef

<b>Å skriftleggjere og formalisera fordeling av roller, ansvar og oppgåver som gjeld plan- og byggjesakshandsaming</b>	Etablere stillingsomtaler for alle stillingar med minimum årleg revidering.	Tydeleggjering av forventningar, roller, ansvar og oppgåver.	01.jun	01.nov	Kommunalsjef
<b>Å etablere rutinar for gjennomføring av jamlege risikovurderingar av arbeidsprosessar i plan- og byggjesakshandsaming, som grunnlag for utforming av sakshandsamingsrutinar og kontrollar av kvalitet i sakshandsaming</b>	Det vert lagt opp til å gjennomføra ein ny risikovurdering etter at e-byggesak er implementert	Nytt sakshandsamingssystem eliminerer nokre risikoelement, samstundes kan det oppstå nye. Dette gjer at det er fornuftig å gjera ei ny ROS analyse når systemet er implementert	01.jun	01.nov	Kommunalsjef
<b>Å sikre at felles rutinar, sjekklister og vedtaksmalar for plan- og byggjesakshandsaming, samt for gjennomføring av tilsyn og ulovlegheitsoppfølging, er tilstrekkeleg godt kjent og blir nytta av alle tilsette</b>	Dette vert løyst ved innføring av e- byggesak	E byggesak har verktøy for prosessstøtte og felles malar innarbeidd i fagsystemet.	01.mar	01.nov	Kommunalsjef
<b>Iverksette kontroll av at rutinar/sjekklister/malar blir nytta og etterlevd</b>	Dette vert løyst ved innføring av e- byggesak	E-byggesak har innarbeidd støtte som krev avsjekk lags flyten.	01.mar	01.nov	Kommunalsjef
<b>At det vert utarbeid rutinar for som sikrar at det blir gjennomført kvalitetssikring av alle saker som blir handsama og vedtak som blir fatta.</b>	Det er iverksett ein gjennomgang av system for sidemannskontroll, det er vert nedfelt i skriftlege rutinar for å sikra balanse mellom	Skriftleg rutine lagt inn i Compilo	01.jun	01.nov	Kommunalsjef



	<p>kvalitetskrav og produktivitet.</p>				
<p><b>Å sikre at det vert utarbeidd rutinar for å dokumentere habilitetsvurderingar som blir utført i samband med sakshandsaming av plan- og byggjesaker</b></p>	<p>Me vil vurderer om det er trong for ei ekstra rutine for dette, alternativt vil me leggja det opp som eit fast sjekkpunkt i e-byggesak</p>	<p>Skriftleg rutine lagt inn i Compilo</p>	<p>01.jun</p>	<p>01.nov</p>	<p>Kommunalsjef</p>
<p><b>Å oppdaterer strategi for gjennomføring av tilsyn med at byggetiltak blir gjennomført i samsvar med løyve og føresegner i regelverk</b></p>	<p>Strategiplan for tilsyn og kontroll i vart vedteken i utvalet 1. desember 2022</p>		<p>Er utført</p>	<p>01.nov</p>	<p>Kommunalsjef</p>
<p><b>At det vert etablert eit meir systematisk arbeid med kompetanse, læring og forbetring som sikrar at kommunen til ein kvar tid har tilgang på naudsynt kompetanse</b></p>	<p>Det skal utarbeidast eit system for årlege opplæringsplanar for å sikra rett kompetanse til ein kvar tid</p>	<p>Lage opplæringsplan med bakgrunn i behov, utvikling og årlege medarbeidarsamtalar.</p>	<p>01.nov</p>	<p>01.nov</p>	<p>Kommunalsjef</p>
<p><b>Å sikre at plan- og byggjesaksavdelinga sine nettsider vert gjennomgått og utbetra saksgang og kommunen sine krav til søknader og planforslag.</b></p>	<p>Fagetaten og sentraladministrasjonen har omdisponert ressursar for å styrka dette arbeidet. Ny</p>	<p>Auka moglegheit for sjølvhjelp og eventuelt hjelp ved første kontakt til kommunen.</p>	<p>01.jun</p>	<p>01.nov</p>	<p>Kommunalsjef</p>

heimeside vert lansert  
ila februar

**Å sikre at arbeid med  
samanstilling og innrapportering  
av grunnlagsdata som skal inngå  
i sjølvkostkalkylar på plan- og  
byggjesaksområdet, vert  
formalisert og rutinefesta**

Innføring av e-  
byggesak,  
førehandskalkulasjon  
av EnviDan,  
etterkalkyle av  
Momentum.

Det er i dag fast system for  
etterkalkyle på sjølvkost, for 2022  
har me også nytta oss av  
EnviDan sitt system for  
førehandskalkulasjon.  
Ebyggesak har også direkte  
rapportering til KOSTRA.

Er  
utført

01.nov

Kommunalsjef

Me er deltar gjerne i møte for å gå gjennom planen for vidare oppfølging!

Med helsing

Steinar Dalland  
rådmann

*Brevet er elektronisk godkjent.*

Kopi til:

Helge Inge Johansen

### Forvaltningsrevisjon plan og byggesak - oppfølging av handlingsplan

Det vert vist til kontrollutvalet sitt vedtak i møte 09.02.2023:

1. *Kontrollutvalet registrerer at kommunen har starta opp betringsarbeidet etter forvaltningsrevisjon av plan- og byggesakshandsaming*
2. *Kontrollutvalet ber om skriftleg tilbakemelding på handlingsplan til møte i kontrollutvalet 05.10.23. Handlingsplan vert å senda sekretariatet innan 14.09.23*

Handlingsplanen følgjer vedlagt, me går kort gjennom status på dei ulike punkta i handlingsplanen og vil også vera tilgjengeleg for kontrollutvalet i møte. Dei punkta som allereie var utført når planen sist vart handsama i kontrollutvalet har me ikkje kommentert noko vidare.

#### 1. Sikre at gjeldande fristar for sakshandsaming vert etterlevd

E-byggesak vart innført i februar 2023 og sikrar at leiar til ei kvar tid har oversikt over tildelte saker og kva som er status opp mot gjeldande fristar.

Sakshandsamar får tilsvarande oversikt over milepælar i eigne saker.

Det er vurdert at dette er tilstrekkeleg til å sikra etterleving av fristar.

#### 2. Utarbeide system og rutinar som gjer det mogleg å ha oversikt over sakshandsamingstid og fristar i alle saker.

E-byggesak, og rett bruk av systemet sikrar god oversikt over sakshandsamingstid og fristar i alle saker.

Det er vurdert at det er tilstrekkeleg til å svare ut dette punktet.

#### 3. Skriftleggjering og formalisering av roller

Dette er delvis på plass det er laga skildringar for rolle som fagansvarleg byggesak og rolle som konsulent, rolle som sakshandsamar er ikkje formalisert utover den ramma som vart

lagt ved utlysning. Når det gjeld rolle som konsulent og fagansvarleg hadde me ikkje tilsvarende ramme då desse kom til som følgje av organisasjonstilpassingar.

Dette punktet vert fylgt vidare opp.

#### 4. Etablere rutiner for jamlege risikovurderingar

Byggesaksavdelinga opplever litt ulike risikofaktorar etter at e-byggesak vart teke i bruk, det er lagt opp til at det vert gjort ei ny ROS vurdering etter november. Det må sjåast i samanheng med at november er sett som evalueringsfrist internt i organisasjonen.

Dette punktet vert fylgt vidare opp.

5. Sikre at felles rutinar, sjekklister og malar for byggesak vert fylgt opp av alle tilsette E-byggesak byggjer på felles malar og sjekklister. Det er ikkje mogleg å kome vidare dersom desse ikkje vert kvittert ut.

Det er vurdert at det er tilstrekkeleg til å svare ut dette punktet.

6. Iverksetje kontroll av at rutinar/sjekklister/malar blir nytta og etterlevd  
Sjå punktet over.

Det er vurdert at det er tilstrekkeleg til å svara ut dette punktet.

7. Rutiner for sikring av kvalitetskontroll  
Det er fast oppsett for sidemannskontroll.

Det er fast oppsett for leiarkontroll for alle saker som skal til politisk handsaming.

Det er vurdert at det er tilstrekkeleg til å svara ut dette punktet.

8. Rutiner for habilitetskontroll  
Alle saker vert tildelt gjennom felles tildelingsmøte, i desse møta er det ein avsjekk også i høve til habilitet, men det er ikkje rutine for å dokumentera vurdering av habilitet.

Dette punktet vert fylgt opp vidare.

9. Systematisk arbeid knytt til kompetanse og læring  
Det vert utarbeida opplæringsplan for avdelinga, dette skal gjerast innan 1. november kvar år.

Det er vurdert at det er tilstrekkeleg til å svara ut dette punktet.

10. Nettsider  
Tysnes kommune lanserte sin nye nettstad i sumar, i samband med dette vart informasjonen om byggesak oppdatert på nettstaden. Det er sett av ressursar for å styrkje dette arbeidet både i byggesaksavdelinga og i sentraladministrasjonen.

Det er vurdert at det er tilstrekkeleg til å svara ut dette punktet.

Med helsing

Steinar Dalland  
rådmann

*Brevet er elektronisk godkjent.*

Kopi til:

Intern kopimottakere:  
Tommy-Rene Stordal

ass.rådmann

Teknisk

Vedlegg

1 Forvaltningsrevisjon av plan og byggesak - handlingsplan



---

Saksframlegg

---

**Saksnr:** 2022/96-26  
**Saksbehandlar:** Helge Inge Johansen

---

### Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	17/23	05.10.2023

## Rekneskapsrevisjon - oppfølging av revisjonsrapport nr.11 - orientering frå rådmann

### Forslag til vedtak

Informasjonen vert teken til orientering.

### Samandrag

I rekneskaps saka i maimøtet vart det lagt fram ein revisjonsrapport frå revisor med nokre oppfølgingspunkt. I vedtaket frå maimøtet ber kontrollutvalet om at rådmannen kjem til dette møtet med ei tilbakemelding på forholda som kjem fram i revisjonsrapporten.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

### Vedlegg

- 1 Revisjonsrapport 2022 Tysnes kommune
- 2 Tilbakemelding til kontrollutvalet - oppfølging av rev.rapp.nr.11

## Saksutgreiing

### Bakgrunn for saka

Frå møtet i kontrollutvalet 11.05.2023 (PS 10/23) vart dette mellom anna protokollert:

*«På bakgrunn av det som kjem fram i revisjonsrapport nr. 11 frå Deloitte AS ber kontrollutvalet om at rådmann kjem i møte 05.10.2023 for å gjera greie for kva som vil bli gjort i høve tilrådingane i rapporten»*

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse til å gje uttale til kommunestyret om årsrekneskapen og årsberetninga. Jf. forskrift om kontrollutval og revisjon § 3.

### Vurderingar og verknader

Revisjonsrapport nr. 11 frå Deloitte AS er vedlagt saka og det er to tilrådingar som kjem fram i rapporten gjeldande tidspunkt for avstemmingar av vesentlege balansepostar og sjølvkost innan renovasjon.

Rådmann er orientert om at dette er ei sak til dette møtet og sekretariatet har motteke skriftleg tilbakemelding til saka 26.09.2023. Kontrollutvalet må ut i frå det som kjem fram av informasjon i møtet og det som kjem fram av saksframlegg og vedlegg, vurdere kva ein skal gjera vidare med saka. Er informasjon som kjem fram i møtet tilfredsstillande kan kontrollutvalet lukke saka. Alternativt kan kontrollutvalet be om ei ny orientering til eit seinare møte.

### Konklusjon

Informasjonen vert teken til orientering.



Tysnes kommune  
Att.: Rådmann  
Rådhuset

5685 UGGDAL

13. april 2023

Revisjonsrapport nr. 11  
(journalføres)

## REVISJONSRAPPORT 2022

### Innleiing

Vi har avslutta revisjonen av rekneskapen for 2022. Vi vil i det høve gje ei kort utgreiing for utført revisjon i år og for tilhøve som vi ynskjer å ta opp. Rapporten omhandlar tilhøve som vi meiner bør vere av interesse for leiinga i kommunen.

I vår revisjon har vi gjennomført dei revisjonshandlingane vi har sett som naudsynte for å få stadfesta at årsrekneskapen ikkje inneheld vesentlege feil eller manglar og for å gje vår revisjonsmelding.

Deloitte utfører risikobasert revisjon. Dette vil sei at kontrollmetodar og kontrollomfang vert tilpassa risikoen i organisasjonen og rutinar. Vi kartlegg og vurderer difor dei viktigaste økonomi- og rekneskapsrutinane for å identifisere kor det er størst risiko for feil i rekneskapsrapporteringa.

Basert på utført revisjon har vi notert oss enkelte tilhøve vi meiner kommunen si leiing bør vere merksame på. Vi vil presisere at det er leiinga i kommunen som er ansvarleg for å etablere og oppretthalde ein tilfredsstillande intern kontroll. Som ein del av dette må leiinga sjå til at rekneskapsføringa er i samsvar med lover og forskrifter og at formueforvaltninga er ordna på ein trygg måte.

### Uavhengigheit og objektivitet

Vi stadfestar at revisjonsteamet tilfredsstillar dei krava til uavhengigheit og objektivitet for revisorar som reviderer kommunal og fylkeskommunal verksemd, og som går fram av § 24-4 i kommunelova og som er nærare konkretisert i forskrift om kontrollutval og revisjon §§ 16-18.

### Revisjonen gjennom året

Ved vår revisjon gjennom året har vi på nokre utvalde rekneskapsområde kartlagt og testa vesentlege interne kontrollar. I tillegg har vi nytta analysar og kontrolltestar som grunnlag for å vurdere kvaliteten på årsrekneskapen. Vidare har vi utført direkte kontroll av utvalde postar i rekneskapen.

Vi har ikkje avdekkja tilhøve som var av ein slik karakter eller storleik at dei fører til uvisse med omsyn til den framlagde årsrekneskapen.

### Revisjonen av årsoppgjeret

Revisjonen av årsrekneskapen har i stor grad vore retta mot å verifisere balansepostane per 31.12.2022. Vi har lagt vekt på å kontrollere at inntekter og gjeld er fullstendig og at eigedelar og utgifter er gyldige og eksisterer. I tillegg har vi kontrollert større inntektspostar som skattar, rammeoverføringar og andre statlege tilskot, og vesentlege utbetalingar som løn, tilskot og avdrag. Vi har og utført kontrollar av estimat som pensjon og avskrivningar.

Vi har gjennom våre revisjonshandlingar ikkje funne vesentlege formelle eller materielle feil i den framlagde rekneskaper, men har nokre tilhøve som vi vil peika på.

**Avstemming av balansekontoar**

Balansekontoar av vesentleg betydning skal avstemmast, jf. bokføringsforskrifta. Kommunen har utarbeidd avstemming for dei fleste av postane i balanserekneskaper, men har ikkje utarbeidd avstemming for to vesentlege postar. Vi tilrår kommunen å få på plass avstemmingar av alle vesentlege balansekontoar i 2023.

**Sjølvkost**

I samsvar med forurensningslova er det krav om 100 % utgiftsdekking på renovasjon. Kommunen har i 2022 85 % dekning. Tilhøyrande etterkalkyle viser at krav om full utgiftsdekking er oppfylt over ein femårsperiode.

**Avslutning**

Dersom noko skulle vere uklårt i framstillinga ovanfor, eller at det er trong for hjelp i samband med tilrådde tiltak eller andre tilhøve, står vi gjerne til teneste.

Vi vil avslutningsvis nytta høve til å takke for samarbeidet.

Med venleg helsing  
Deloitte AS

Unni-Renate Moe  
statsautorisert revisor

Kopi: Kontrollutvalet

# PENNEO

Signaturene i dette dokumentet er juridisk bindende. Dokument signert med "Penneo™ - sikker digital signatur".  
De signerende parter sin identitet er registrert, og er listet nedenfor.

"Med min signatur bekrefter jeg alle datoer og innholdet i dette dokument."

## Unni-Renate Moe

Statsautorisert revisor

Serienummer: 9578-5995-4-99839

IP: 51.174.xxx.xxx

2023-04-13 14:37:09 UTC



Penneo Dokumentnøkkel: 4E01Q-Q5YZ4-8BDZP-IL11-KECB3-1ANFQ

Dokumentet er signert digitalt, med **Penneo.com**. Alle digitale signatur-data i dokumentet er sikret og validert av den datamaskin-utregnede hash-verdien av det opprinnelige dokument. Dokumentet er låst og tids-stemplet med et sertifikat fra en betrodd tredjepart. All kryptografisk bevis er integrert i denne PDF, for fremtidig validering (hvis nødvendig).

### Hvordan bekrefter at dette dokumentet er originalen?

Dokumentet er beskyttet av ett Adobe CDS sertifikat. Når du åpner dokumentet i

Adobe Reader, skal du kunne se at dokumentet er sertifisert av **Penneo e-signature service** <[penneo@penneo.com](mailto:penneo@penneo.com)>. Dette garanterer at innholdet i dokumentet ikke har blitt endret.

Det er lett å kontrollere de kryptografiske beviser som er lokalisert inne i dokumentet, med Penneo validator - <https://penneo.com/validator>

Kontrollutvalet  
v/Helge Inge Johansen

### Tilbakemelding til kontrollutvalet

Me viser til kontrollutvalet sitt vedtak 11.058.23 der det mellom anna heiter:

«På bakgrunn av det som kjem fram i revisjonsrapport nr. 11 frå Deloitte AS ber kontrollutvalet om at rådmann kjem i møte 05.10.2023 for å gjera greie for kva som vil bli gjort i høve tilrådingane i rapporten»

I den aktuelle rapporten peiker revisor på to tilhøve. Det eine gjeld avstemming av balansekontoar der det er snakk om avstemming av to vesentlege postar. Revisjonen tilrår at kommunen får på plass avstemming av alle vesentlege balansekontoar i 2023.

Desse to kontiane vert berre brukt rundt årsskiftet :

21399002 Forskotsbetaling : I ein del tilfelle får me faktura i desember, som gjeld neste år (typisk abonnement, IT lisensar etc). For å få desse på riktig år vert desse fakturaene mellomført på konto for forskotsbetaling.

21399996 INTERRIM BANK : Fakturaer som me mottar i januar/februar men som gjeld føregåande rekneskapsår, vert ført mot denne kontoen.

Begge desse kontiane vert nullstilt i byrjinga av nytt år, når avstemming av bankkontoen vert utført. Kontiane vert såleis indirekte avstemt når banken vert avstemt. Men me kan i fortsetjinga legge meir vekt på å dokumentera fortløpande føringar mot desse kontiane.

Det står ein liten saldo på kontoen for forskotsbetaling (kr. 20.000), men dette skriv seg frå eit tidlegare år. Denne kan førast bort for å unngå avstemmingsproblem framover.

Den andre merknaden i revisjonsrapport 11 er knytt til at kommunen ikkje hadde full inndekking på sjølvkostområde for renovasjon. Her er det slik at det er lovleg å gjera avsetjing til både positive og negative fond slik at inndekking blir 100 % over ein periode på nokre år.

Tabellen under viser kalkulasjon og inndekking av fondet som revisjonen peikar på:

### Selvkostoppstilling Renovasjon

Selvkostregnskap (1.000 kr)	2022	2023	2024	2025	2026	2027	2028
10*** Lønn	78	40	41	42	43	45	46
11*** Varer og tjenester	30	36	37	37	38	39	40
12*** Varer og tjenester	27	15	16	16	16	17	17
13*** Tjenester som erstatter kommunal egenprod.	4 636	4 843	4 988	5 138	5 292	5 451	5 614
14*** Overføringsutgifter	0	5	5	5	5	5	5
Direkte driftsutgifter	4 772	4 939	5 086	5 238	5 395	5 556	5 722
Indirekte kostnader (drift og kapital)	108	111	114	117	120	124	127
+/- Øvrige inntekter og kostnader	-1	0	0	0	0	0	0
Gebyrgrunnlag	4 878	5 049	5 200	5 355	5 515	5 680	5 849
Gebyrinntekter	4 129	5 352	5 379	5 670	5 726	5 888	5 847
Selvkostresultat	-749	302	179	215	211	208	-2
Selvkost dekningsgrad i %	84,64 %	105,96 %	103,44 %	104,01 %	103,83 %	103,66 %	99,96 %
Selvkostfond/fremførbart underskudd (1.000 kr)	2022	2023	2024	2025	2026	2027	2028
Selvkostfond 01.01	-234	-1 005	-741	-593	-400	-202	2
+/- Bruk av/avsetning til selvkostfond	-749	302	179	215	211	208	-2
+/- Kalkulert rentekostnad/-inntekt selvkostfond	-22	-38	-31	-22	-13	-4	0
Selvkostfond 31.12	-1 005	-741	-693	-400	-202	2	0

Tysnes kommune har gode rutinar både for budsjettoppfølging og etterkalkulasjon innanfor sjølvkostområda.

Med helsing

Steinar Dalland  
rådmann

*Brevet er elektronisk godkjent.*

Kopi til:



---

Saksframlegg

---

**Saksnr:** 2022/100-1  
**Saksbehandlar:** Helge Inge Johansen

---

### Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	18/23	05.10.2023

## Rådmann orienterer om etikk og misleg framferd i Tysnes kommune

### Forslag til vedtak

1. Kontrollutvalet tar informasjonen til orientering
2. Utvalet tilrår at tilsvarende sak vert sett på sakslista i siste møte i 2024.

### Samandrag

Føremålet med denne saka er at kontrollutvalet skal få orientering frå rådmann på korleis status er i Tysnes kommune når det gjeld arbeid med etikk og misleg framferd.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

## Saksutgreiing

### Bakgrunn for saka

Det er ønskjeleg at rådmann orienterer kontrollutvalet om status når det gjeld arbeid med etikk og misleg framferd i Tysnes kommune. Ei slik orientering kan t.d. innehalde slike opplysningar:

1. Kva er gjort på etikk området siste året?
2. Kva er planlagt å gjera innan etikk det neste året?
3. Er det gjennomført dilemmatrening?
4. Er det halde kurs eller seminar om etikk?
5. Generell informasjon om omfang og handtering av eventuell misleg framferd i kommunen
6. Osv.

Omgrepet misleg framferd vert definert slik i revisjonsstandar ISA 240

<https://www.revisorforeningen.no/fag/standarder-og-veiledninger/revisjonsstandardene/>:

*«En bevisst handling begått av en eller flere personer innen ledelsen, av personer som har overordnet ansvar for styring og kontroll, av ansatte eller av andre, som innebærer uredelighet for å oppnå en urettmessig eller ulovlig fordel.»*

KS og Transparency International Norge (TI Norge) har laga ei dilemmasamling om refleksjon rundt etikk og antikorrupsjon i kommunar og fylkeskommunar som finns på denne lenkja:

[Dilemmasamling for kommuner og fylkeskommuner - Forum for kontroll og tilsyn \(fkt.no\)](#)

Det vil vera ei føremon om det også vert orientert om kommunen har laga eit Antikorrupsjonsprogram eller har vurdert å lage eit slikt program. Jf. i den forbindelse «Håndbok i antikorrupsjon – Beskytt kommunen» som du finn på denne lenkja:

[Beskytt-kommunen-Handbok-i-antikorrupsjon.pdf \(ks.no\)](#)

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse i sak der utvalet vil innhente informasjon, jf. kommuneloven § 23-2.

### Vurderingar og verknader

Det er gjort avtale med rådmann i epost 26.09.2023 om at han kjem i dette møtet for å orientere kontrollutvalet om temaet. Sekretariatet ser dette som eit viktig saksfelt for kontrollutvalet og tilrår at utvalet har tilsvarande sak oppe med jamne mellomrom.

### Konklusjon

Sekretariatet tilrår at kontrollutvalet tar informasjonen til orientering, samt kjem med tilråding om at kontrollutvalet i neste valperiode handsamar tilsvarande sak i siste møte i 2024.



---

Saksframlegg

---

**Saksnr:** 2023/413-1  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	19/23	05.10.2023

## Kontrollutvalet si rolle i varslingsaker

### Forslag til innstilling

1. Kommunestyret har intensjon om at kontrollutvalet, av omsyn til naudsynt uavhengigheit, ikkje lenger skal ha ei rolle i varslingsaker slik det er omtala i «Rutine for intern varsling av kritikkverdige forhold» pkt.4.2 på side 5.
2. Kommunestyret vedtek at rutinane for varslingsrutine for tilsette og folkevalde i Tysnes kommune», skal reviderast i tråd med det som går fram av punkt 1.

### Samandrag

Føremålet med denne saka er at kontrollutvalet skal komme med innspel til endringar i «Varslingsrutine for tilsette og folkevalde i Tysnes kommune» når det gjeld kontrollutvalet si rolle i varslingsaker.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

Vedlegg

1

Varslingsrutinen-2



## Saksutgreiing

### Bakgrunn for saka

I «Rutine for intern varsling av kritikkverdige forhold» i Tysnes kommune (sjå vedlegg), kjem det fram slik informasjon om kontrollutvalet (s.5).

*«Dersom varsling i tenestelinja ikkje er mogleg, eller den som varslar ikkje ønskjer å ta opp forholda på eigen arbeidsplass, kan vedkommande ta kontakt med:*

*Kontrollutvalet»*

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse i sak der utvalet vil innhenta informasjon, jf. kommunelova § 23-2.

Ved forvaltningsrevisjonar mv. er det kontrollutvalet som har ansvar for å gjennomføre slike revisjonar. Det er likevel kommunestyret som har avgjersmynde i saka, etter innstilling frå kontrollutvalet, når revisjonsrapport ligg føre, jf. kommunelova § 23-3.

Ved dette høve har kontrollutvalet, gjennom reglement, fått ein funksjon ift. varsling. Kontrollutvalet er kommunestyret sitt kontrollorgan, og må kunna rapportera attende om utvalet kjenner på at utvalet er tildelt ein rolle som kan vera problematisk ift. uavhengigheit.

### Vurderingar og verknader

Sekretariatet meiner at det er problematisk i høve uavhengigheit at kontrollutvalet skal ha ei rolle i varslingssaker. Dette vert m.a. grunnjeve i at kontrollutvalet samstundes skal ha ansvar for å gjennomføre forvaltningsrevisjon når det gjeld korleis kommunen sine varslingsrutinar er utforma og korleis dei vert praktisert. Det vil kunne medføre at kontrollutvalet kan møte seg sjølv i døra i gjennomføringa av ein slik revisjon. Det vil samstundes vera problematisk for revisor å bistå kontrollutvalet i eit slikt arbeid dersom dei tidlegare har levert ein rapport om varsling. Det vil kunne vera med på å svekke tilliten til varslingsinstituttet.

Det bør på bakgrunn av dette vurderast om kontrollutvalet, av omsyn til naudsynt uavhengigheit, ikkje skal ha ei rolle i varslingssaker. Noverande rutinar for varsling bør difor reviderast.

### Konklusjon

På bakgrunn av det som går fram over vert det tilrådd at kontrollutvalet tar opp med kommunen at utvalet, av omsyn til naudsynt uavhengigheit, ikkje lenger skal ha ei rolle i varslingssaker slik det er omtala i «Rutine for intern varsling av kritikkverdige forhold» i Tysnes kommune (sjå vedlegg), der det kjem fram slik informasjon om kontrollutvalet (s.5).

Vidare vert det tilrådd at kontrollutvalet føreslår for kommunen at rutineane for varsling vert revidert i tråd med dette.



TYSNES KOMMUNE

## **Rutine for intern varsling av kritikkverdige forhold**

Vedtatt i kommunestyret 10. juni 2009  
Rullering i kommunestyret 24. september 2020

## Innhald

1	Om varslingsrutinen .....	3
1.1	Bakgrunn.....	3
1.2	Føremål .....	3
1.3	Iverksetjing og ansvar.....	3
1.3.1	Rådmannen.....	3
1.3.2	Einingsleiarar.....	3
1.3.3	Tilsette.....	4
2	Kva er kritikkverdige forhold?.....	4
3	Forsvarleg varsling.....	4
4	Kanalar for varsling.....	5
4.1	Intern varsling – tenesteveg .....	5
4.2	Intern varsling – andre kanalar.....	5
4.3	Intern varsling – varslingssekretariatet .....	5
4.4	Ekstern varsling.....	5
5	Handsaming av varsel .....	6
5.1	Mottak av varsel .....	6
5.2	Oppfølging av varsel .....	6
5.3	Oppfølging av den som varslar .....	6
5.4	Oppfølging av den det vert varsla om.....	7
5.5	Varslar som omfattar rådmann eller ordførar.....	7
5.6	Rapportering.....	7





#### **EIN ORGANISASJON MED GOD YTRINGSKULTUR KJENNETEIKNAST VED AT:**

- Leiararar praktiserer openheit
- Leiararar møter kritikk og usemje på ein konstruktiv måte
- Det leggst til rette for dialog og diskusjon på både formell og uformelle arenar
- Kritikkverdige forhold vert avdekka og handtert
- Varslarar utsetjast ikkje for gjengjelding

Kjelde: KS



# 1 Om varslingsrutinen

## 1.1 Bakgrunn

Som ein kvar kommune, er me i Tysnes kommune avhengig av tillit for å utføre våre oppgåver på best mogleg måte. For at me saman skal nå kommunenes overordna mål, er det både ønskeleg og naudsynt at kritikkverdige forhold vert avdekka.

Ein god ytringskultur og gode rutinar rundt varsling er viktig for lokaldemokratiet. Det er òg med på å sikre gode tenester, eit godt arbeidsmiljø og god samhandling mellom leiarar og medarbeidarar.

Alle tilsette og folkevalte i Tysnes kommune **kan** og **bør** varsle dersom dei vert kjent med kritikkverdige forhold i organisasjonen. Dette gjelder også for innleigd arbeidskraft.

Retten til å varsle er nedfelt i Arbeidsmiljølovens kapittel 2A. Her er det også pålegg til arbeidsgjevar om å utarbeide rutine for intern varsling.

## 1.2 Føremål

Hensikta med varslingsrutinen er å legge til rette for ei trygg og forsvarlig varsling for tilsette som melder i frå om brot på lover og regelverk på arbeidsplassen. Ved å følgje varslingsrutinen skal ein være trygg på at ein er beskytta mot gjengjelding og negative reaksjonar når ein varslar om kritikkverdige forhold.

Varslingsrutinen skal sikre at varsel vert handsama på ein god måte. Den skal informera om saksgang, og den skal tydeliggjere kva forventning den som varslar kan ha til informasjon om vidare handsaming av varsel.

## 1.3 Iverksetjing og ansvar

### 1.3.1 Rådmannen

Det er viktig at varslingsrutinen er kjent og vert nytta når det er naudsynt. Rådmannen skal leggja til rette for at varslingsrutinen vert gjort kjent for tilsette og folkevalde i Tysnes kommune, og at leiarar på alle nivå er godt kjent med innhaldet. Tilsette skal gjerast kjent med retningslina ved tilsetjing og det er verta utarbeida opplæringsmateriale som skal nyttast ved årlig oppfrisking i einingane.

### 1.3.2 Einingsleiarar

I Tysnes kommune ønskjer me å ha ein ytringskultur med låg terskel for å ta opp uheldige forhold i tenesteveg. Slik ønskjer me at uheldige forhold vert avdekka og handtert på lågt nivå, før dei utviklar seg til kritikkverdige forhold. For å oppnå det er det viktig at ytringar og

kritikk blir møtt på ein konstruktiv måte. Einingsleiarar har eit særskilt ansvar i arbeidet for ein god yringskultur.

### 1.3.3 Tilsette

Forutan rett til å varsle, ligg det òg ein plikt hos dei tilsette til å varsle dersom ein oppdagar kritikkverdige forhold på arbeidsplassen. Plikt til å varsle finnast i «Arbeidstakars medvirkningsplikt» Aml. § 2-3, særlig i bokstavane b og d. Plikt til å varsle kan òg finnast i særlover, på dei ulike fagområda me jobbar med.

## 2 Kva er kritikkverdige forhold?

a) Eksempel på kritikkverdige forhold:

- Brot på lovar og reglar, eller på våre etiske retningslinjer
- Brot på teieplikta
- Forhold som medfører fare for liv og helse
- Korrupsjon, underslag, tjuveri eller maktmisbruk
- Brot på reglar for innkjøp
- Mangelfull utføring av forventta arbeid
- Mobbing, krenking, trakassering eller diskriminering

Lista er meint som rettleiing, og er ikkje uttømmende.

b) Forhold arbeidstakar meiner er kritikkverdige ut frå eigen politisk eller etisk overtyding, vert ikkje omfatta av retten til å varsle.

## 3 Forsvarleg varsling

Når varsling vert gjort på forsvarlig måte, er den som varslar sikra mot gjengjelding og negative reaksjonar. Varslingsrutinen stiller krav til måten det blir varsla på, men den skal ikkje avgrense retten til å varsle.

a) For at varslinga skal være forsvarleg må to punkt være oppfylt:

- Arbeidsgivar sin legitime interesser vert teke omsyn til i måten det vert varsla på, og
- varslar er i god tru om at det ligg føre kritikkverdige forhold

b) Varsling i samsvar med varslingsrutinen er alltid forsvarleg.

c) Varsling til offentlige tilsynsmyndigheter, til dømes Arbeidstilsynet eller Fylkesmannen, er forsvarleg.



d) Dersom varslinga vert uført på ein måte som unødig skadar arbeidsmiljø, einiskilde personar, tenestebrukarar eller anna i verksemda, vert ikkje varslinga rekna som forsvarleg.

## 4 Kanalar for varsling

Tilsette som kjenner til kritikkverdige forhold som bør undersøkast nærmare, eller som nødvendigjer tiltak, bør som hovudregel ta dette opp på eigen arbeidsplass. Dersom varsling i tenestlinja vert vurdert som utilstrekkeleg, oppmodar me til å varsle andre vegar. Anonym varsling er ikkje omfatta av varslingsrutinen.

### 4.1 Intern varsling – tenesteveg

- Hovudregelen er at kritikkverdige forhold skal takast opp med **nærmaste leiar**
- **Verneombodet og tillitsvalt** på arbeidsplassen kan varslast dersom det vert vurdert som føremålstenleg
- Dersom nærmaste leiar ikkje følgjer opp saka, bør **overordna leiar** varslast

### 4.2 Intern varsling – andre kanalar

Dersom varsling i tenestelinja ikkje er mogleg, eller den som varslar ikkje ønskjer å ta opp forholda på eigen arbeidsplass, kan vedkommande ta kontakt med:

- Verneombod
- Tillitsvalde
- Bedriftshelsetenesta
- Kontrollutvalet

### 4.3 Intern varsling – varslingssekretariatet

Varslingssekretariatet er ei særskild gruppe som har ansvar for å følgja opp varsel som ikkje vert varsla på anna måte. Varslingssekretariatet er satt saman av ordføraren, rådmannen og hovudverneombod.

Varsle til varslingssekretariatet kan gjerast direkte til eit av medlemmane eller via e-post: [varsling@tysnes.kommune.no](mailto:varsling@tysnes.kommune.no)

### 4.4 Ekstern varsling

I Tysnes kommune er det tilrettelagt for intern varsling. Dette er likevel ikkje til hinder for at kritikkverdige forhold kan varslast til lovfesta offentlege tilsyn.



## 5 Handsaming av varsel

Når det vert varsla om kritikkverdige forhold i organisasjonen, er det arbeidsgivar si plikt å syte for at varselet vert tilstrekkeleg undersøkt innan rimelig tid.

### 5.1 Mottak av varsel

Hovudregelen er at alle kommunen sine dokument er offentlege med mindre det fins unntak i lov som hindrar dette. Varsling vil ofte komme inn under unntaka i følgjande lover:

- Offentleglova § 13: opplysningar underlagt lovfesta teieplikt, jf. Forvaltningslova § 13
- Offentleglova § 23 dokument som kan unnatakast for å sikre ei forsvarleg gjennomføring av kommunen si personalforvaltning
- Offentleglova § 24 Dokument som omhandlar lovbrøt kan bli unnateke innsyn.

### 5.2 Oppfølging av varsel

Varslar skal følgjast opp i samsvar med Forvaltningslova og Arbeidsmiljøloven 2A.

### 5.3 Oppfølging av den som varslar

Arbeidsgivar skal syte for at den som har varsla har eit fullt forsvarleg arbeidsmiljø. Dersom det er naudsynt, skal arbeidsgivar syte for tiltak for å førebygge gjengjelding. Det betyr mellom anna at identiteten til den som varslar ikkje skal gjerast kjent for fleir enn strengt naudsynt.

Den som varslar skal ha stadfesting på motteke varsel, seinast innan ei veke.

I Tysnes kommune ønskjer me å gje den som varslar informasjon om utfallet av saken.

a) I nokre saker kan informasjon til den som varslar avgrensast av teieplikt, eller dersom det er ei personalsak. Me skal alltid strekke oss etter å ivareta den som varslar med tilstrekkelig informasjon. Viss me ikkje kan gje anna informasjon, vil me søkje å informera om kva tid me reknar saka er avslutta.

b) Dersom tilbakemelding ikkje vert hindra av teieplikta, skal tilbakemelding om utfallet av saka bli gitt seinast ei veke etter at handsaming av saka er avslutta.





#### **5.4 Oppfølging av den det vert varsla om**

Arbeidsgivar skal handsama varsel på ein slik måte at det ivaretek arbeidsmiljøet, og den det eventuelt vert varsla om. Ein kan aldri utelukka at ordninga med varsling vert misbrukt til å sverte andre. Før varselet er gjennomgått må det difor handsamast med stor varsemd.

Dersom saka vert følgt opp vidare, skal den det vert varsla om så tidleg som mogleg få skriftleg informasjon om at det er motteke varsel. Tilsette som det vert varsla, vil som hovudregel ha rett til å uttala seg i saka.

Hovudregelen er at den det vert varsla om har partsinnsyn i alle opplysningar i varselet. Dersom det ikkje ligg føre spesielle forhold, inkluderer dette informasjon om kven som har fremja varselet.

#### **5.5 Varslar som omfattar rådmann eller ordførar**

Dersom det vert varsla om rådmann eller ordførar vil formannskapet virka som sekretariat og kommunestyre som besluttande organ.

#### **5.6 Rapportering**

Dersom det kritikkverdige forholdet er relevant for kommunen sitt arbeid med helse, miljø og tryggleik, skal det rapportert til Arbeidsmiljøutvalet. Slike varsel skal inn i årsrapporten for vernearbeidet i kommunen.





---

Saksframlegg

---

**Saksnr:** 2022/98-4  
**Saksbehandlar:** Helge Inge Johansen

---

### Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	20/23	05.10.2023

## Vurdering av om Deloitte er uavhengig i høve Tysnes kommune

### Forslag til vedtak

Kontrollutvalet tar eigenvurderinga frå ansvarleg revisor, Unni-Renate Moe, vedrørande om Deloitte AS er uavhengig i høve Tysnes kommune, til etterretning.

### Samandrag

Føremålet med denne saka er at kontrollutvalet skal ta stilling til om Deloitte er uavhengig i høve Tysnes kommune. Vedlagte uavhengighetserklæring ligg til grunn for handsaming av denne saka.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

Vedlegg

1 Uavhengighetserklæring 2023 Tysnes kommune

## Saksutgreiing

### Bakgrunn for saka

I samsvar med Forskrift om kontrollutvalg og revisjon skal ansvarleg revisor for kommunar og fylkeskommunar løpande vurdere sin uavhengighet. Oppfølging av dette kravet ligg til kontrollutvalet.

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse i denne saka jf. Kommunelova § 23-2, jf. Forskrift om kontrollutvalg og revisjon §§ 16 og 19.

### Vurderingar og verknader

I kommunelova § 23-2 Kontrollutvalgets ansvar og myndighet står det m.a. dette:

*«Kontrollutvalget skal påse at*

*a) kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte»*

I Forskrift om kontrollutvalg og revisjon § 16 Krav til revisors uavhengighet står det dette:

*«Revisor kan ikke utføre revisjon eller annen kontroll for kommunen eller fylkeskommunen hvis det foreligger særegne forhold som er egnet til å svekke tilliten til revisorens uavhengighet og objektivitet.*

*Ansettelse som revisor i kommunen eller fylkeskommunen eller i en interkommunal samarbeidsordning medfører ikke i seg selv at revisoren mangler nødvendig uavhengighet og objektivitet.»*

Vidare står det i § 19 Krav til egenvurdering av uavhengighet i same forskrift dette:

*«Den som utfører revisjon eller annen kontroll for en kommune eller fylkeskommune, skal løpende vurdere sin uavhengighet.*

*Oppdragsansvarlig revisor skal hvert år, og ellers ved behov, gi en skriftlig egenvurdering av sin uavhengighet til kontrollutvalget.*

*En skriftlig egenvurdering om revisjonens uavhengighet skal følge alle tilbud om revisjon.»*

Ansvarleg revisor hjå Deloitte, Unni Renate Moe, har no sendt over ei slik egenvurdering dagsett 20.09.2023. Denne ligg ved saka.

Som det går fram av kommunelova har kontrollutvalet ansvar for å sjå til at kommunen har ein tryggande revisjon. Kontrollutvalet si behandling av ansvarleg revisor si egenvurdering, vil vera ein lekk i å sjå til dette.

I nokre kommunar har revisor utført oppgåver / prosjekt for kommunen, som ikkje er bestilt av kontrollutvalet. Det er ingen ting i vegen for at dette kan gjennomførast, dersom det ikkje kjem i konflikt med uavhengigheit og objektivitet eller er arbeid av stort omfang. Det bør difor opplysast om revisor har utført oppdrag for kommunen ut over det som er bestilt av kontrollutvalet, og storleiken på oppdraget. Sekretariatet har fått avklart i epost 22.09.2023 frå Deloitte at ein ikkje har hatt andre oppdrag.

### Konklusjon

Ut frå innhaldet i eigenerklæringa vert det tilrådd å ta informasjonen til etterretning.



# PENNEO

Signaturene i dette dokumentet er juridisk bindende. Dokument signert med "Penneo™ - sikker digital signatur".  
De signerende parter sin identitet er registrert, og er listet nedenfor.

"Med min signatur bekrefter jeg alle datoer og innholdet i dette dokument."

## Unni-Renate Moe

Statsautorisert revisor

Serienummer: 9578-5995-4-99839

IP: 51.174.xxx.xxx

2023-09-19 09:32:26 UTC



Penneo Dokumentnøkkel: 2CEJ4-KBMZNI-HJ8KO-IEQ2X-P7F1O-71PMJ

Dokumentet er signert digitalt, med **Penneo.com**. Alle digitale signatur-data i dokumentet er sikret og validert av den datamaskin-utregnede hash-verdien av det opprinnelige dokument. Dokumentet er låst og tids-stemplet med et sertifikat fra en betrodd tredjepart. All kryptografisk bevis er integrert i denne PDF, for fremtidig validering (hvis nødvendig).

### Hvordan bekrefter at dette dokumentet er originalen?

Dokumentet er beskyttet av ett Adobe CDS sertifikat. Når du åpner dokumentet i

Adobe Reader, skal du kunne se at dokumentet er sertifisert av **Penneo e-signature service** <[penneo@penneo.com](mailto:penneo@penneo.com)>. Dette garanterer at innholdet i dokumentet ikke har blitt endret.

Det er lett å kontrollere de kryptografiske beviser som er lokalisert inne i dokumentet, med Penneo validator - <https://penneo.com/validator>



---

Saksframlegg

---

**Saksnr:** 2022/96-25  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	21/23	05.10.2023

## Revisjonsplan og risikovurdering i samband med etterlevingskontroll av økonomiforvaltninga i 2023

### Forslag til vedtak

1. Kontrollutvalet tek Deloitte sin presentasjon av revisjonsplan og risikovurdering i samband med forenkla etterlevingskontroll av økonomiforvaltninga til orientering.
2. Utvalet ber om at interimrevisjonsrapport 2023 vert klar til behandling i møte i kontrollutvalet 23.11.2023 med frist for levering til sekretariatet 02.11.2023.
3. Kontrollutvalet ber også om at uttale om resultatet av den forenkla etterlevingskontrollen vert levert til same møtet som årsrekneskapen for 2023 skal behandlast, normalt i mai-møtet 2024, sjølv om den nasjonale fristen er sett til 30.06.

### Samandrag

Kontrollutvalet i Tysnes kommune har ansvar for at det vert gjennomført rekneskapsrevisjon i kommunen. I denne saka skal den valde revisor, Deloitte, presentere sin plan for gjennomføring av rekneskapsrevisjonen, kva som er gjort av rekneskapsrevisjon så langt og risiko- og vesentlegvurdering dei har føreteke om forenkla etterlevingskontroll for 2023.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

### Vedlegg

- 1 Revisjonsplan og risikovurdering 2023 Tysnes kommune
- 2 Risiko-og vesentlighetsvurdering FEØ 2023 Tysnes kommune

## Saksutgreiing

### Bakgrunn for saka

Kontrollutvalet i Tysnes kommune har ansvar for at det vert gjennomført rekneskapsrevisjon i kommunen på ein tryggande måte. Denne saka er eit ledd i oppfølginga av dette.

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse i denne saka, jf. Kommunelova § 23-2 Kontrollutvalgets ansvar og myndighet som lyd m.a. slik

*«Kontrollutvalget skal påse at*

- a) kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte*
- b) det føres kontroll med at den økonomiske forvaltningen foregår i samsvar med gjeldende bestemmelser og vedtak»*

På bakgrunn av punkt b) over står det dette i kommunelova § 24-9 Forenklet etterlevelseskontroll med økonomiforvaltningen:

*«Regnskapsrevisor skal se etter om kommunens eller fylkeskommunens økonomiforvaltning i hovedsak foregår i samsvar med bestemmelser og vedtak.*

*Revisor skal basere oppgaven på en risiko- og vesentlighetsvurdering, som skal legges fram for kontrollutvalget. Revisor skal innhente tilstrekkelig informasjon til å vurdere om det foreligger brudd på lover, forskrifter eller vedtak, der bruddet er av vesentlig betydning for økonomiforvaltningen.*

*Revisor skal senest 30. juni avgi en skriftlig uttalelse til kontrollutvalget, med kopi til kommunedirektøren, om resultatet av kontrollen.»*

Vidare går det fram av Forskrift om kontrollutvalg og revisjon § 3 m.a. dette:

*«Kontrollutvalget skal holde seg løpende orientert om revisjonsarbeidet og påse at*

- a) kommunens eller fylkeskommunens årsregnskaper blir revidert på en betryggende måte*
- b) regnskapsrevisjonen utføres i samsvar med lov, forskrift og kontrollutvalgets instruksjer og avtaler med revisor*
- c) regnskapsrevisjonen blir utført av revisorer som oppfyller kravene i kapittel 2 og 3.»*

### Vurderingar og verknader

Etter sekretariatet si oppfatning er Deloitte sin revisjonsplan 2023 og revisor si risiko- og vesentlegvurdering om forenkla etterlevingskontroll av økonomiforvaltninga for 2023 to sider av same sak. Det er difor naturleg at desse to tilhøva vert handsama i same sak.

Kontrollutvalet si behandling av revisjonsplan, informasjon om rekneskapsrevisjonen så langt og risiko- og vesentlegvurdering i høve forenkla etterlevingskontroll som skal utførast i 2023, vil vere eit ledd i å sjå til at kommunen sin rekneskap vert revidert på ein tryggande måte. Revisjonsplanen og risikovurderinga for etterlevingskontroll er vedlagt saka.

Når det gjeld kontrollutvalet sitt ansvar i høve kommunelova § 24-9 om forenkla etterlevingskontroll av økonomiforvaltninga er det naturleg at Deloitte legg fram sin uttale om resultatet av denne i same møte som årsrekneskaperen for 2023 skal behandlast, normalt i mai-møtet i 2024, sjølv om den nasjonale fristen er sett til 30.06.

**Konklusjon**

Dersom det ikkje kjem fram noko spesielt i møtet vert det tilrådd at kontrollutvalet tar informasjonen frå Deloitte til orientering.

Vidare vert det tilrådd at kontrollutvalet ber om at interimrevisjonsrapport 2023 vert klar til behandling i møte i kontrollutvalet 23.11.2023, med frist for levering til sekretariatet innan 02.11.2023.

Det vert også tilrådd at kontrollutvalet ber om at uttale om resultatet av den forenkla etterlevingskontrollen vert levert til same møte som årsrekneskapen for 2023 skal behandlast, normalt i mai-møtet i 2024, sjølv om den nasjonale fristen er sett til 30.06.





## Revisjonsplan og risikovurdering 2023

Tysnes kommune



**MAKING AN  
IMPACT THAT  
MATTERS**  
*since 1845*

# Revisjonsplan

Tysnes kommune 2023

September

Oktober/november

November

Februar-april

April/mai



Revisjonsplan,  
risikovurdering revisjon og  
risiko- og  
vesentlegheitsvurdering  
forenkla  
etterlevingskontroll med  
økonomiforvaltinga vert  
handsama i kontrollutvalet

Interimrevisjon  
oktober/november

Oppstartsmøte med  
administrasjon

Kartlegging av rutinar og testing av  
kontrollar

Detaljkontrollar inntekter og  
utgifter

Oppsummering  
interimrevisjon vert  
handsama i kontrollutvalet

Årsoppgjer  
februar-april

Balansepostar

Årsmelding

Konsolidert rekneskap

Forenkla etterlevingskontroll  
økonomiforvalting

Årsmelding, årsrekneskap,  
revisjonsmelding,  
revisjonsrapport og uttale  
frå forenkla  
etterlevingskontroll med  
økonomiforvaltinga vert  
handsama i kontrollutvalet

Attestasjonar

# Risikovurdering

Tysnes kommune 2023



Låg



Middels



Høg

Område	Kommentar	Risikonivå
Inntekter	Mange og store transaksjonar av ulik art og incentiv for mislegheiter knytt til inntektsføring.	
Meirverdiavgift	Komplisert regelverk, mange transaksjonar, mange tilsette involvert i prosessering av inngående faktura og utfakturering. Risiko for forelding ved meirverdiavgiftskompensasjon og at kommunen urettmessig gjer krav på kompensasjon.	
Pensjon	Vesentlege forpliktingar og midlar, kompliserte regelverk og rekneskapsmessig handsaming, viktig for den enkelte tilsette at opplysningar er korrekt registrerte hos pensjonsleverandør.	
Skilje investering/drift	Forskrift og standard regulerer avgrensing. Vesentleg for tilgang til lånefinansiering.	
Utgifter	Risiko knytt til regelverk for offentleg anskaffing og mange tilsette involvert i prosessering av inngående faktura.	
Anleggsmidlar	Vesentlege verdier. Risiko for feilaktig aktivering og manglande avskrivningar. Store investeringar.	

# Risikovurdering

Tysnes kommune 2023



Låg



Middels



Høg

Område	Kommentar	Risikonivå
Bank	Risiko knytt til tilgang til bankkontoar og utbetalingsrutinar.	Middels
Låneopptak	Låneopptak vert regulert av kommunelov og kommunestyret sitt budsjettvedtak. Minimumsavdrag viktig storleik.	Middels
Bundne fond	Risiko for at avsetjing og bruk ikkje er i høve lov, forskrift eller gjevar sine vilkår.	Middels
Avslutting av rekneskapen	Kommunestyret sitt budsjettvedtak set rammer for disponering og inndekking. Budsjett- og rekneskapsforskrifta regulerer avslutning. Historisk avdekka feil knytt til avslutting av rekneskapen.	Middels
Kundefordringar	Fordringsmasse består av mange mindre fordringar, liten risiko for vesentlege feil. Risiko for svakheit i rutinar for purring og tapsavsetjing. Risiko for tap låg for kommunale avgifter og eigedomsskatt grunna legalpant.	Middels
Andre kortsiktige fordringar	Risiko for at verdi på fordring ikkje er til stades. Risiko knytt til storleik på krav ressurskrevande tenester grunna nøyaktighet og tidsriktigheit av utrekning.	Middels

# Risikovurdering

Tysnes kommune 2023



Låg



Middels



Høg

Område	Kommentar	Risikonivå
Aksjar og andelar	Risiko for at verdi på aksjene ikke er til stades.	
Noteopplysingar	Risiko for at notar inneheld feil eller at forskriftsbestemte noteopplysingar manglar.	
Annan kortsiktig gjeld	Risiko for at ikkje all gjeld er bokført eller at gjelda er forfalt.	
Leverandørgjeld	Risiko for at ikkje all gjeld er bokført eller at gjelda er forfalt.	
Offentlege avgifter	Risiko for manglar og feil ved innberetning meirverdiavgift, arbeidsgjevaravgift og forskotstrekk. Risiko for at offentlege avgifter ikkje vert betalt tidsriktig og at det ikkje er tilstrekkeleg med midlar på skattetrekkkonto.	
Løn	Svært mange transaksjonar gjev liten risiko for vesentlege feil i rekneskapen. Velfungerande prosess, rutinar og kontrollar.	
Reiseutgifter	Risiko for at formalkrav og dokumentasjonskrav ikkje vert etterlevd. Elektronisk handsaming med attestering og anvising reduserer risiko.	



# Forenklet etterlevelseskontroll med økonomiforvaltningen 2023

## Risiko- og vesentlighetsvurdering

- 1 Utlån - startlån
- 2 Investeringsprosjekter
- 3 Selvkost
- 4 Offentlig støtte



- Utlån startlån MNOK 20,9 per 31.12.2022
- Økning i utlån siste to år
- Etterspørsel og risiko økt jf. den makroøkonomiske utviklingen
- Outsourcet tjeneste

**«Hvordan sikrer Tysnes kommune tilfredsstillende internkontroll på utlån?»**



---

Saksframlegg

---

**Saksnr:** 2023/406-1  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	22/23	05.10.2023

## Plan for forvaltningsrevisjon for perioden 2024-2028 - Bestilling av prosjektplan

### Forslag til vedtak

1. Kontrollutvalet ber Deloitte innan 02.11.2023, laga eit forslag til prosjektplan som bl.a. inneheld korleis analyse- og planarbeidet skal gjennomførast, ressursbruk og forventa levering.

Prosjektplanen skal omfatta:

- a. Korleis risiko- og vesentlegvurdering av Tysnes kommune si verksemd og verksemda i kommunen sine selskap skal gjennomførast.
  - b. Forslag til korleis arbeidet med plan for forvaltningsrevisjon for perioden 2024 – 2028 skal gjennomførast.
2. Forslag til prosjektplan skal leggjast fram for godkjenning i kontrollutvalet sitt møte 23.11.2023.
  3. Kontrollutvalet ber om at prosessen vert lagt opp slik at forslag til plan for forvaltningsrevisjon kan leggjast fram for kommunestyret i juni 2024.

### Samandrag

I starten av ny valperiode skal det utarbeidast ny plan, slik det kjem fram av kommuneloven. Bestilling av dette planarbeidet vert gjennomført i siste møte i valperioden, slik at det nye kontrollutvalet får handsama dette i første møte. Ein tek sikte på at kommunestyret skal godkjenne planen i første halvår 2024.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*



## Saksutgreiing

### Bakgrunn for saka

Av § 23-3 kjem det fram bl.a. dette gjeldande forvaltningsrevisjon:

*«Kontrollutvalget skal minst én gang i valgperioden, og senest innen utgangen av året etter at kommunestyret eller fylkestinget er konstituert, utarbeide en plan som viser på hvilke områder det skal gjennomføres forvaltningsrevisjoner. Planen skal baseres på en risiko- og vesentlighetsvurdering av kommunens eller fylkeskommunens virksomhet og virksomheten i kommunens eller fylkeskommunens selskaper. Hensikten med risiko- og vesentlighetsvurderingen er å finne ut hvor det er størst behov for forvaltningsrevisjon. Planen skal vedtas av kommunestyret og fylkestinget selv. Kommunestyret og fylkestinget kan delegerer til kontrollutvalget å gjøre endringer i planen.»*

Nytt i forhold til gjeldande kommunelov er at plan for forvaltningsrevisjon no og skal innehalda eventuelle forvaltningsrevisjonar i selskap som kommunen har eigarskap i.

Dette inneber at kontrollutvalet innan utgangen av 2024 må sørgja for:

- å gjennomføra ei risiko- og vesentlegvurdering av kommunen si verksemd og verksemda i kommunen sine selskap.
- å utarbeida ein plan for gjennomføring av forvaltningsrevisjon i perioden 2020 – 2024 basert på den gjennomførte risiko og vesentlegvurderinga
- at planen blir vedteken av kommunestyret, som kan delegera til kontrollutvalet å føreta endringar i planperioden.
- fram til ny plan er vedteken vil plan for forvaltningsrevisjon 2020 – 2024 gjelda

### Vedtakskompetanse

Kontrollutvalet har i tråd med kommunelova §§ 23 og 24 vedtakskompetanse for å dra i gang og gjennomføre prosess med å utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll og kommunestyret skal gjere vedtak i saka.

### Vurderingar og verknader

Gjennomføring av ei risiko- og vesentlegvurdering av kommunen si verksemd og verksemda i kommunen sine selskap, og utarbeiding av forslag til plan for forvaltningsrevisjon, kan gjerast av den valde revisor, sekretariatet eller anna eksternt selskap med kompetanse på området. Det som er mest vanleg i dei kommunar me er sekretariat for er å be den valde revisor, Deloitte, gjennomføra oppdraget.

Deloitte har vore revisor for kommunen nokre år og kjenner organisasjonen temmeleg godt. Det gjer at dei vil ha eit godt grunnlag for å gjennomføra dette arbeidet på ein god måte. Kontrollutvalet bør og drøfta seg fram til enkelte føringar for gjennomføring av arbeidet. Slike føringar kan f.eks. vera kven som bør involverast i gjennomføringa av risiko og vesentlegvurderinga, i kor stor grad kontrollutvalet sjølv bør involverast i arbeidet, kor djupt skal analysen gå (omfanget), kor mange timar skal ein kunna bruka på jobben og når skal arbeidet leverast ferdig til kontrollutvalet for endeleg handsaming. Denne drøftinga bør munna ut i ei skisse for vidare framdrift i saka.

Det skal og utarbeidast plan for eigarskapskontroll i løpet av 2024, jf. anna sak til dette møtet, og det vil vera føremålstenleg og kostnadssparande å sjå arbeidet med utarbeiding av begge planane under eitt. Dersom ein skal dela dette arbeidet opp i eit prosjekt innan forvaltningsrevisjon, og eit prosjekt innan eigarskapskontroll, vil det truleg føra til meir ressursbruk.

**Konklusjon**

Sekretariatet tilrår at kontrollutvalet ber Deloitte utarbeida forslag til prosjektplan for arbeidet med gjennomføring av risiko- og vesentlegvurderingar av Tysnes kommune si verksemd og verksemda i kommunen sine selskap. Vidare bør prosjektplanen omfatta utarbeiding av forslag til plan for forvaltningsrevisjon for perioden 2024 – 2028, inkludert ressursbruk og forventa levering.



---

Saksframlegg

---

**Saksnr:** 2023/407-1  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	23/23	05.10.2023

## Plan for eigarskapskontroll for perioden 2024-2028 - Bestilling av prosjektplan

### Forslag til vedtak

1. Kontrollutvalet ber Deloitte innan 02.11.2023, laga eit forslag til prosjektplan, som bl.a. inneheld korleis analyse- og planarbeidet skal gjennomførast, ressursbruk og forventa levering.

Prosjektplanen skal omfatta:

- a. Korleis risiko og vesentlegvurdering av Tysnes kommune sine eigarskap i selskap skal gjennomførast
  - b. Forslag til korleis arbeid med plan for eigarskapskontroll for perioden 2024 – 2028 skal gjennomførast.
2. Forslag til prosjektplan skal leggjast fram for godkjenning i kontrollutvalet i første møte for det nye kontrollutvalet, 23.11.2023.
  3. Kontrollutvalet ber om at prosessen blir lagt opp slik at forslag til plan for eigarskapskontroll kan leggast fram for kommunestyret innan juni 2024.

### Samandrag

I starten av ny valperiode skal det utarbeidast ny plan, slik det kjem fram av kommuneloven. Bestilling av dette planarbeidet vert gjennomført i siste møte i valperioden, slik at det nye kontrollutvalet får handsama dette i første møte. Ein tek sikte på at kommunestyret skal godkjenne planen i første halvår 2024.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

### Saksutgreiing

## Bakgrunn for saka

I kommunelova (§ 23-4) kjem det fram slik informasjon gjeldande eigarskapskontroll:

*«Kontrollutvalget skal minst én gang i valgperioden, og senest innen utgangen av året etter at kommunestyret eller fylkestinget er konstituert, utarbeide en plan for hvilke eigarskapskontroller som skal gjennomføres. Planen skal baseres på en risiko- og vesentlighetsvurdering av kommunens og fylkeskommunens eigarskap. Hensikten med risiko- og vesentlighetsvurderingen er å finne ut hvor det er størst behov for eigarskapskontroll. Planen skal vedtas av kommunestyret og fylkestinget selv. Kommunestyret og fylkestinget kan delegere til kontrollutvalget å gjøre endringer i planen.»*

Plan for eigarskapskontroll skal ikkje innehalda forvaltningsrevisjon i selskap som kommunen har eigarskap i. Desse skal eventuelt inn i plan for forvaltningsrevisjon.

Dette inneber at kontrollutvalet innan utgangen av 2024 må sørgja for:

- å gjennomføra ei risiko- og vesentlegvurdering av kommunen sine eigarskap i selskap.
- å utarbeide ein plan for gjennomføring av eigarskapskontroll i perioden 2024 – 2028, basert på den gjennomførte risiko- og vesentlegvurderinga.
- at planen blir vedteken av kommunestyret, som kan delegera til kontrollutvalet å føreta endringar i planperioden.
- fram til ny plan er vedteken vil plan for eigarskapskontroll for perioden 2020-2024 gjelda.

## Vedtakskompetanse

Kontrollutvalet har i tråd med kommunelova §§ 23 og 24 vedtakskompetanse for å dra i gang og gjennomføre prosess med å utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll og kommunestyret skal gjere vedtak i saka.

## Vurderingar og verknader

Gjennomføring av ei risiko- og vesentlegvurdering av kommunen sine eigarskap i selskap, og utarbeiding av forslag til plan for eigarskapskontroll, kan gjerast av den valde revisor, sekretariatet eller anna eksternt selskap med kompetanse på området. Det som er mest vanleg i dei kommunar me er sekretariat for er å be den valde revisor, Deloitte, gjennomføra oppdraget. Deloitte har vore revisor for kommunen nokre år og kjenner organisasjonen temmeleg godt. Det gjer at dei vil ha eit godt grunnlag for å gjennomføra dette arbeidet på ein god måte.

Kontrollutvalet bør og drøfta seg fram til enkelte føringar for gjennomføring av arbeidet. Slike føringar kan f.eks. vera kven som bør involverast i gjennomføringa av risiko og vesentlegvurderinga, i kor stor grad kontrollutvalet sjølv bør involverast i arbeidet, kor djupt skal analysen gå (omfanget), kor mange timar skal ein kunna bruka på jobben og når skal arbeidet leverast ferdig til kontrollutvalet for endeleg handsaming. Denne drøftinga bør munna ut i ei skisse for vidare framdrift i saka.

Det skal og utarbeidast plan for forvaltningsrevisjon i løpet av 2024, jf. anna sak til dette møtet, og det vil vera føremålstenleg og kostnadssparande å sjå arbeidet med utarbeiding av begge planane under eitt. Dersom ein skal dela dette arbeidet opp i eit prosjekt innan forvaltningsrevisjon, og eit prosjekt innan eigarskapskontroll, vil det truleg føra til meir ressursbruk.

## Konklusjon

Sekretariatet tilrår at kontrollutvalet ber Deloitte utarbeida forslag til prosjektplan for arbeidet med gjennomføring av risiko- og vesentlegvurderingar av Tysnes kommune sine eigarskap i selskap. Vidare bør prosjektplanen omfatta utarbeiding av forslag til plan for eigarskapskontroll for perioden 2024 – 2028, inkludert ressursbruk og forventna levering.



---

Saksframlegg

---

**Saksnr:** 2022/101-4  
**Saksbehandlar:** Helge Inge Johansen

---

### Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	24/23	05.10.2023

### Budsjett 2024 for kontrollutvalet

#### Forslag til innstilling

1. Kontrollutvalet godkjenner budsjettforslaget for kontrollarbeidet i Tysnes kommune.
2. Budsjettforslaget skal følgja sak med budsjettarbeidet fram til handsaming i kommunestyret.
3. Kommunestyret gjer endeleg vedtak om budsjett for kontrollarbeidet i 2024.

#### Samandrag

Kontrollutvalet har ansvar for utarbeiding av forslag til budsjett for kontrollarbeidet i kommunen. Forslaget skal følgje innstillinga for årsbudsjettet til kommunestyret, som gjer endeleg vedtak i budsjettsaka.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

#### Vedlegg

- 1 Budsjett 2024 - talark til saka

## Saksutgreiing

### Bakgrunn for saka

I forskrift for kontrollutvalg og revisjon kan ein i § 2 «Kontrollutvalgets rolle i fastsettelsen av budsjett for kontrollarbeidet» står det:

*«Kontrollutvalget skal utarbeide forslag til budsjett for kontrollarbeidet i kommunen eller fylkeskommunen. Forslaget skal følge innstillingen til årsbudsjettet etter kommuneloven § 14-3 tredje ledd til kommunestyret eller fylkestinget.»*

I reglement for politiske organ, som er vedteke av kommunestyret 25.09.2013, ajourført i februar 2018 står det i pkt. 4.6.2:

*Kontrollutvalet skal ha eige budsjett som omfattar kontroll- og tilsynsarbeidet i kommunen. Kontrollutvalet skal laga forslag til budsjett, som skal følgja formannskapet si innstilling til kommunestyret.*

I tråd med forskrifta og reglementet fremjar kontrollutvalet med dette sitt forslag til budsjett for 2024. I budsjettframlegget bereknar kontrollutvalet kostnad med dei oppgåver budsjettet skal dekkja. Det som er særskilt med kontrollarbeidet er at det eigentleg er administrasjonen som vert revidert. Såleis skal kontrollutvalet, i budsjettsaka, innstilla direkte overfor politisk organ.

### Vedtakskompetanse

Kontrollutvalet skal utarbeide budsjettforslag for kontrollarbeidet, medan det er kommunestyret som har vedtakskompetansen i saka, jf. forskrift om kontrollutvalg og revisjon § 2.

### Vurderingar og verknader

Lovgrunnlag.

#### § 23-2.Kontrollutvalgets ansvar og myndighet

Kontrollutvalget skal påse at

- a) kommunens eller fylkeskommunens regnskaper blir revidert på en betryggende måte
- b) det føres kontroll med at den økonomiske forvaltningen foregår i samsvar med gjeldende bestemmelser og vedtak
- c) det utføres forvaltningsrevisjon av kommunens eller fylkeskommunens virksomhet, og av selskaper kommunen eller fylkeskommunen har eierinteresser i
- d) det føres kontroll med forvaltningen av kommunens eller fylkeskommunens eierinteresser i selskaper mv. (eierskapskontroll)
- e) vedtak som kommunestyret eller fylkestinget treffer ved behandlingen av revisjonsrapporter, blir fulgt opp.

#### § 23-3.Forvaltningsrevisjon

*«Forvaltningsrevisjon innebærer å gjennomføre systematiske vurderinger av økonomi, produktivitet, regeletterlevelse, måloppnåelse og virkninger ut fra kommunestyrets eller fylkestingets vedtak.»*

*Kontrollutvalget skal minst én gang i valgperioden, og senest innen utgangen av året etter at kommunestyret eller fylkestinget er konstituert, utarbeide en plan som viser på hvilke områder det skal gjennomføres forvaltningsrevisjoner. Planen skal baseres på en risiko- og vesentlighetsvurdering av kommunens eller fylkeskommunens virksomhet og virksomheten i kommunens eller fylkeskommunens selskaper. Hensikten med risiko- og vesentlighetsvurderingen er å finne ut hvor det er størst behov for forvaltningsrevisjon.*

*Planen skal vedtas av kommunestyret og fylkestinget selv. Kommunestyret og fylkestinget kan delegerer til kontrollutvalget å gjøre endringer i planen.»*

#### **§ 23-4.Eierskapskontroll**

*«Eierskapskontroll innebærer å kontrollere om den som utøver kommunens eller fylkeskommunens eierinteresser, gjør dette i samsvar med lover og forskrifter, kommunestyrets eller fylkestingets vedtak og anerkjente prinsipper for eierstyring.*

*Kontrollutvalget skal minst én gang i valgperioden, og senest innen utgangen av året etter at kommunestyret eller fylkestinget er konstituert, utarbeide en plan for hvilke eierskapskontroller som skal gjennomføres. Planen skal baseres på en risiko- og vesentlighetsvurdering av kommunens og fylkeskommunens eierskap. Hensikten med risiko- og vesentlighetsvurderingen er å finne ut hvor det er størst behov for eierskapskontroll.*

*Planen skal vedtas av kommunestyret og fylkestinget selv. Kommunestyret og fylkestinget kan delegerer til kontrollutvalget å gjøre endringer i planen.»*

Formuleringane i desse paragrafane viser at hovudoppgåvene til kontrollutvalet er å gjennomføra prosjektarbeid ut frå dei planar som kommunestyret har vedteke.

Planar vert lovmessig utarbeidd første heile år etter kommuneval, 2020, 2024 osv. Såleis er det teke med 140 timar til planarbeid for forvaltningsrevisjon og eigarskapskontroll i 2024, for ny planperiode (2024 – 2028).

I kontrollutvalet sitt budsjett bør det leggast inn midlar til å gjennomføra prosjekt innan forvaltningsrevisjon og eigarskapskontroll i tråd med planane. Ut frå gjeldande planar vil prosjektarbeid krevje ei ramme på omlag 300 timar for kommunar med Tysnes kommune sin storleik.

Erfaring frå kommunane dei siste åra viser at det kjem til prosjekt, som kontrollutvalet vert oppmoda om å sjå på, og som ikkje er med i planar for forvaltningsrevisjon / eigarskapskontroll. Dette har ofte ført til kostnader som har medført at kontrollutvalet har måtta be om ekstra midlar / ekstraløyving. Sekretariatet meiner difor at det vil vera rett å leggja inn i budsjettet ein post for ekstra tiltaksmidlar. Dette vil vera midlar som er tenkt til ev. ad-hoc oppgåver, til dømes tiltak som måtte koma til utanom prosjekt frå planane og til utgreiingar som kontrollutvalet finn naudsynt å gjennomføra undervegs i året. Grunnlag for slike ekstra oppgåver kan t.d. vera henvendingar frå innbyggjarar, medieoppslag eller bestillingar frå kommunestyret som ikkje står i godkjend plan. Det er lagt inn 25.000 kroner til denne posten i budsjettforslag for 2024. Dette var også med i budsjett for 2023.

For revisjonstenestene er det teke utgangspunkt i avtalen med ekstern revisor. Budsjettert kostnad med revisjon skal dekkja både arbeid med rekneskapsrevisjon og anna revisjonsarbeid, t.d. prosjekt innan forvaltningsrevisjon og eigarskapskontroll. For 2024 er det budsjettert med auke i tråd med SSB sine berekningar. Det vil det vera ein usikkerhet for 2. halvår i og med at det skal gjennomførast konkurranse om revisjonstenester for ny avtaleperiode (01.07.24 – 30.06.28). Såleis er ikkje kostnaden for andre halvår 2024 kjent enno.

Vidare er det lagt til grunn 5 møte i kontrollutvalet i 2024, med om lag like stor saksmengd som inneverande år. Det er vidare lagt inn kostnader med kurs, og at medlemmane i kontrollutvalet kan delta på fagkonferansar samt servering på utvalsmøta. Folkevaldopplæring for kontrollutvala vert vanlegvis gjennomført i partalsår, som 2020, 2022 og 2024. Derfor er det satt av ei pott til dette i

2024. Elles er det lagt inn møtegodtgjersle og tapt arbeidsforteneste i tråd med godtgjerslereglementet til kommunen.

For sekretariatskostnadene er ny avtale frå 01.01.2023 lagt til grunn. Konkurransen om ny avtale for åra 2023 – 2026 var ikkje avslutta då budsjett 2023 vart utarbeidd. Til grunn for budsjettering 2024 ligg såleis ein pris som gjekk noko opp for ny fireårsperiode, konsumprisregulering ift. avtalen og timetal som tidlegare brukt pr. år.

### **Konklusjon**

På slik bakgrunn tilrår sekretariatet at kontrollutvalet godkjenner framlegg til budsjett. Budsjettframlegget skal så følgja sak med budsjettarbeid fram til handsaming i kommunestyret. Det er kommunestyret som skal gjera endeleg vedtak når det gjeld budsjett for kontrollarbeidet i Tysnes kommune.



## Budsjettforslag for kontrollutvalet i Tysnes kommune for 2024

Konto	Tekst	Budsjett 2022	Budsjett 2023	Budsjett 2024
10800	Godtgjersle folkevalde	kr 24,448	kr 29,734	kr 32,374
	Tapt arbeidsforteneste	kr -	kr -	kr 10,000
	Feriepenger tapt arbeidsforteneste	kr -	kr -	kr 1,200
	Delsum	<b>kr 24,448</b>	<b>kr 29,734</b>	<b>kr 43,574</b>
10990	Arbeidgiveravgift (AGA)	kr 2,592	kr 3,152	kr 4,619
	Delsum	<b>kr 27,040</b>	<b>kr 32,886</b>	<b>kr 48,192</b>
11001	Abonnement og faglitteratur	kr 11,500	kr 11,500	kr 12,000
11150	Matvarer / servering	kr 3,000	kr 3,000	kr 3,000
11500	Opplær./kursutg./folkev.opplæring	kr 35,000	kr 15,000	kr 35,000
11600	Skyss- og kostgodtgjøring	kr 5,000	kr 5,000	kr 5,000
11955	Kontingentar	kr 3,700	kr 3,700	kr 4,000
13300	Kjøp av sekretariatstenester	kr 158,725	kr 164,875	kr 192,310
13700	Revisjonstenester	kr 583,570	kr 623,308	kr 855,529
12700	Ekstra tiltaksmidl./konsulenttenester	kr 25,000	kr 25,000	kr 25,000
	Delsum	<b>kr 825,495</b>	<b>kr 851,383</b>	<b>kr 1,131,839</b>
14290	Meirverdiavgift	kr 205,424	kr 211,896	kr 282,010
17290	Moms-kompensasjon	kr -205,424	kr -211,896	kr -282,010
	Total budsjetttramme	<b>kr 852,535</b>	<b>kr 884,269</b>	<b>kr 1,180,031</b>



---

Saksframlegg

---

**Saksnr:** 2022/102-7  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	25/23	05.10.2023

## Gjennomgang av møteprotokollar frå andre politiske utval

### Forslag til vedtak

Kontrollutvalet tar møteprotokollane som går fram av saksutgreiinga til orientering.

### Samandrag

Gjennomgang av møteprotokollar frå andre politiske utval er nyttig. Då kan utvalet halde seg orientert om kva som skjer i kommunen og andre politiske utval. Det vert tilrådd at kontrollutvalet tar ein gjennomgang av desse.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

## Saksutgreiing

### Bakgrunn for saka

Gjennomgang av møteprotokollar frå politiske organ vert sett på saklista til kontrollutvalet til kvart møte. Møteprotokollane kan lastast ned frå Tynesnes kommune si heimeside. Protokollane gjev primært informasjon om dei sakene som har vore til politisk handsaming. Kontrollutvalet kan be om nærare informasjon om enkeltsaker og drøfte ulike problemstillingar som ein finn av særleg interesse.

Kontrollutvalet har gjort vedtak om at ansvar for gjennomgang av møteprotokollar skal fordelast slik:

Politisk organ:	Kontrollutvalsmedlem:
Kommunestyret	Sigvard M. Madsen
Formannskapet	Lars Heine Kåsa
Tenesteutvalet	Kåre Haugland
Utval for landbruk og teknisk	Britt Ersvær

### Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse til å handsame sak om gjennomgang av møteprotokollar, jf. Kommuneleien § 23-2.

### Vurderingar og verknader

Til dette møtet er det desse møteprotokollane som kan vera aktuell for gjennomgang.

- Kommunestyret 15.06 og 26.09
- Formannskapet 01.06, 15.06 og 07.09
- Tenesteutvalet 30.05, 14.06 og 05.09
- Utval for landbruk og teknisk 13.06 og 05.09

### Konklusjon

Dersom det ikkje kjem fram noko spesielt i gjennomgang av protokollane, blir det tilrådd at kontrollutvalet tar møteprotokollane som går fram av saksutgreiinga over til orientering.



---

Saksframlegg

---

**Saksnr:** 2022/108-3  
**Saksbehandlar:** Helge Inge Johansen

---

### Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	26/23	05.10.2023

### Evaluering av arbeidet i kontrollutvalet i denne perioden

#### Forslag til vedtak

Resultat av evaluering av arbeidet i kontrollutvalet i Tysnes kommune for valperioden 2019 – 2023 vert å leggja fram i kontrollutvalet for valperioden 2023 – 2027.

#### Samandrag

Kontrollutvalet i kommunen har tradisjon for å evaluera kontrollutvalsarbeidet i sitt siste møte i fireårsperioden, og at resultat av evalueringa vert lagt fram for nytt kontrollutval i deira første møte.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

Vedlegg

1 Skjema for evaluering valperioden 2019 - 2023

## Saksutgreiing

### Bakgrunn for saka

Etter at ny kommunelov av 2018 vart iverksett, gav Kommunal- og Distriktsdepartementet (KDD) ut 3. utgåve av kontrollutvalsboka. Lenkje:

<https://www.regjeringen.no/no/dokumenter/kontrollutvalsboka/id2893214/>

Boka er utarbeidd for å styrke arbeidet med eigenkontrollen i kommunane, og er å rekna som ein rettleiar til kommunelova av 2018.

### Vedtakskompetanse

Kontrollutvalet har fullmakt til å evaluera sitt eige arbeid.

### Vurderingar og verknader

I kontrollutvalsboka er evalueringsarbeid mv. omtalt i kapittel 11, med slik oppsummering:

- Kontrollutvalet bør utarbeide ei årsmelding til kommunestyret.
- Kontrollutvalet må følgje opp korleis den kommunale forvaltninga gjennomfører og etterlever vedtaka til kommunestyret i samband med forvaltningsrevisjon og eigarskapskontroll.
- Kontrollutvalet bør gjennomføre evaluering av eige arbeid. Målsetjinga er å sørge for kontinuerleg læring og forbetring. Utvalet bør evaluere samhandlinga med både revisjonen og sekretariatet.
- Det er viktig å involvere både kommunestyret og administrasjonen i evalueringa av arbeidet til kontrollutvalet.
- Ved utgangen av ein periode er det viktig at kontrollutvalet legg til rette for ei god erfaringsoverføring til neste kontrollutval.

No er snart valperioden 2019 – 2023 ferdig og det kan, etter sekretariatet si meining, vere bra at det blir gjennomført ei evaluering av det arbeidet kontrollutvalet har gjort i denne valperioden, i tråd med det som går fram over. Dette kan gjerast f.eks. ved at kontrollutval, sekretariat og revisjon saman drøfter aktuelle spørsmål som omhandlar evaluering og erfaringsoverføring til nytt kontrollutval. Sekretariatet har utarbeidd eit skjema med forslag til spørsmål som kan brukast i ei slik evaluering. Skjemaet ligg ved. Ordførar og rådmann også invitert til å delta i evalueringa.

### Konklusjon

Sekretariatet rår til at det blir gjennomført ei evaluering i dette møtet. Evalueringa bør resultera i eit forslag til ev. endringar/forbetringar i rutineane som kan gjera arbeidet med eigenkontrollen i kommunen endå betre. Resultatet av evalueringa bør leggjast fram for kontrollutvalet for valperioden 2023 – 2027, fortrinnsvis i deira første møte.

## Skjema for evaluering av arbeidet i kontrollutvalet i Tysnes kommune, valperioden 2019 – 2023.

Kontrollutvalet (heretter kalla KUV), ordførar, rådmann, revisor og sekretariatet vert invitert til å gjennomføre evaluering av arbeidet i KUV i valperioden 2019 – 2023. Evalueringa inneheld desse spørsmåla:

Nr.	Spørsmål	Svar
1	I kva grad blir møta leia og gjennomførte på ein effektiv og engasjerande måte? Kva kan gjerast betre?	
2	Er talet på møte tilstrekkeleg i høve til saksmengda?	
3	Korleis vert kvaliteten på møtepapira vurdert?	
4	Kor nøgd er du med møtelokala?	
5	Klarar KUV å fylle kontrollfunksjonen på ein god måte? Kva kan gjerast betre?	
6	I kva grad har KUV hatt økonomiske rammer til å gjennomføre oppgåvene på ein god måte?	
7	Korleis blir KUV oppfatta av andre sentrale aktørar, slik som kommunestyret og administrasjonen?	
8	Har kommunestyret og administrasjonen forståing av kva rolle og ansvar KUV har? Korleis kan KUV bidra til ei god forståing?	
9	Er det klare roller og klår ansvarsdeling mellom KUV, kommunestyret og administrasjonen?	
10	I kva grad er KUV synleg nok på kommunen si heimeside?	
11	Bør KUV gjere meir og/ eller mindre av noko?	
12	Korleis fungerer samhandlinga med revisor – både i høve administrasjonen og KUV? Kva kan gjerast betre?	
13	Korleis fungerte arbeidet med plan for forvaltningsrevisjon og plan for eigarskapskontroll?	
14	Korleis fungerer samhandlinga med sekretariatet - både i høve administrasjonen og KUV ? Kva kan gjerast betre?	
15	Korleis fungerer arbeidet med henvendingar til kontrollutvalet: - Frå innbyggjarar - Tilsette - Andre folkevalde - Media - Andre	
16	Kva bør folkevaldopplæringa for det nye KUV innehalde? - Forslag til tema? - Er det sett av tilstrekkeleg med ressursar til opplæring.	

17	Folkevaldopplæring for kommunestyret (KS): <ul style="list-style-type: none"><li>- Er det lagt planar for dette?</li><li>- Bør KUV få delta her?</li><li>- Bør roller og ansvar for KUV presenterast her?</li></ul>	
18	Andre innspel til nytt utval	



---

Saksframlegg

---

**Saksnr:** 2022/95-7  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	27/23	05.10.2023

## Eventuelt

### Forslag til vedtak

Saka vert lagt fram utan forslag til vedtak.

### Samandrag

Det vert lagt opp til å ha eventuelt på saklista for å ivareta det enkelte medlem i utvalet si mogelegheit til sjølv å ta opp saker eller for å gje utvalet mogelegheit til å gjere vedtak i saker som ikkje er på saklista.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*



## **Saksutgreiing**

### **Bakgrunn for saka**

Vedtak i kontrollutvalet 09.03.2020 i PS 9/20 der utvalet vedtok å ha eventuelt som sak i kvart møte.

### **Vedtakskompetanse**

Kontrollutvalet har vedtakskompetanse i denne saka, jf. kommunelova § 11-3 og § 23-2.

### **Vurderingar og verknader**

Dersom det blir tatt opp saker som krev nærare undersøkingar, eller innhenting av fleire opplysningar, før ein kan konkludere med at det er ei sak for kontrollutvalet, bør utvalet be sekretariatet førebu sak om dette til neste møte

### **Konklusjon**

Føremålet med saka er å gje opning for å få nærare undersøkingar av saker som kontrollutvalet ynskjer å få utgreidd til neste møte, eventuelt til eit seinare møte i utvalet. Saka kan utover dette nyttast til å be om orienteringar frå rådmannen eller andre i eit seinare møte.



---

Saksframlegg

---

**Saksnr:** 2023/371-5  
**Saksbehandlar:** Helge Inge Johansen

---

## Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	28/23	05.10.2023

## Konkurransetsetting av revisjonstenester - forslag til konkurransegrunnlag

### Forslag til vedtak

1. Forslag til konkurransegrunnlag, med dei endringane som kom fram i møtet, vert vedteke.
2. Sekretariatet får fullmakt til å gjera naudsynte redaksjonelle og strukturelle endringar i konkurransegrunnlaget før det vert send ut.

### Samandrag

Det er kommunestyret sjølv som skal velgje revisor for kommunen. Vedtaket vert gjort etter innstilling frå kontrollutvalet, som gjennomfører prosessen fram til val av revisor.

Hogne Haktorson  
kontrollsjef

Helge Inge Johansen  
spesialrådgjevar

*Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift*

## Saksutgreiing

### Bakgrunn for saka

Tysnes kommune nyttar konkurranseutsetting av revisjonstenestene. Noverande avtaleperiode for revisjonstenester for kommunen gjeld til og med revisjon av rekneskapen for 2023, det vil seia til og med 30.6.2024. Frå 1.7.2024 må revisor for ny avtaleperiode vera på plass.

### **Kontrollutvalet la fram slik innstilling til kommunestyret som vart vedteke i sak 12/23 i møte 11.05.2023:**

#### *Innstilling*

1. *Kommunestyret gir kontrollutvalet fullmakt til å gjennomføra ny konkurranse om val av revisor for Tysnes kommune. Tidsramma må leggjast slik at den som vert vald ut frå konkurransen, er revisor f.o.m. 01.07.2024.*
2. *Fullmakta omfatter gjennomføring av heile prosessen, herunder:*
  - *Utarbeiding og godkjenning av tilbodsdokument*
  - *Knytte til seg naudsynt hjelp.*
  - *Vurdere mottekne tilbod og innstillta overfor kommunestyret på val av revisor.*

### **Vedtakskompetanse**

Det er kontrollutvalet som har vedtakskompetanse til å gjennomføre prosess med konkurranseutsetting av revisjonstenestene og lage innstilling til kommunestyret på val av revisor, medan det er kommunestyret sjølv som gjer vedtak, jf. kommunelova § 24-1.

### **Vurderingar og verknader**

I tråd med vedtaket over vert forslag til konkurransegrunnlag lagt fram for kontrollutvalet. Sekretariatet har saman med jurist utlånt frå innkjøpsseksjonen i Vestland fylkeskommune utarbeida forslag til konkurransegrunnlag. Kontrollutvalet må gjennomgå og ta stilling til dei aktuelle dokumenta som viser forslag til område som konkurransegrunnlaget skal omfatte, og som blir lyst ut på DOFFIN.

Konkurransegrunnlaget er unnateke offentleggjering etter offentleglova § 23, 3. avsnitt. Det er planlagt at dokumenta vert synt for kontrollutvalet på skjerm i møtet. Alternativt vert dokumenta delt ut på papir i møtet, gjennomgått og samla inn igjen for makulering. Det vert tilrådd at møtet vert lukka under behandlinga av denne saka med heimel i kommunelova § 11-5, jf. offl. § 14. Det må bereknast god tid for kontrollutvalet til gjennomgang og drøfting av innhaldet.

Kontrollutvalet bør gje sekretariatet fullmakt til å gjera naudsynte redaksjonelle og strukturelle endringar i konkurransegrunnlaget før det vert lagt ut på DOFFIN.

### **Konklusjon**

Kontrollutvalet gjennomgår anbodsdocumenta i møtet, vedtar innhaldet i konkurransegrunnlaget og gjev sekretariatet fullmakt til å gjera naudsynte redaksjonelle og strukturelle endringar i anbodsdocumenta før dei vert lagt ut på DOFFIN.

Fra: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]  
Sendt: 07.08.2023 14:07:00  
Til: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]  
Tittel: VS: FKT Medlemsinfo juni 2023

---

**Fra:** Hogne Haktorson <Hogne.Haktorson@vlfk.no>  
**Sendt:** torsdag 29. juni 2023 09:12  
**Til:** Roald Breistein <Roald.Breistein@vlfk.no>; Kjartan Haugsnes <Kjartan.Haugnes@vlfk.no>; Helge Inge Johansen <Helge.Inge.Johansen@vlfk.no>; Einar Kåre Ulla <Einar.Kare.Ulla@vlfk.no>  
**Emne:** VS: FKT Medlemsinfo juni 2023

Til orientering.

HH

---

**Fra:** Forum for Kontroll og Tilsyn <[fkt@fkt.no](mailto:fkt@fkt.no)>  
**Sendt:** fredag 23. juni 2023 14:04  
**Til:** Forum for Kontroll og Tilsyn <[fkt@fkt.no](mailto:fkt@fkt.no)>  
**Emne:** FKT Medlemsinfo juni 2023

Til FKTs medlemmer  
v/kontrollutvalgsledere og ansatte i sekretariat

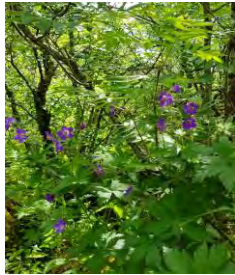
Se vedlagte dokument

*Med vennlig hilsen*

**Anne-Karin Femanger Pettersen**  
Generalsekretær

---

**Forum for kontroll og tilsyn** / Postboks 41 Sentrum, 0101 Oslo / [fkt@fkt.no](mailto:fkt@fkt.no) / +47 414 71 166 / [www.fkt.no](http://www.fkt.no)



23. juni 2023

## Kjære medlemmer

Mange av dere folkevalgte vil sannsynligvis ikke fortsette i kontrollutvalget etter valget i september. Til dere vil jeg si takk for nå og lykke til med nye prosjekter. Men mange blir sittende, og dere håper jeg å se igjen på konferanser og samlinger.

Vi håper at sekretariatene kan ha nytte av FKTs nye opplæringspakke når utvalgene skal læres opp. Vi håper også at nyvalgte kontrollutvalgsledere vil delta på Kontrollutvalgslederskolen.

Mer informasjon om konferanser og samlinger kommer. Hold deg også oppdatert ved å følge med på [www.fkt.no](http://www.fkt.no).

### OPPLÆRINGSPAKKE FOR NYE KONTROLLUTVALG

[FKTs opplæringspakke](#) inneholder PowerPoint-presentasjoner med disse temaene: (Nedlastning av presentasjonene krever pålogging til medlemssidene.)

- Roller og samspill
- Planarbeidet
- Arbeid med forvaltningsrevisjon og eierskapskontroll
- Økonomiforvaltningen
- Påseansvaret
- Henvendelser

Her er også en kortversjon av presentasjonen om roller og samspill som kan benyttes i den generelle folkevalgtopplæringen av kommunestyret og fylkesting.

Det er lagt inn tekst i notatfeltet under lysbildene som kan tilpasses og benyttes av foredragsholder. Vi anbefaler at utvalgene får tilsendt presentasjonene med tilhørende notater.

## KONFERANSER OG SAMLINGER

### Kontrollutvalgslederskolen

Kontrollutvalgslederskolen har som mål å gjøre lederne tryggere i rollen. Vi vil tilby faglig innsikt utover det som tilbys i ordinære konferanser. Undervisningen vil være variert. Kontrollutvalgsmedlemmer og sekretærer kan også delta.

- [Del 1, november 2023](#) (dato er ikke bestemt ennå) digital/Teams  
Her legger vi vekt på grunnleggende rolleforståelse og kontrollutvalgets samspill med andre aktører. Andre viktige tema vil være påseansvaret, bestiller-rollen og hvilke verktøy kontrollutvalget har til rådighet. Samlingen blir sannsynligvis arrangert over to dager, (3 + 3 timer).
- [Del 2, 5. og 6. februar 2024](#), Clarion Oslo Airport, Gardermoen  
På den fysiske samlingen legger vi opp til god tid til diskusjoner i grupper om relevante problemstillinger som dukker opp i møter og som kontrollutvalgslederen må være forberedt på. På dag 2 vil håndtering av media være sentralt.

### Sekretariatskonferansen

19. og 20. mars 2024, Quality Airport Hotel Gardermoen

### Fagkonferansen

3. og 4. juni 2024, Quality Airport Hotel Gardermoen

I forbindelse med fagkonferansen, har vi også årsmøte 3. juni.

## PROSJEKTER

FKT og NKRF er godt i gang med et samarbeidsprosjekt om utvikling av normer for sekretariatene.

Følgende anbefalinger ble fastsatt av styrene i FKT og NKRF i slutten av mai:

- [Anbefaling for god skikk og praksis i kontrollutvalgssekretariatene – bestilling, behandling og oppfølging av forvaltningsrevisjon og eierskapskontroll](#)

Formålet med denne er å gi relevant veiledning til kontrollutvalgssekretariat om arbeidet som følger av foreliggende plan for forvaltningsrevisjon og eierskapskontroll. Anbefalingen kan også anvendes på andre bestillinger så langt det passer.

- [Anbefaling for god skikk og praksis i kontrollutvalgssekretariatene – møtebok](#)

Formålet med denne er å gi anbefalinger om hvordan kontrollutvalgssekretariatene skal føre protokoll fra kontrollutvalgsmøter.

Samarbeidet med anbefalinger fortsetter videre, og for tiden er to arbeidsgrupper i gang med å utarbeide forslag til anbefalinger for:

- Risiko- og vesentlighetsvurdering (ROV) og plan for forvaltningsrevisjon og eierskapskontroll
- Budsjetten for kontrollarbeidet

Disse kommer på ekstern høring i løpet av høsten.

## ORGANISASJONEN

Du finner styreprotokollene på [medlemssiden](#) (krever pålogging). Send e-post til [fkt@fkt.no](mailto:fkt@fkt.no) hvis du ønsker å få tilsendt brukernavn og passord.

Styrets møtekalender for høsten 2023: 14. august, 16. oktober og 7. desember.

[Protokollen fra årsmøtet 2023 finner du her:](#)

I løpet av det siste halvåret har FKT fått ni nye medlemmer. Disse er: Sekretariatet for kontrollutvalget i region Nordhordland, kontrollutvalgene i Sykkylven, Sula, Giske, Fjord, Stranda, Voss, Fedje og Austrheim kommuner. Velkommen skal dere være!

## NYHETS BREV

I tillegg til medlemsbrev sender FKT ut nyhetsbrev til alle som er interessert.

Personvernreglene krever ditt samtykke hvis du vil ha nyhetsbrev fra FKT. Du kan melde deg på her: [www.fkt.no](http://www.fkt.no) (like under hoved-nyhetene)

Følg oss gjerne på [facebook](#) og på [twitter](#)

*Med ønske om en riktig god sommer og et godt valg!*

**Anne-Karin Femanger Pettersen**

Generalsekretær

Fra: Helge Inge Johansen[]  
Sendt: 16.08.2023 11:24:00  
Til: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]  
Tittel: VS: Reglement for kontrollutvalet for valperioden 2023 - 2027

---

**Fra:** Roald Breistein <[Roald.Breistein@vlfk.no](mailto:Roald.Breistein@vlfk.no)>  
**Sendt:** tirsdag 15. august 2023 15:02  
**Til:** Kjartan Haugsnes <[Kjartan.Haugnsnes@vlfk.no](mailto:Kjartan.Haugnsnes@vlfk.no)>; Einar Kåre Ulla <[Einar.Kare.Ulla@vlfk.no](mailto:Einar.Kare.Ulla@vlfk.no)>; Helge Inge Johansen <[Helge.Inge.Johansen@vlfk.no](mailto:Helge.Inge.Johansen@vlfk.no)>  
**Kopi:** Hogne Haktorson <[Hogne.Haktorson@vlfk.no](mailto:Hogne.Haktorson@vlfk.no)>  
**Emne:** Reglement for kontrollutvalet for valperioden 2023 - 2027

I tråd med kommunelova § 5-13 skal det fastsetjast reglement for folkevalde organ for tidsperioden som organet er oppretta for.

Kommunelova § 5-13 lyd slik:

**§ 5-13.Reglement for folkevalgte organer**

Folkevalgte organer skal ha et reglement som fastsetter

- a. organets virkeområde og eventuelle vedtaksmyndighet
- b. tidsperioden som organet er opprettet for
- c. eventuelle andre sentrale bestemmelser om organets virksomhet.

Plikten etter første ledd gjelder ikke representantskap og andre styringsorganer for interkommunalt politisk råd, representantskap og andre styringsorganer for kommunalt oppgavefelleskap og styre for kommunalt eller fylkeskommunalt foretak.

I Vestland fylkeskommune er det sett i gang ein prosess med å utarbeide reglement for alle politiske utval for neste valperiode med tanke på handsaming i konstituerande fylkesting i oktober 2023.

Dersom kommunen er i gang med å revidere sine reglement, og det er tenkt vesentlege endringar i reglementet som gjeld for kontrollutvalet, er det fint om vi kan få tilsend utkast for gjennomsyn med tanke på å komme med innspel, før det vert handsama politisk.

Med helsing

**Roald Breistein**  
seniorrådgjevar

sekretariat for kontrollutvalet



Tlf: 97 50 51 52  
[www.vestlandfylke.no](http://www.vestlandfylke.no)

*Ver merksam på at all dialog på e-post kan bli journalført.*



Fra: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]  
Sendt: 07.08.2023 14:08:29  
Til: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]  
Tittel: VS: Valg og opplæring av kontrollutvalg for perioden 2023–2027

---

---

**Fra:** Hogne Haktorson <Hogne.Haktorson@vlfk.no>  
**Sendt:** torsdag 29. juni 2023 09:15  
**Til:** Roald Breistein <Roald.Breistein@vlfk.no>; Kjartan Haugsnes <Kjartan.Haugnes@vlfk.no>; Helge Inge Johansen <Helge.Inge.Johansen@vlfk.no>; Einar Kåre Ulla <Einar.Kare.Ulla@vlfk.no>  
**Emne:** VS: Valg og opplæring av kontrollutvalg for perioden 2023–2027

Til orientering.

Antar vedlagt brev vart sendt 26.06.23, sjølv om det er datert 26.07.23.

Med helsing

**Hogne Haktorson**  
kontrollsjef

sekretariat for kontrollutvalet



tlf: 91 10 59 82  
[www.vestlandfylke.no](http://www.vestlandfylke.no)

*Ver merksam på at all dialog på e-post kan bli journalført.*

---

**Fra:** Forum for Kontroll og Tilsyn <[fkt@fkt.no](mailto:fkt@fkt.no)>  
**Sendt:** mandag 26. juni 2023 12:02  
**Til:** Forum for Kontroll og Tilsyn <[fkt@fkt.no](mailto:fkt@fkt.no)>  
**Emne:** Valg og opplæring av kontrollutvalg for perioden 2023–2027

Til  
kommuner og fylkeskommuner

Kopi:  
FKTs kontrollutvalgs- og sekretariatsmedlemmer

Se vedlagte dokument.

*Med vennlig hilsen*

**Anne-Karin Femanger Pettersen**

Generalsekretær

---

**Forum for kontroll og tilsyn** / Postboks 41 Sentrum, 0101 Oslo / [fkt@fkt.no](mailto:fkt@fkt.no) / +47 414  
71 166 / [www.fkt.no](http://www.fkt.no)

Til  
kommuner og fylkeskommuner

Attn.:  
Ordfører  
kommunaldirektør / fylkeskommunedirektør  
Byråd / fylkesråd  
Saksansvarlig valgteknisk forberedelse

Oslo 26.7 2023

## **Valg og opplæring av kontrollutvalg for perioden 2023–2027**

Kontrollutvalget er ett av de få lovfestede utvalgene i kommunen/fylkeskommunen - et stadig mer sentralt utvalg, ikke minst på grunn av økt satsing på forvaltningsrevisjon og eierskapskontroll. Det gjør også at kommunestyrene og fylkestingene prioriterer utvalget høyere nå enn før. Forum for kontroll og tilsyn ser det som en naturlig og gledelig utvikling.

Kontrollutvalget er ellers spesielt mht. hvem som kan velges. Vi bruker å få meldinger om feil ved valg av kontrollutvalg etter kommune- og fylkestingsvalg. Vi vil derfor gi noen råd og innspill før nytt utvalg skal velges til høsten:

## KOMMUNELOVENS BESTEMMELSER OM VALG AV KONTROLLUTVALG

### § 7-1 Konstituerende møte i kommunestyret og fylkestinget

Kontrollutvalget skal velges på det konstituerende møtet, etter valg av formannskap/fylkesutvalg, ordfører/fylkesordfører og varaordfører/fylkesvaraordfører.

### § 23-1 Kontrollutvalget

Kommunestyret og fylkestinget velger selv en leder, en nestleder og øvrige medlemmer og varamedlemmer til utvalget. Lederen kan ikke være medlem av samme parti eller tilhøre samme gruppe som ordføreren. Utvalget skal ha minst fem medlemmer. Minst ett medlem skal velges blant kommunestyrets eller fylkestingets medlemmer.

Utelukket fra valg er

- a) Ordfører og varaordfører
- b) Medlemmer og varamedlemmer av formannskap eller fylkesutvalg
- c) medlemmer og varamedlemmer av folkevalgt organ med beslutningsmyndighet  
Medlemmer og varamedlemmer av kommunestyret eller fylkestinget er likevel valgbare
- d) medlemmer av kommuneråd eller fylkesråd
- e) medlemmer og varamedlemmer av kommunestyrekomité eller fylkestingskomité
- f) ansatte i den aktuelle kommunen eller fylkeskommunen (gjelder også deltidsstillinger)
- g) personer som har en ledende stilling, eller som er medlem eller varamedlem av styret
- h) eller bedriftsforsamlingen, i et selskap som kommunen eller fylkeskommunen har eierinteresser i
- i) personer som har en ledende stilling, eller som er medlem eller varamedlem av styret i et interkommunalt politisk råd eller et kommunalt oppgavefellesskap.

Kommunelovens regler om kjønnsmessig balanse gjelder også for kontrollutvalget.

## **KONTROLLUTVALGETS ROLLE I FOLKEVALGTPROGRAMMET**

Kommunestyret og fylkestinget har det øverste ansvaret for å kontrollere kommunens og fylkeskommunens virksomhet. Derfor er det viktig at kontrollutvalgets funksjon og rolle gis god plass i folkevalgtopplæringen.

### **Basisprogrammet**

Vi er kjent med at det i forkant av basisprogrammet i KS sitt folkevalgtprogram 2023-2027, vil arrangeres formøte mellom prosessveileder fra KS og kommunen/fylkeskommunen. FKT oppfordrer til at kontrollutvalgets sekretariat inviteres til møtet. Sekretariatet kan bidra med sin erfaring og gi gode tips om kunnskapsbehovet. Hvis kontrollutvalget skal kunne gjøre en god jobb for kommunestyret og fylkestinget, er det viktig at medlemmene kjenner hele den kommunale/fylkeskommunale virksomheten. Basisprogrammet er i så måte en god anledning og kontrollutvalget bør få tilbud om å delta på opplæringen.

### **Temadager**

KS anbefaler at det arrangeres temadager som kommer i tillegg til basisprogrammet. Her kan kommunen/fylkeskommunen selv legge inn fordypninger i ulike emner. Det er særlig viktig at kommunestyret og fylkestinget kjenner sin styringsrolle og sitt ansvar som øverste ansvarlig for egenkontrollen. Kunnskap om kontrollutvalgets rolle og arbeid er viktige i denne sammenhengen. FKT har laget en PowerPoint-presentasjon, «Roller og samspill» som kan benyttes i den generelle folkevalgtopplæringen av kommunestyret og fylkesting.

## **OPPLÆRING AV KONTROLLUTVALG**

Kontrollutvalget er et lovfestet og viktig utvalg som bør ha dyktige medlemmer. FKT er godt i gang med å planlegge opplæringstiltak for kontrollutvalgene etter valget. Vi vil tilby våre medlemmer en seire PowerPoint-presentasjoner som kan benyttes lokalt evt. regionalt. [https://www.fkt.no/publikasjoner/opplaeringspakke\\_for\\_kontrollutvalg/](https://www.fkt.no/publikasjoner/opplaeringspakke_for_kontrollutvalg/)

Vi vil også tilby et eget kursopplegg for kontrollutvalgsledere. «Kontrollutvalgslederskolen» har som mål å gjøre lederne tryggere i rollen. Vi tilbyr faglig innsikt utover det som tilbys i ordinære konferanser. Del 1 er digital og gjennomføres i november. Her gjennomgår vi grunnleggende opplæring om roller og samspill i den kommunale og fylkeskommunale egenkontrollen. Andre interesserte er velkommen til å delta på del 1. Del 2 er fysisk samling 5.– 6. februar på Gardermoen. Vi vil sende ut invitasjoner mer informasjon om tilbudet etter valget.

Vi oppfordrer kommuner og fylkeskommuner til å avsette tilstrekkelige ressurser i budsjettet for 2024 til opplæring av nytt kontrollutvalg.

FKT er tilgjengelige for spørsmål som måtte dukke opp i forbindelse med valg av kontrollutvalg, egenkontrollens plass i folkevalgtopplæringen og opplæring av kontrollutvalg.

Kopi:

FKTs kontrollutvalgs- og sekretariatsmedlemmer

*Med vennlig hilsen*

**Anne-Karin Femanger Pettersen**

Forum for kontroll og tilsyn

*Forum for kontroll og tilsyn (FKT) ble stiftet i 22. november 2005. Vi har 195 kommuner og 7 fylkeskommuner som medlemmer og vi har 22 kontrollutvalgssekretariat som dekker mer enn 250 kommuner/fylkeskommuner.*

---

**FORUM FOR KONTROLL OG TILSYN**

Postboks 41 Sentrum, 0101 Oslo / +47 414 71 166 / fkt@fkt.no / www.fkt.no

