Tysnes kommune

Tysnes kommune,
Kontrollutvalet

Møteinnkalling

Utval:	Tysnes kommune, Kontrollutvalet
Møtestad:	Rådhuset, Kommunestyresalen
Dato:	07.03.2024
Tid:	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 til Helge Inge Johansen, tlf. mob.402 03 664, mail helge.inge.johansen@vlfk.no eller til Hogne Haktorson, tlf. mob. 911 05 982, mail: hogne.haktorson@vlfk.no .

Det er planlagt at Helge Inge Johansen, møter frå sekretariatet på dette møtet.

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.

Anne Kristi Alfstad
kontrollutvalsleiar

Hogne Haktorson
kontrollsjef

Helge Inge Johansen
seniorrådgjevar

Dokumentet er godkjent elektronisk og har difor ingen handskriven underskrift

Kopi: Vararepresentantar til kontrollutvalet
Ordførar
Revisor
Kommunedirektør/Rådmann

Sakliste

Utvals-saknr	Innhald	Arkiv-saknr	U.Off
	Godkjenningssaker		
GK 1/24	Godkjenning av innkalling og sakliste		
GK 2/24	Godkjenning av møteprotokoll frå møte 23.11.2023	2024/6	
	Politiske saker		
PS 1/24	Forvaltningsrevisjon av informasjonstryggleik og personvern - revisjonsrapport	2022/324	
PS 2/24	Plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024-2028 - prosessmøte 1	2023/406	
PS 3/24	Årsmelding 2023 for kontrollutvalet	2024/32	
PS 4/24	Gjennomgang av møteprotokollar frå andre politiske utval	2023/479	
PS 5/24	Møteplan 2024 for kontrollutvalet	2024/30	
PS 6/24	Eventuelt	2023/478	
PS 7/24	Konkurranseutsetting av revisjonstenestene for Tysnes kommune	2023/371	
	Referat saker		
RS 1/24	Budsjett 2024 for kontrollutvalet - vedtak frå KS	2022/101	
RS 2/24	FKT - medlemsinformasjon desember 2023	2022/109	
RS 3/24	Årsmelding mobbeombodet i Vestland 2022-2023	2024/15	

GK 1/24 Godkjenning av innkalling og sakliste

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2024/6-1
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**2/24**	**07.03.2024**

Godkjenning av møteprotokoll frå møte 23.11.2023

Møteprotokoll frå møte 23.11.2023 er vedlagt saka

Møteprotokoll

Utval:	Kontrollutvalet
Møtestad:	Rådhuset, Stjernereiso
Dato:	23.11.2023
Tid:	10:00 - 14:15

Følgjande faste medlemer møtte:

Namn	Funksjon	Representerer
Anne Kristi Alfstad	Leiar	H
Lorentz Lunde	Medlem	KRF
Tor Magnus Hauge	Medlem	INP

Følgjande medlemer hadde meldt forfall:

Namn	Funksjon	Representerer
Lars Heine Kåsa	Nestleiar	SP
Anna Haugsgjerd	Medlem	AP

Følgjande varamedlemer møtte:

Namn	Møtte for	Representerer
Kristin Teigland Gjerstad Kleppe	Lars Heine Kåsa	SP

Andre som møtte:

Namn	Stilling
Helena Hildershavn Winkel	Rekneskapsrevisor, Deloitte AS
Kari Gåsemyr	Forvaltningsrevisor, Deloitte AS
Annbjørg Ryssdal	Forvaltningsrevisor, Deloitte AS
Helge Inge Johansen	Spesialrådgjevar, Vestland fylkeskommune

Anne Kristi Alfstad
utvalsleiar

Helge Inge Johansen
utvalssekretær

Dokumentet er godkjent elektronisk og har difor inga handskriven underskrift

Sakliste

Utvals-saknr	Innhald	Arkiv-saknr	U.Off
	Godkjenningssaker		
GK 7/23	Godkjenning av innkalling og sakliste		
GK 8/23	Godkjenning av møteprotokoll frå møte 05.10.2023	2022/106	
	Politiske saker		
PS 29/23	Rutinar gjeldande kontrollutvalet for perioden 2023-2027	2023/480	
PS 30/23	Evaluering av arbeidet i kontrollutvalet for valperioden 2019-2023	2023/480	
PS 31/23	Deloitte AS presenterer interimsrevisjonsrapport 2023	2023/443	
PS 32/23	Plan for forvaltningsrevisjon og plan for eigarskapskontroll 2024-2028 - Forslag til prosjektplan	2023/406	
PS 33/23	Gjennomgang av møteprotokollar - 2023-2027	2023/479	
PS 34/23	Eventuelt	2023/478	
	Referat saker		
RS 6/23	Nytt frå FKT - Oktober	2022/109	

Godkjenningsaker

GK 7/23 Godkjenning av innkalling og sakliste

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Det kom ingen merknad til innkalling eller saksliste.

Vedtak

Innkalling og saksliste vart samrøystes godkjent

GK 8/23 Godkjenning av møteprotokoll frå møte 05.10.2023

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Det var ingen merknad til protokoll frå møte 05.10.2023.

Vedtak

Møteprotokoll frå møte 05.10.2023 vart samrøystes vedteke.

Politiske saker

PS 29/23 Rutinar gjeldande kontrollutvalet for perioden 2023-2027

Forslag til vedtak

1. Kontrollutvalet tek rutinar for kontrollutvalet til etterretning.
2. Kontrollutvalet er informert om og tek til etterretning reglar for teieplikt.
3. Kontrollutvalet er samde i at det er leiar i utvalet som kan uttale seg til media på vegne av utvalet.
4. Kontrollutvalet sine faste medlemmar får abonnement på «Kontroll & revisjon» (Kommunerevisoren), og utvalsleiar får og abonnement på Kommunal rapport
5. Kontrollutvalet vil prioritere at nokon frå utvalet deltek på ein eller fleire av konferansane for kontrollutval i 2024.
6. Kontrollutvalet vil prioritere at alle medlemmene deltek på folkevaldopplæring for kontrollutvala på Solstrand 2024.
7. Første møte i kontrollutvalet i Tysnes kommune i 2024 vert .....xx.xx.2024.

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Rutinar for kontrollutvalet vart gjennomgått.

Medlem Tor Magnus Hauge frå Inp melde seg på folkevaldopplæringa. Sekretariatet har motteke påmelding frå Anne Kristi Alfstad og Lorentz Lunde. Utvalsleiar ønskjer at alle medlemmene i kontrollutvalet skal delta. Lars Heine Kåsa og eventuelt nytt medlem for Anna Haugsgjerd om ho ikkje er valbar, kan melda seg på.

Vedtaket vart samrøystes vedteke.

Vedtak

1. Kontrollutvalet tek rutinar for kontrollutvalet til etterretning.
2. Kontrollutvalet er informert om og tek til etterretning reglar for teieplikt.
3. Kontrollutvalet er samde i at det er leiar i utvalet som kan uttale seg til media på vegne av utvalet.
4. Kontrollutvalet sine faste medlemmar får abonnement på «Kontroll & revisjon» (Kommunerevisoren).
5. Kontrollutvalet vil prioritere at nokon frå utvalet deltek på ein eller fleire av konferansane for kontrollutval i 2024.
6. Kontrollutvalet vil prioritere at alle medlemmene deltek på folkevaldopplæring for kontrollutvala på Solstrand 2024.
7. Første møte i kontrollutvalet i Tysnes kommune i 2024 vert 08.02.2024.

PS 30/23 Evaluering av arbeidet i kontrollutvalet for valperioden 2019-2023

Forslag til vedtak

1. Kontrollutvalet sluttar seg til evalueringa frå kontrollutvalet for valperioden 2019 - 2023.
2. Utvalet ber sekretariatet om å arbeide vidare med evalueringspunkta.

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Evalueringskjema vart gjennomgått.

Forslag til vedtak vart samrøystes vedteke.

Vedtak

1. Kontrollutvalet sluttar seg til evalueringa frå kontrollutvalet for valperioden 2019 - 2023.
2. Utvalet ber sekretariatet om å arbeide vidare med evalueringspunkta.

PS 31/23 Deloitte AS presenterer interimsrevisjonsrapport 2023

Forslag til vedtak

Kontrollutvalet tek oppsummering etter interimsrevisjon 2023 frå Deloitte AS til orientering.

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Rekneskapsrevisor presenterte interimsrevisjonsrapport for 2023 og svarte på spørsmål frå kontrollutvalet.

Forslag til vedtak vart samrøystes vedteke.

Vedtak

Kontrollutvalet tek oppsummering etter interimsrevisjon 2023 frå Deloitte AS til orientering.

PS 32/23 Plan for forvaltningsrevisjon og plan for eigarskapskontroll 2024-2028 - Forslag til prosjektplan

Forslag til vedtak

1. Kontrollutvalet ber Deloitte AS gjennomføre risiko- og vesentlegvurderingar (ROV) av verksemda i Tysnes kommune, verksemda i kommunen sine selskap og av Tysnes kommune sin eigarskap i selskap.
2. Vidare ber kontrollutvalet Deloitte AS utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024 – 2028.
3. Det er ei målsetting at prosessmøte 1 skal gjennomførast i første møte i kontrollutvalet i 2024 og at prosessmøte 2 skal gjennomførast i kontrollutvalet i mai 2024.
4. Det er videre ei målsetting at forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for 2020 – 2024 skal leggast fram for kommunestyret i juni 2024.

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Forvaltningsrevisjorane orienterte om forslag til prosjektplan, og svarte på spørsmål frå kontrollutvalet.

Forslag til vedtak vart samrøystes vedteke.

Vedtak

1. Kontrollutvalet ber Deloitte AS gjennomføre risiko- og vesentlegvurderingar (ROV) av verksemda i Tysnes kommune, verksemda i kommunen sine selskap og av Tysnes kommune sin eigarskap i selskap.
2. Vidare ber kontrollutvalet Deloitte AS utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024 – 2028.
3. Det er ei målsetting at prosessmøte 1 skal gjennomførast i første møte i kontrollutvalet i 2024 og at prosessmøte 2 skal gjennomførast i kontrollutvalet i mai 2024.
4. Det er videre ei målsetting at forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for 2024 – 2028 skal leggast fram for kommunestyret i juni 2024.

PS 33/23 Gjennomgang av møteprotokollar - 2023-2027

Forslag til vedtak

1. Kontrollutvalet tek møteprotokollane som går fram av saksutgreiinga til orientering.
2. Særskilt ansvar for gjennomgang av framtidige møteprotokollar vert fordelt slik:

Politisk organ:	Kontrollutvalsmedlem:
Kommunestyret	
Formannskapet	
Tenesteutval	
Utval for landbruk og teknisk	

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Kontrollutvalet ønskjer at at denne saka skal vere på sakslista og i denne valperioden.

Særskilt ansvar for gjennomgang av framtidige møteprotokollar vert fordelt slik:

Kommunestyret: Anna Haugsgjerd (eller nytt medlem dersom nyval for henne)

Formannskapet: Lars Heine Kåsa

Tenesteutvalet: Lorentz Lunde

Utval for Landbruk og teknisk: Tor Magnus Hauge

Vedtaket vart samrøystes vedteke.

Vedtak

1. Kontrollutvalet tek møteprotokollane som går fram av saksutgreiinga til orientering.
2. Særskilt ansvar for gjennomgang av framtidige møteprotokollar vert fordelt slik:

Politisk organ:	Kontrollutvalsmedlem:
Kommunestyret	Anna Haugsgjerd (eller nytt medlem dersom nyval for henne)
Formannskapet	Lars Heine Kåsa
Tenesteutval	Lorentz Lunde
Utval for landbruk og teknisk	Tor Magnus Hauge

PS 34/23 Eventuelt

Forslag til vedtak

Saka vert lagt fram utan forslag til vedtak.

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Det var ingen saker til eventueltsaka.

Vedtak

Det vart ikkje gjort vedtak i saka.

Referat saker

RS 6/23 Nytt frå FKT oktober

Saksprotokoll 23.11.2023 - Tysnes kommune, Kontrollutvalet

Behandling i møte

Det kom ikkje fram noko spesielt ved handsaming av referatsaka.

Vedtaket vart samrøystes vedteke.

Vedtak

Kontrollutvalet tar referatsaka til orientering.

Saksframlegg

Saksnr: 2022/324-11
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**1/24**	**07.03.2024**

Forvaltningsrevisjon av informasjonstryggleik og personvern - revisjonsrapport

Forslag til innstilling

Kommunestyret ber rådmannen om å:

1. Sørgje 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 det er tydelege rollar og ansvar i arbeidet med informasjonstryggleik, og vidare at rollar og ansvar er tydeleg tildelt og kommunisert både til dei tilsette det gjeld og relevante tilsette i kommunen elles.

   b) Sikrar at det er etablert nødvendige rutinar og retningslinjer knytt til arbeidet med informasjonstryggleik, i kommunen.

   c) Etablere system for kontroll og etterprøving av informasjonstryggleik i kommunen, og sikrar at dette blir gjennomført jamleg (t.d. leiinga sin årlege gjennomgang av tryggleiksrevisjonar).

2. Sørgje 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 (både ved oppstart, endra arbeidsoppgåver og avslutting av arbeidsforholdet)

   b) Sikrar at etablerte rutinar og retningslinjer for tilgangsstyring er tilgjengelege for alle relevante tilsette

3. Sørgje for 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 personvernordninga).

4. Sørgje for at det blir utarbeidd protokoll over behandlingsaktivitetar av personopplysningar, som blir utført i kommunen.

5. Sørgje 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 (DPIA).

6. Sørgje for at retningslinjer for informasjonstryggleik tydeleg skildrar melding om avvik til Datatilsynet (ansvar og frist til og melde avvik vidare til tilsynsmyndigheita).

7. Sørgje for å få oversikt over kva kompetanse det er behov for hos leiarar og tilsette i arbeid med informasjonstryggleiksarbeidet i kommunen

8. Sørgje 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 møte i kontrollutvalet 26.09.2024, 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 ansvaret for iverksettinga. Prioritert handlingsplan vert å senda sekretariatet innan 05.09.2024.

Samandrag

Kontrollutvalet bestilte forvaltningsrevisjon av informasjonstryggleik og personvern i møte 24.11.2022, og kontrollutvalet hadde rapporten til handsaming i møte 05.10.2023 der kontrollutvalet måtte utsetje saka grunna at rådmannen hadde gjeve ny uttale til rapporten i møte. Kontrollutvalet skal handsame rapporten i dette møte og 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 Endeleg rapport med utvida høyringsuttale

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 tilfredsstiller 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 – 43), 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.

Revisjonen vurderer at Tysnes kommune sine styrande dokument på revisjonstidspunktet langt på veg er i samsvar med krav i regelverket. Kommunen har gjennom handbok for informasjonssikkerhet og IKT-strategi 2022-2025 etablert mål og strategi for arbeidet med informasjonstryggleik i kommunen og styrande dokument er vidare tilgjengeleg for dei tilsette i organisasjonen via intranett og kvalitetssystemet (Compilo). Dette er i samsvar med krav på området (jf. eForvaltningsforskrifta § 15).

Digitaliseringsdirektoratet tilrår at verksemder utformar føringar for arbeidet med informasjonstryggleik, og at struktur og innhald i styringsaktivitetane blir dokumentert på ein føremålstenleg måte slik at det er tydeleg kven som skal gjere kva, og korleis det skal gjerast (slik at dokumenteringa t.d. kan nyttast som oppslagsverk for tilsette). Undersøkinga viser at styrande dokument ikkje gir informasjon om kva tryggleiksrevisjonar omfattar, når det skal gjennomførast eller kven som har ansvar for dette. Revisjonen er merksam på at kommunen sine styrings-dokument relativt nyleg er etablert, og at arbeidet med å implementere rutinar og system i samsvar med dette framleis var pågåande på revisjonstidspunktet.

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

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

Revisjonen vurderer at Tysnes kommune ikkje har etablert tilstrekkeleg system for kontroll og etterprøving av informasjonstryggleik på alle område. I handbok for informasjonssikkerhet blir retningslinjer for leiinga sin gjennomgang skildra, og det blir vist til at det skal gjennomførast tryggleiksrevisjonar. Revisjonen påpeiker difor at kommunen på revisjonstidspunktet ikkje oppfyller sentrale krav i eForvaltningsforskrifta som seier at kommunen skal ha ein internkontroll på området som baserer seg på anerkjente standardar for styringssystem for informasjonstryggleik (§ 15).

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

Tysnes kommune har utnemnt eit personvernombod, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Revisjonen vil påpeike at kommunen pliktar

å stille til rådigheit dei ressursar som er nødvendig for at personvernombodet skal kunne utføre lovpålagde oppgåver (2. punkt i artikkel 38).

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

Tysnes kommune har etablert personvernerklæring. Revisjonen vurderer samtidig at kommunen ikkje har sikra at denne erklæringa har tilstrekkeleg klar og tydeleg informasjon tilpassa brukarane. 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.

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 personopplysingar og at dette heller ikkje blir gjort systematisk. Det er heller ikkje tilstrekkeleg tydeleggjort kven som skal ha dette ansvaret for dei ulik systema. Dette er ikkje i samsvar med krav om utarbeiding av behandlingsprotokollar (artikkel 30 i personvernforordninga).

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

Tysnes kommune har ved innføring av elektronisk avviksmeldesystem sikra oversikt over avvik som blir meldt knytt til personvern. Revisjonen vurderer samtidig at kommunen ikkje i tilstrekkeleg grad har etablert retningslinjer som sikrar tilfredsstillande rutinar for kven som har hovudansvar for å melde frå til Datatilsynet dersom det blir meldt om alvorlege brot på personopplysnings-tryggleiken, og det går heller ikkje fram kva som er frist for å melde slike avvik vidare til tilsyns-myndigheita. 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).

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.

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

Basert på funna i spørjeundersøkinga, vurderer revisjonen at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Til dømes svarar om lag halvparten av alle respondentane, og om lag ein av tre respondentar med leiaransvar, at dei ikkje kjenner innhaldet i kommunen si handbok i informasjonssikkerhet.

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. Revisjonen vil i den samanheng understreke at det å dele passord med andre ikkje er i samsvar med grunnleggjande prinsipp for informasjonstryggleik, også i tilfella der det er IT-tenesta ein deler passordet med.

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

1. Sørgje 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 det er tydelege rollar og ansvar i arbeidet med informasjonstryggleik, og vidare at rollar og ansvar er tydeleg tildelt og kommunisert både til dei tilsette det gjeld og relevante tilsette i kommunen elles.

   b) Sikrar at det er etablert nødvendige rutinar og retningslinjer knytt til arbeidet med informasjonstryggleik, i kommunen.

   c) Etablere system for kontroll og etterprøving av informasjonstryggleik i kommunen, og sikrar at dette blir gjennomført jamleg (t.d. leiinga sin årlege gjennomgang av tryggleiksrevisjonar).

2. Sørgje 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 (både ved oppstart, endra arbeidsoppgåver og avslutting av arbeidsforholdet)

   b) Sikrar at etablerte rutinar og retningslinjer for tilgangsstyring er tilgjengelege for alle relevante tilsette

3. Sørgje for 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 personvernordninga).

4. Sørgje for at det blir utarbeidd protokoll over behandlingsaktivitetar av personopplysningar, som blir utført i kommunen.

5. Sørgje 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 (DPIA).

6. Sørgje for at retningslinjer for informasjonstryggleik tydeleg skildrar melding om avvik til Datatilsynet (ansvar og frist til og melde avvik vidare til tilsynsmyndigheita).

7. Sørgje for å få oversikt over kva kompetanse det er behov for hos leiarar og tilsette i arbeid med informasjonstryggleiksarbeidet i kommunen

8. Sørgje 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

Rådmannen har gjeve utvida uttale til revisjonsrapporten på s. 44 – s. 54 i rapporten:

Dette kjem mellom anna fram av utvida uttale frå rådmannen:

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

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

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

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

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

Revisjonen kjem med tilbakemelding på rådmannen si utvida uttale på s. 55 - 57 i rapporten.

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

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

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

I den utvida høyringsuttalen skriv rådmann at det ikkje er eit krav at offentlege verksemder skal sertifiserast etter ISO/IEC 27001, og at det mellom anna framstår som unøyaktig at revisjonen ikkje har kommentert at standarden (ISO/IEC 27001) ikkje var tilrådd i delar av Digdir sitt tidlegare skriftlege rettleiingsmateriell. Revisjonen vil påpeike at vi ikkje har lagt til grunn at kommunen skal sertifiserast etter ISO-standarden. Det er riktig at det i ein rettleiar frå Digdir på revisjons-tidspunktet gjekk fram at offentlege verksemder verken var pålagd eller tilrådd å vere i samsvar med standarden. Som rådmannen påpeiker er det no utarbeidd ein ny versjon av denne rettleiaren

der teksten er noko endra for å ta inn endringar i ny versjon av standarden. I oppdatert versjon av rettleiaren går det også fram at offentlege verksemder i Noreg ikkje er pålagde å vere i samsvar med ISO-standarden, men at pålegget er å basere seg på anerkjende standardar og at tilrådinga er å basere seg på gjeldande versjon av NSISO/IEC 27001.

Revisjonen er samd i at det er eit viktig poeng at offentlege verksemder ikkje er påkravd å etterleve standarden ISO/IEC 27001, men at ein er påkravd å ha internkontroll på informasjonstryggleiks-området som baserer seg på anerkjente styringssystem for informasjonstryggleik.

Revisjonen vil presisere at vi ikkje har henta inn ny eller oppdatert data frå kommunen etter at undersøkingsperioden var ferdigstilt i september 2023, og at endringane som er gjort i vurderinga dermed ikkje inkluderer eventuelle endringar som er gjort i kommunen sine styrande dokument, rutinar mv. etter revisjonsperioden.
Rådmann peiker på at det i rapporten blir vist til at styrande dokument ikkje viser til standardar eller konkrete regelverk på området, og at det er vanskeleg å sjå at dette er ein mangel. Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette. Revisjonen er samtidig samd i at det viktigaste ikkje er at styrande dokument skal vise til konkrete regelverk og standardar, men at dei styrande dokumenta er basert på dette. Vi har difor tatt omsyn til dette i avsnitt 3.3.2.

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

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

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

Revisjonen oppfattar vidare utifrå rådmannen sin utvida høyringsuttale at han er samd i at svara i spørjeundersøkinga tyder på at kommunen har rom for betring når det gjeld å sikre at avvik blir meldt, og at manglande avviksmeldingar aukar risiko for at svakheiter i systema ikkje blir retta.

Rådmann peiker også på at revisjonen burde vurdere validiteten nærare i data som kjem fram av spørjeundersøkinga. Rådmannen viser til at tilsette innanfor eit av tenesteområda i kommunen i samband med eit av spørsmåla truleg har lagt noko anna i svara sine enn det som var meint med spørsmålet. Revisjonen vurderer både reliabilitet og validitet i alt arbeid med forvaltningsrevisjonen. Revisjonen meiner det ikkje er sannsynleggjort at det er ei anna tolking enn det som er lagt til grunn i rapporten som er den rette.

Rådmannen viser også i utvida høyringsuttale til at det i kapittel 6 (konklusjon og tilrådingar) blir opplevd som vanskeleg å sjå samanheng mellom datagrunnlaget, vurderingane undervegs og

konklusjonane. Revisjonen har utvida punkta i konklusjonen slik at all informasjon frå vurderingane i rapporten blir tatt med.

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

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.

Deloitte.

Forvaltningsrevisjon | Tysnes kommune

Informasjonstryggleik og personvern

Februar 2024

«Forvaltningsrevisjon av informasjonstryggleik og personvern»

Februar 2024

Rapporten er utarbeidd for Tysnes kommune av Deloitte AS.

Deloitte AS
Postboks 6013 Postterminalen, 5892 Bergen
tlf: 55 21 81 00
www.deloitte.no
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 personvernlovgjevinga.

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 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.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[1] Datatilsynet. Virksomhetenes plikter. Informasjon og åpenhet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/

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

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

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

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

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

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

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

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

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

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

Ordliste

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

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 nettidentifikator eller eitt eller fleire element som er spesifikke for nemnde fysiske person sin fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet).

Sensitive personopplysningar /særlege kategoriar personopplysningar: opplysningar om rasemessig eller etnisk opphav, politisk oppfatning, religion, filosofisk overtyding, fagforeiningsmedlemskap, genetiske opplysningar, helseopplysningar, opplysningar om ein fysisk person sine seksuelle forhold, opplysningar om ein fysisk person si seksuelle orientering, straffedommar, lovbrot, 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.[4]

[3] Digitaliseringsdirektoratet (Digdir): Informasjonssikkerhet – en forutsetning for å nå virksomhetens mål: https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet-en-forutsetning-na-virksomhetens-mal/1123
[4] Det store norske leksikon: Datasikkerhet: https://snl.no/datasikkerhet

Innhald

Detaljert innhald

Figurar

Tabellar

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 personvernlovgjevinga.

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 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?

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 intervjua 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 %
TOTAL	**347**	**163**	**47 %**

1.4.4 Verifiseringsprosessar

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

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

1.5 Revisjonskriterier

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

2 Organisering av arbeidet med informasjonstryggleik

2.1 Organisering

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

Figur 1: Administrativ organisering av Tysnes kommune

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

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

3 Styringssystem for informasjonstryggleik

3.1 Problemstilling

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

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

Under dette:

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

3.2 Revisjonskriterier

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

Kommunen skal:

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

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

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

[5] Datatilsynet. Virksomhetenes plikter/informasjonssikkerhet og internkontroll/Etablere internkontroll/sikkerhetsrevisjon og egenkontroll. Sist endret: 23.06.2018. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/

[6] Digitaliseringsdirektoratet. Informasjonssikkerhet. Internkontroll i praksis. Etableringsaktiviteter. Utforme føringer. https://www.digdir.no/informasjonssikkerhet/utforme-foringer/3159

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

Sjå vedlegg 4 for utfyllande revisjonskriterium.

3.3 Styrande dokument for informasjonstryggleik

3.3.1 Datagrunnlag

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

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

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

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

Kommunen har også nyleg etablert ein ***IKT-strategi for 2022-2025***, og det går fram av strategien at kommunen har valt å prioritere fire innsatsområde i planperioden, der personvern og informasjonssikring inngår som eit av dei fire områda. Det blir vidare peikt på at det er definerte strategiar innanfor kvar av dei fire innsatsområda som skal 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
Ivareta informasjonstryggleik og personvern frå start til slutt	Vurdere informasjonstryggleik og personvern frå start til slutt i kommunen sine digitale løysingar for å sikre tillit frå verksemder og innbyggjarar. Informasjonstryggleik må følgje informasjonen frå den oppstår til den blir sletta.

[7] Digitaliseringsdirektoratet: https://www.digdir.no/informasjonssikkerhet/ledelsens-styring-og-oppfolging/3044
[8] Tysnes kommune. *Handbok i informasjonssikkerhet for Tysnes kommune*. 2022.

Leggja til rette for å gje innbyggaren innsyn og kontroll over eigne data	Kommunen skal leggja til rette for å gje innbyggarane lovbestemt innsyn i alle typar data som er registrert om dei. Innsyn vil kunna medføra rettingar som igjen gjev ei betring av datakvaliteten i kommunen.
Understøtta sikre tenester for elektronisk kommunikasjon med innbyggarane	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 innbyggarane den nødvendige grad av tryggleik og også bidra til effektivisering.
Syta for rett sikkerheitsnivå og oppdaterte sikkerheitsrutinar	For å oppnå så god kombinasjon av brukarvenlegheit og tryggleik som mogleg, er det viktig å definere rett nivå av tryggleik på data som ligg i dei ulike fagsystema. Behandlingsansvarlige (systemeigarar) har som ansvar å kjenna lovkrava og gje nødvendig informasjon til IT-avdelinga slik at aktuelle tryggleikstiltak blir gjort i infrastrukturen og drifta til kommunen. Kommunen må til ei kvar tid ha gode nok tryggleiksrutinar og bruke sikringsløysingar som sikrar for at informasjonen berre når autoriserte personar.
Gjennomføra organisatoriske tiltak for å vareta personvern og informasjonssikkerhet	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.
Bevisstgjera og gje opplæring	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.
Sikra moderne og effektive løysingar for å vareta informasjonstryggleik	Kommunen må tilpassa seg kontinuerleg teknologisk utvikling ved å implementera moderne og effektive løysingar som kan handtere kommande tryggleiksutfordringar.

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

Det blir i intervju vist til at informasjonstryggleik og personvern blir tatt opp som tema i møta i strategisk leiing, utvida leiarteam og einingsleiarmøte, men at det ikkje er etablert praksis for å ha dette oppe som fast tema i desse leiarmøta. Det blir elles vist til at det er etablert 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 på revisjonstidspunktet langt på veg var i samsvar med krav i regelverket. Kommunen har gjennom handbok for informasjonssikkerhet og IKT-strategi 2022-2025 etablert mål og strategi for arbeidet med informasjonstryggleik i kommunen og styrande dokument er vidare tilgjengeleg for dei tilsette i organisasjonen via intranett og kvalitetssystemet (Compilo). Dette er i samsvar med krav på området (jf. eForvaltningsforskrifta § 15). Digitaliseringsdirektoratet peiker på at eForvaltningsforskrifta § 15 stiller krav om å basere internkontrollarbeidet på anerkjente standardar, og at styringsdokumenta som blir utarbeidd på området bør synleggjere dette. Revisjonen vil på peike at Tysnes kommune, i samsvar med denne tilrådinga, bør synleggjere kva krav og /eller anerkjende standardar dei baserer sine styrande dokument på.

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

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

3.4 Rutinar og ansvarsforhold

3.4.1 Datagrunnlag

Ansvar og rollar knytt til informasjonstryggleik

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

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

Rolle	Skildring	Ansvar
Rådmann	Rådmannen har hovudansvaret for behandling av personopplysningar i Tysnes kommune	
Einingsleiarar	Ansvar for den daglege behandlinga av personopplysningar Einingsleiarar er også **systemeigar**, og med dette eigar av fagsystema/IT-systema som naturleg høyrer inn under området einingsleiar er ansvarleg for.	• Einingsleiar er systemeigar, og er eigar av fagsystema/IT-systema som naturleg høyrer inn under området einingsleiar er ansvarleg for. • ansvarleg for å behandla personopplysningar på ein lovleg, rettferdig og gjennomsiktig måte, ha eit behandlingsgrunnlag, behandla personopplysningane på ein sikker måte og sikra at dei registrerte får utøvd rettane sine. • 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 opptrer i samsvar med reglane. • 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.
Personvernombod	Personvernombod kontrollerer etterleving av forordninga og skal kunna gje råd i personvernkonsekvens-utgreiingar og kontrollere gjennomføringa.	• Personvernombod skal hjelpe tilsette, registrerte og leiinga i spørsmål om personvern og informasjonssikkerhet. • Personvernombod har teieplikt, skal ikkje få instruksjonar i samband med utføring av oppgåvene som personvernombod, og rapporterer til rådmannen.
IT-leiar	IT-leiar er ansvarleg for at informasjonstryggleiken blir varetatt i infrastruktur, maskinvare og tryggleikssystem.	• 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. • IT-leiar er ansvarleg for at fagsystema/IT-systema er tilgjengeleg for tilsette. • Hjelper til med teknisk kompetanse i dialog med superbrukar/fagsystemansvarleg.

Leiarar	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.	• 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. • Leggje til rette for at tilsette lagrar og behandlar opplysningar på rett stad i fagsystema, på heime- eller fellesområdet eller i Teams for kommunen. • Ansvar for at formålet med behandling av data skal registrerast i samsvar med GDPR reglane. Det skal utarbeidast ROS analysar ved nye system eller større endringar i eit fagsystem. • Ansvarleg for at tilsette har underteikna tilsetjingskontrakt og erklæring om teieplikt før dei får tilgang til IT- og fagsystema. • 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.
Superbrukar/ fagsystemansvarleg	Superbruker/fagsystemansvarleg er utpeikt av einingsleiar.	• Hovudansvar for å gi opplæring til tilsette om forsvarleg forvaltning av informasjonen i fagsystema/IT-systema. • Ansvar å utarbeida risikoanalyse.
Tilsette	Alle tilsette skal overhalde informasjonstryggleiks-reglementet, og vere med på å verne informasjon i fagsystem, elektroniske einingar og infrastruktur.	• Alle tilsette skal ha kjennskap til korleis avvik skal registrerast i avvikssystemet til kommunen (Compilo). • 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. • 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.

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 innformasjonstryggleik og personvern i kommunen. Det er fast agenda på desse møta, og ein går mellom anna gjennom meldte avvik og status for rutine- og systemarbeid innan personvern.

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

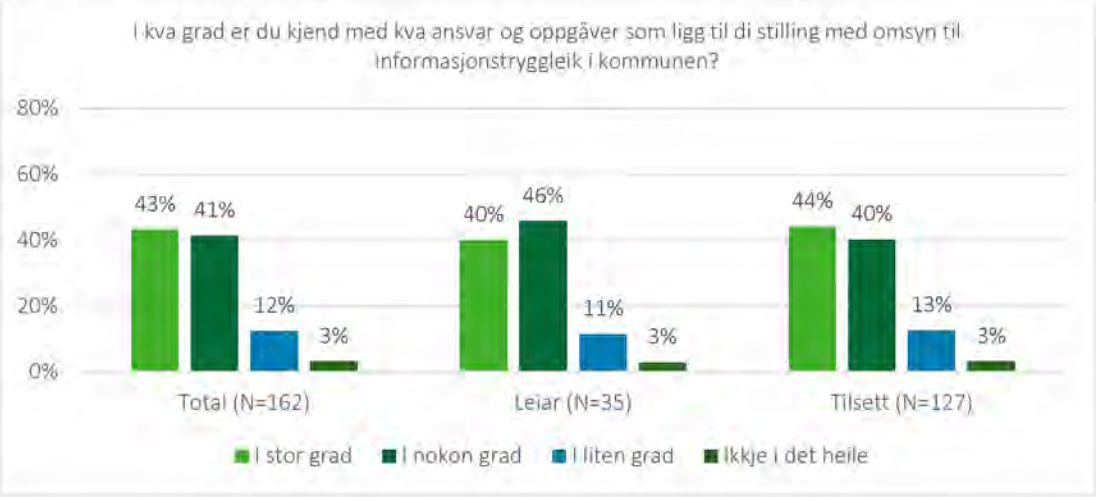
I intervju er det fleire som peiker på at sjølv om rollar og ansvar knytt til informasjonstryggleik er skildra i handboka, så har kommunen framleis ein veg å gå på dette området. Mellom anna blir det vist til at rollar og ansvar er tydeleg fordelt i toppleiargruppa, men at det står att ein del når det gjeld å tydeleggjere kva ein som tilsett eller leiar på ulike nivå er pålagd 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.[9] 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 prosesskildring 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[10] for tinging av brukartilgang som leiarar skal nytte ved tildeling av nye brukartilgangar. Skjema ligg tilgjengeleg på kommunen sine intranettsider. Det er vidare utarbeidd sjekkliste for handsaming av personvernopplysningar, mal for behandling av personvernopplysningar og mal for personvernkartlegging av fagsystem. Dei nemnte sjekklistene 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

[9] Tysnes kommune. Compilo: Støtteprosessar. GDPR/personvern.
[10] Tysnes kommune. *Tinging av brukarident*. Ikkje datert.

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

3.4.2 Vurdering

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

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

3.5 System for og gjennomføring av kontroll og etterprøving av informasjonstryggleik

3.5.1 Datagrunnlag

Kontroll av informasjonstryggleik

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

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

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

Det blir i intervju vist til at kommunen jobbar for å få på plass regelmessig rapportering om informasjonstryggleik og personvern og at det etter planen framover skal utarbeidast ein årleg rapport på tema. Rapporten skal utarbeidast av IT-leiar med innspel og merknader frå personvernombod og vil utgjere grunnlaget for årleg gjennomgang til leiinga. Det blir vist til at det ikkje er planlagd 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.[11]

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

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

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

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[14] 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 nytilsette skal sende dette skjema til *systembrukaransvarleg,* eventuelt til systembrukaransvarleg via e-post til fellestenesta i kommunen. I skjema skal det mellom anna fyllast inn kva fagprogram brukar skal ha tilgang til og kva type tilgangar vedkomande skal ha. Det går fram at skjema skal fyllast ut ved nytilsetjing, 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.[15] I desse skildringane går det fram ansvar for tildeling og ajourhald av brukarrettigheiter i systema. Ikkje alle instruksane er ferdig utfylte, til dømes når det gjeld rettigheiter 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

[11] 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.
[12] Tysnes kommune. *Tinging av brukarident*. Ikkje datert.
[13] Ein kan gjennom intranettskjema bestille brukartilgang for tilsette i domenet @tysnes.kommune.no, men ikkje for tilsette i domenet @tysnesoppvekst.no.
[14] Tysnes kommune. Arkivplan. https://tysnes.arkivplan.no/
[15] ESA (sak og arkivsystem), DIPS Sosial, CosDoc, Agresso UBW, GIS/LINE, Visma Flyktning, Visma Flyt Skole (for kvar av dei tre skulane) og Visma Flyt barnehage.

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

3.5.2 Vurdering

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

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

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

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

Sjå vedlegg 4 for utfyllande revisjonskriterium.

4.3 Personvernombod og personvernerklæring

4.3.1 Datagrunnlag

Personvernombod

Tysnes kommune har utnemnt eit personvernombod og etablert stillingsskildring for personvernombod i kommunen[16]. Rolle og ansvar for personvernombodet er også skildra i kommunen si *handbok i informasjonssikkerhet*.

I stillingsskildringa for kommunen sitt peronvernombod går det fram føremål med stillinga, ansvar og mynde og arbeidsoppgåver. I følgje 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 utpeikt i samsvar med Datatilsynet sine vurderingar knytt til kvalifikasjonskrav for personvernombod.[17] Han påpeiker vidare at personvernombodet har relevant praksis og er godt skikka for oppgåvene som ligg til rolla. Rådmann understrekar vidare at kommunen har følgt 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 vedkommande 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

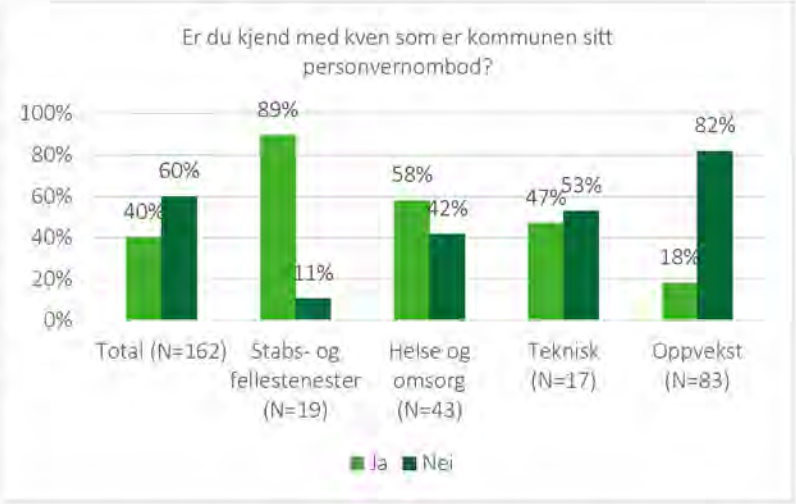
[16] Tysnes kommune. Personvernombod. Ikkje datert

[17] 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 legga til rette for at personvernombodet kan utføra sitt arbeid. [18]

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.[19] 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 naturlig del av verksemda. Vidare gjer kommunen i personvernerklæringa greie for korleis personopplysningar skal handsamast. Overordna inneheld personvernerklæringa ei utgreiing om følgjande tema i eigne 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 personopplysingar
- Kven deler me dine personopplysningar med?
- Innebygd personvern og personvern som standardinnstilliing
- 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 opplysingar 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 personopplysingane frå oss til nokon andre. Denne retten har likevel fleire unntak». Det blir deretter lenka til personopplysningslova (artikkel 12 og 20).

[18] Datatilsynet. Hvordan tilrettelegge for personvernombudets arbeid? Sist endret 06.01.2023. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/personvernombud/hvordan-tilrettelegge/
[19] Tysnes kommune. Fråsegn om personvern: https://www.tysnes.kommune.no/fraasegn-om-personvern.594897.nn.html

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

4.3.2 Vurdering

Tysnes kommune har utnemnt eit personvernombod, og etterlever med dette krav i artikkel 37 i personvernforordninga. Samtidig viser undersøkinga at det har vore utfordrande å sette av tid til å arbeide systematisk med rolla som personvernombod. Revisjonen vil påpeike at kommunen pliktar å stille til 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[20] 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 sjekkliste 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.[21] Sjekklista har lenker til utdjupande informasjon på Datatilsynet sine nettsider.

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

[20] Datatilsynet. Virksomhetenes plikter. Informasjon og åpenhet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/

[21] Tysnes kommune. *Sjekkliste for behandling av personopplysningar*. Tilgjengeleg frå: https://tysnes.intra.custompublish.com/sjekkliste-for-behandling-av-personopplysningar.6580227-587357.html.

[22] Tysnes kommune. *Protokoll over behandlinger av personopplysningar*. Tilgjengeleg frå: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fimg1.custompublish.com%2Fgetfile.php%2F5111947.2571.tolbbpjumwuwml%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[23]og det er under kolonna «kategoriar av personopplysning» lagt inn lenke til Datatilsynet si skildring av kva ein personopplysning er.[24]

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 personopplysingar 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 personopplysingar og at dette heller ikkje blir gjort systematisk. Det er heller ikkje tilstrekkeleg tydeleggjort kven som skal ha dette ansvaret for dei ulik systema. Dette er ikkje i samsvar med krav om utarbeiding av behandlingsprotokollar (artikkel 30 i personvernforordninga).

4.5 Risiko- og konsekvensvurderingar av behandling av personopplysingar

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.

[23] Datatilsynet. Virksomhetenes plikter. Fastsette formål. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/fastsette-formal/

[24] 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). [25] 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 plattforma er dei same som kommunen viser til i samband med forvaltningsrevisjonen.

Det går fram følgande 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 «hyllevare» til dømes system gjennom Fiks-plattforma 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 peronvernopplysingar (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-plattforma 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

[25] KS FIKS Tjenesteplattform er en plattform for utvikling og drift av kommunale applikasjonstjenester. Fiks-plattforma 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

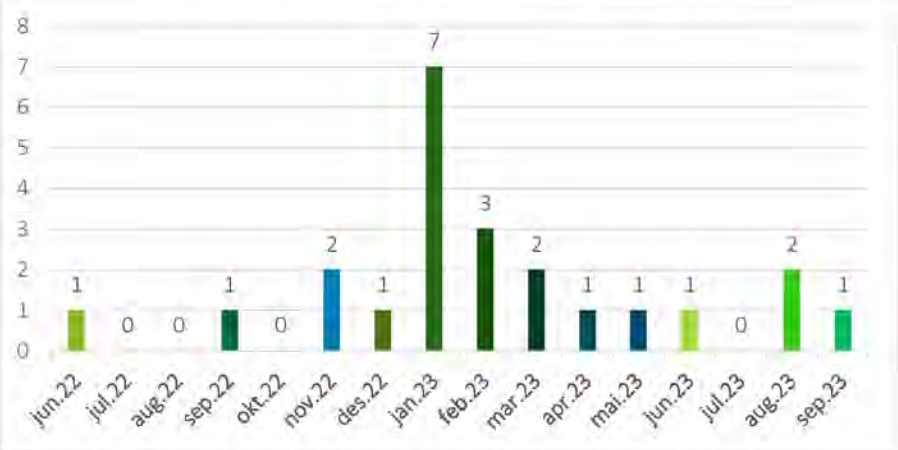
Tysnes kommune omtalar melding av avvik knytt til informasjonstryggleik og personvern i handbok i informasjonssikkerhet. I kapittel 3 om informasjonstryggleik for leiarar går det fram at alle tilsette skal ha kjennskap til korleis avvik skal registrerast i Compilo. Det går vidare fram i same kapittel at alle tilsette som oppdagar brot på informasjonstryggleiken og brot på reglementet, skal varsla 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 utløyser 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*[26] 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.[27] 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)



[26] Tysnes kommune. Rutine for avvik og alvorlege hendingar. Compilo. Ikkje datert.
[27] 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 rettigheiter eller friheiter»[28], 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 innbyggarar 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 uvedkomande 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.

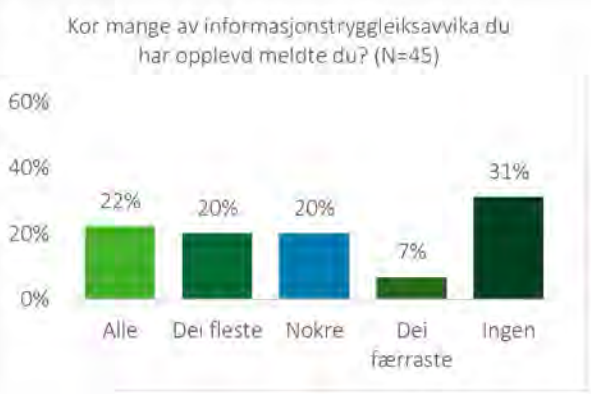
I samband med verifiseringa av rapporten blir det påpeikt at i kommunen er det rådmannen som er behandlingsansvarleg å såleis har plikt til å melda avvik vidare til Datatilsynet. Det blir vidare haldt fram at dersom nokon skulle meine at denne plikta ikkje vert ivareteke av rådmann, så kan personvernombod,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

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

[28] Personvernforordninga artikkel 35, første ledd.
[29] 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[30] 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.

Figur 5: Melding om opplevde informasjonstryggleiksavvik



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. [31] 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 færraste» av avvika fekk spørsmål om avvika dei har meldt frå om har blitt følgt opp.[32] Om lag halvparten (52 prosent) svarer at avvika blei følgt opp, medan 16 prosent oppgjev at avvika delvis blei følgt opp. Litt over 13 prosent svara at avvika dei melde inn ikkje blei følgt opp og 19 prosent svarar «veit ikkje» på dette spørsmålet.

4.6.2 Vurdering

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

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

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

[30] N=45
[31] N=27
[32] N=31
[33] Datatilsynet. Hvilke brudd skal meldes til Datatilsynet? Publisert 24.03.2023. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/avvik/hvilke-brudd-skal-meldes-til-datatilsynet/

5 Kompetanse blant tilsette

5.1 Problemstilling

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

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

Under dette:

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

5.2 Revisjonskriterier

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

Kommunen skal:

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

Digitaliseringsdirektoratet tilrår at kommunen bør[34]:

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

Sjå vedlegg 4 for utfyllande revisjonskriterium.

5.3 Rutinar for opplæring i informasjonstryggleik

5.3.1 Datagrunnlag

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

[34] Digitaliseringsdirektoratet. Veileder i kompetanse- og kulturutvikling innen digital sikkerhet

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

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

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

Tysnes kommunen har vidare vedtatt eit introduksjonsprogram for nytilsette[35]. Introduksjonsprogrammet er ei rutine ved tilsetjing som mellom anna innehald ei sjekkliste som leiar og kontaktperson for den nytilsette skal bruke for å sikre at den nytilsette mottar viktig informasjon og opplæring. Nokre av punkta i sjekklista er at den nytilsette 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 nytilsette. 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.[36] 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.[37] 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.[38]

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

[35] Tysnes kommune. *Introduksjonsprogram for nytilsette*. Vedtatt i kommunestyret 12.12.2017.
[36] 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
[37] Det er om lag 120 tilsette i skular og barnehagar og til saman om lag 350 tilsette i heile kommunen.
[38] Tysnes kommune. *Årsmelding 2021*. 31.03.2021.

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

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

5.4 Kjennskap til og etterleving av retningslinjer og rutinar for informasjonstryggleik

5.4.1 Datagrunnlag

Kjennskap til retningslinjer og rutinar for informasjonstryggleik

Innleiingsvis i spørjeundersøkinga fekk respondentane spørsmål om dei handsamar eller kjem i kontakt med personopplysningar i sitt arbeid.[39] 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.

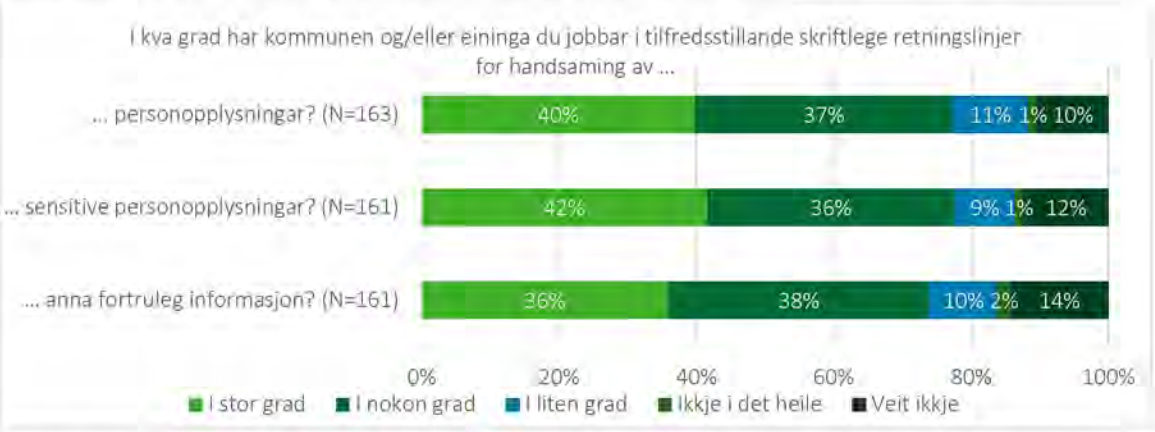
Figur 6: Del respondentar som handsamar personopplysningar og sensitive personopplysningar gjennom sitt arbeid

Respondentane blei også stilt spørsmål om dei handsamar anna *fortruleg informasjon*.[40] 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».

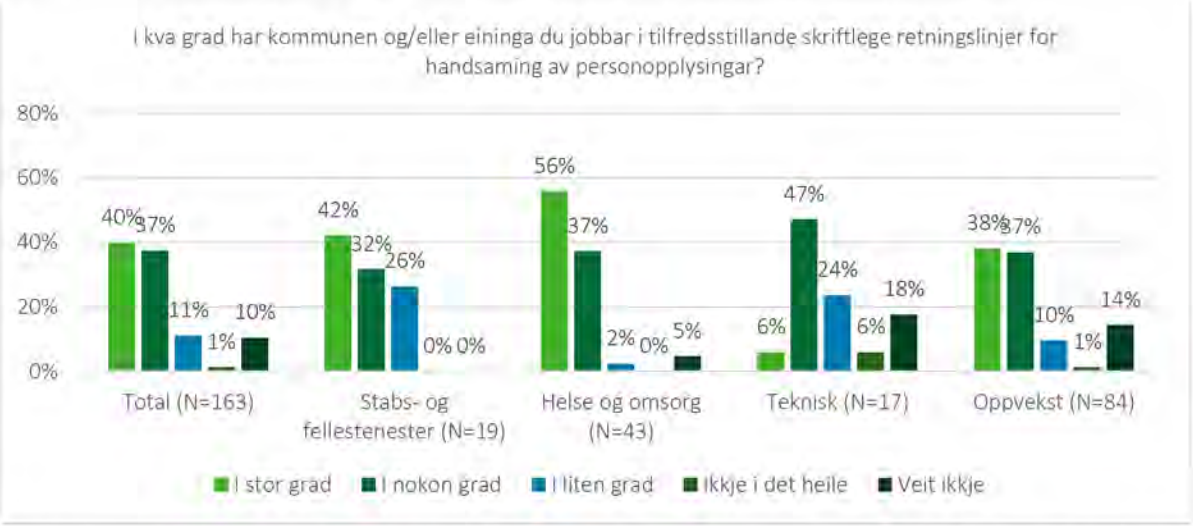
[39] I spørjeundersøkinga var det lagt inn ei forklaring av omgrepa personopplysningar og sensitive personopplysningar i samband med dette spørsmålet.
[40] I spørjeundersøkinga var det lagt inn ei forklaring på kva som er meint med fortruleg informasjon. Sjå elles ordliste på side 3 i rapporten

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



Nærare analyse viser at det er skilnadar 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 skriftelege 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.

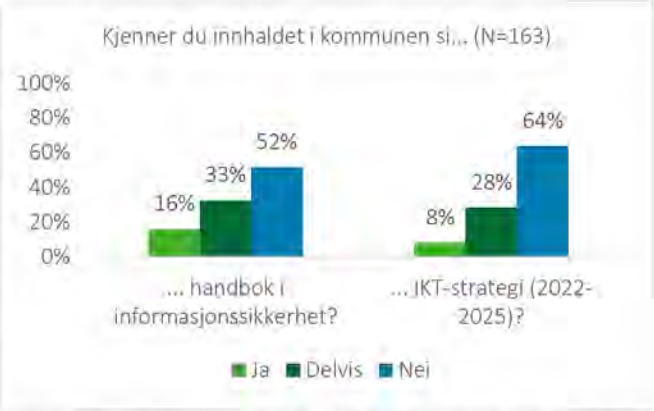
Respondentane som svara at kommunen og/eller einingа «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer på områda som nemnt over, fekk eit oppfølgingsspørsmål om dei veit kvar dei finn rutinar og retningslinjer for handsaming av personopplysningar, sensitive personopplysningar og/eller anna fortruleg informasjon som gjeld kommunen og/eller einingа.[41] På dette spørsmålet svara 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.

[41] 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

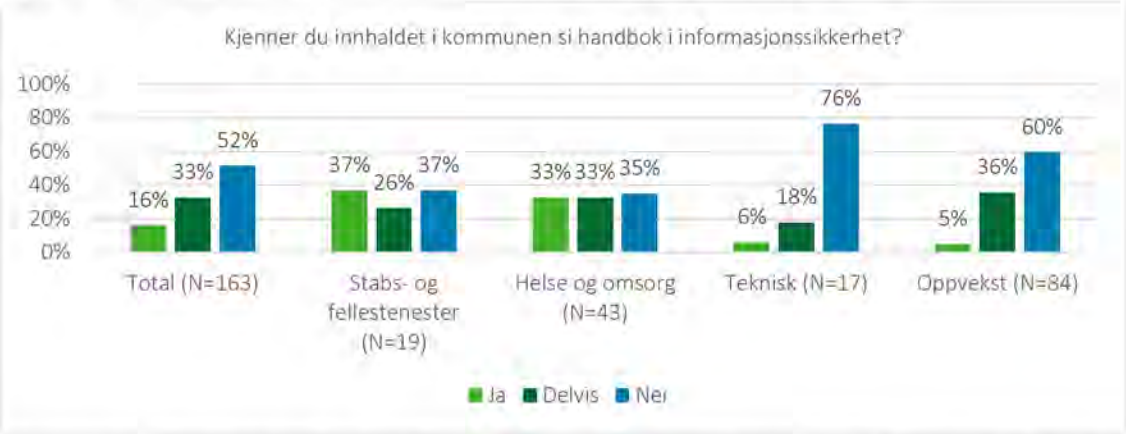


Ved nærare analyse går det fram at det er skilnad på svara frå respondentane på dette spørsmålet på bakgrunn av både kva sektor dei jobbar innan og om dei er tilsett med leiaransvar eller ikkje. Medan om lag ein av tre (34 prosent) tilsette med leiaransvar svarar at dei *ikkje* kjenner til innhaldet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

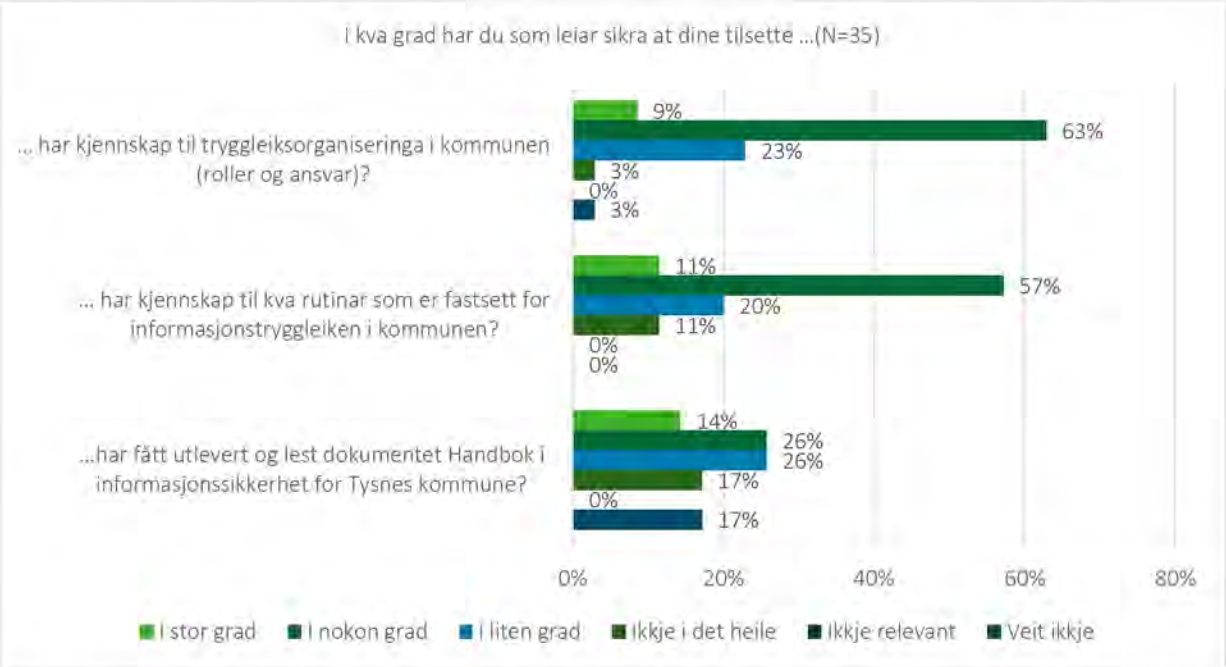


I spørjeundersøkinga svarar 17 prosent[42] av respondentane med leiaransvar at dei «ikkje i det heile» har sikra at dei tilsette har fått utlevert og lest handbok i informasjonssikkerhet, medan 26 prosent svarar at dei høvesvis «i liten grad» eller «i nokon grad» har sikra dette. 14 prosent av leiarane 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[43] svarer at dei «ikkje i det heile» har sikra at deira tilsette har kjennskap til kva rutinar som er fastsett for informasjonstryggleiken i kommunen.

[42] 5 respondentar
[43] 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.[44] 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.

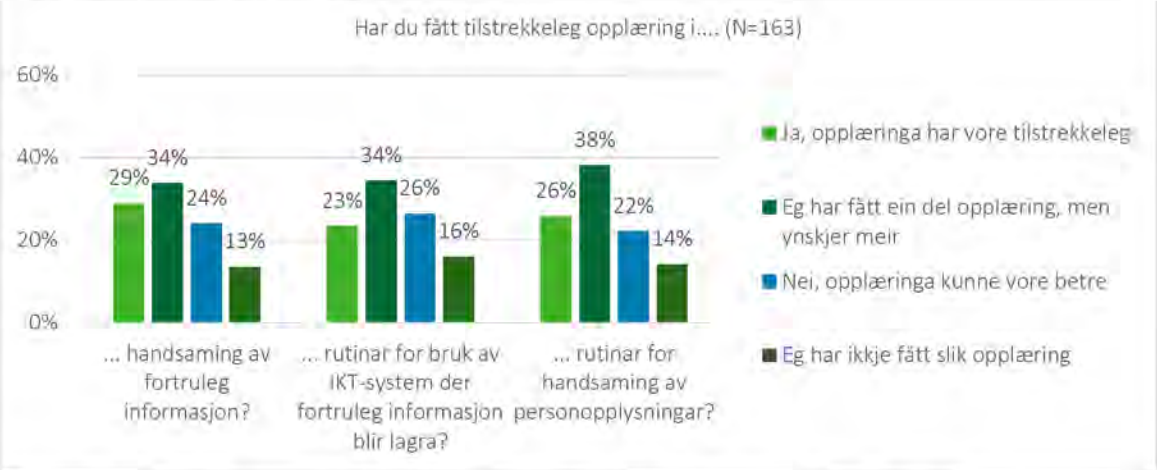
Figur 12: Nødvendig autorisering og kompetanse for å ivareta informasjonstryggleik

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[45] 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

[44] N=35
[45] høvesvis 24 %, 26 % og 22 %

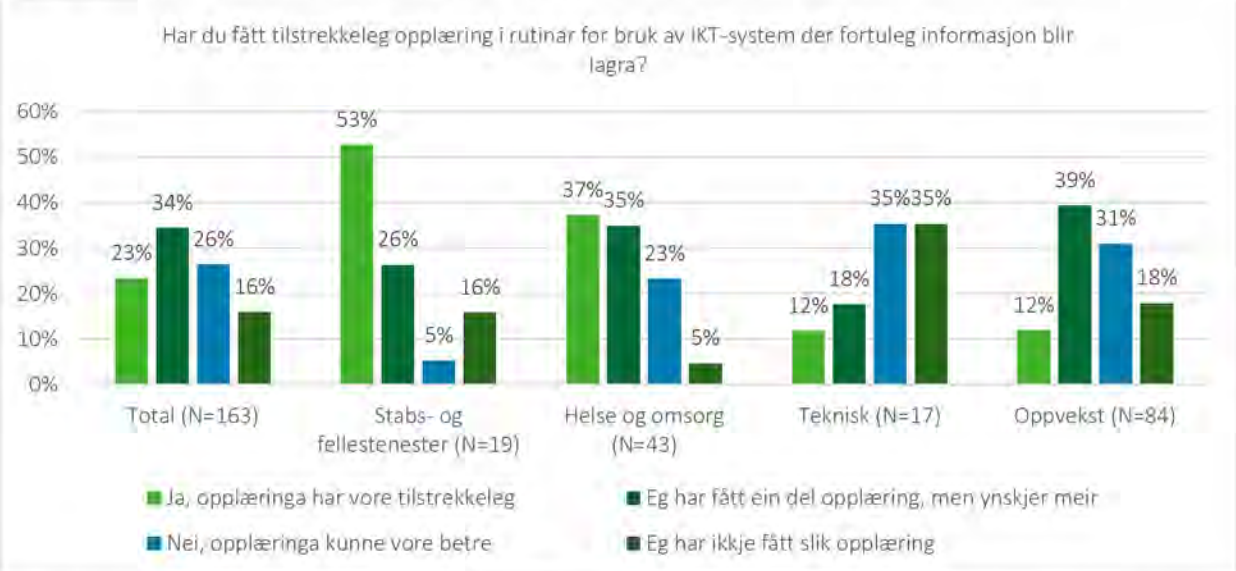
gjeld opplæring i rutinar for handsaming av personopplysningar, så svarar 38 prosent av respondentane at dei har fått ein del opplæring men ønsker meir.

Figur 13: Tilstrekkeleg 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 svarar 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 svarar 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* svara «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

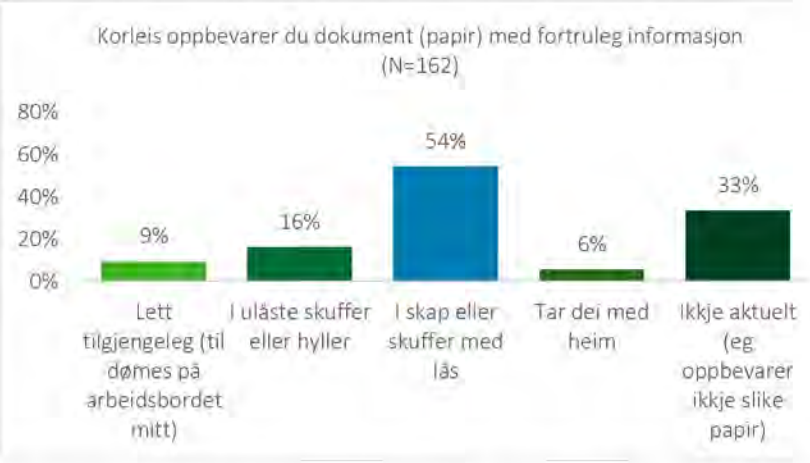
Etterleving av retningslinjer og rutinar for informasjonstryggleik

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».

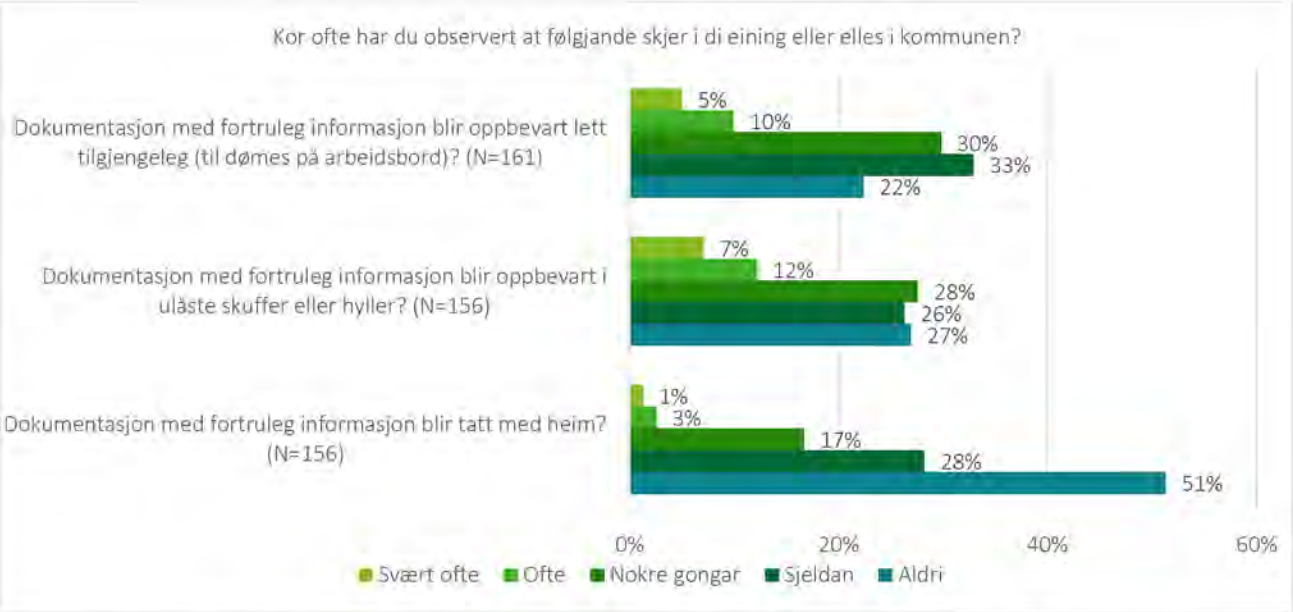
Respondentane i spørjeundersøking blei også stilt ulike spørsmål knytt til eige og andre tilsette si etterleving av retningslinjer og rutinar for informasjonstryggleik. Respondentane blei mellom anna bedt om å svare på korleis dei oppbevarer dokument med fortruleg informasjon. Som det går fram av figuren 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

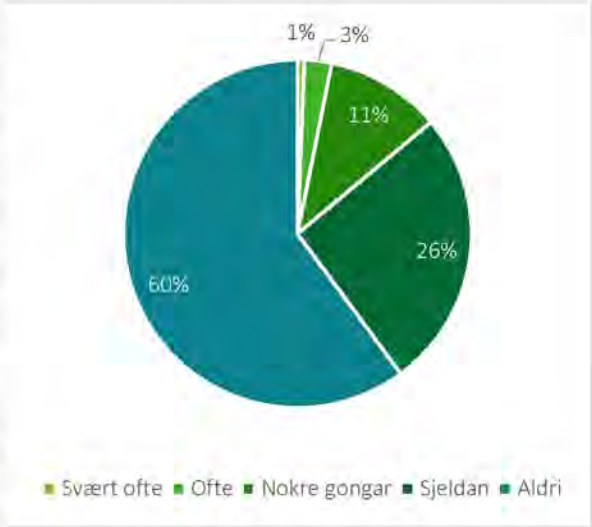


Respondentane fekk vidare spørsmål om kor ofte dei observerer at fortruleg informasjon frå møterom eller liknande (dokument, informasjon på tavle/flipover, osb.) blir fjerna før romma blir forlate.[46] Her svarar over halvparten av respondentane at dette «svært ofte» blir fjerna, medan 16 prosent svarer 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).

[46] 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.

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



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

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

Figur 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 einingа 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 einingа «i stor grad» eller «i nokon grad» har tilfredsstillande retningslinjer for handsaming av personopplysningar, at dei ikkje kjenner til kvar dei finn desse retningslinjene og rutinane. Revisjonen vil understreke at kommunen etter personvernforordninga er forplikta til å sette i verk eigna tiltak, både organisatoriske og tekniske, for å sikre og påvise at personopplysningar blir handsama i samsvar med krav til dette i regelverket (personvernforordninga artikkel 24). Som ein del av dette bør kommunen mellom anna sikre at kommunen sine styrande dokument for informasjonstryggleik er tilgjengeleg og kjend for dei tilsette i kommunen.

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

6 Konklusjon og tilrådingar

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[47] Datatilsynet. Virksomhetenes plikter. Informasjon og åpenhet. https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjon-og-apenhet/

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

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

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

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

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

Basert på funna i spørjeundersøkinga, vurderer revisjonen at dei tilsette i kommunen ikkje har tilstrekkeleg kjennskap til retningslinjer og rutinar for informasjonstryggleik. Til dømes svarar om lag halvparten av alle respondentane, og om lag ein av tre respondentar med leiaransvar, at dei *ikkje* kjenner innhaldet i kommunen si handbok i informasjonssikkerhet. Svar i spørjeundersøkinga indikerer vidare at det relativt store skilnadar mellom sektorane i kommunen når det gjeld kjennskap til styrande dokument for informasjonstryggleik. Til dømes går det fram at 93 prosent av respondentane frå oppvekstsektoren oppgjev å handsame både personopplysningar og sensitive personopplysningar, men 60 prosent av respondentane frå denne sektoren kjenner ikkje til innhaldet i kommunen si handbok i informasjonstryggleik. Det er vidare 14 prosent av respondentane frå oppvekstsektoren som ikkje veit om kommunen eller einingа 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 einingа «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.

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

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

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

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

Vedlegg 1: Høyringsuttale

Tysnes kommune

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
5685 UGGDAL
e-post: post@tysnes.kommune.no
Telefon:53 43 70 00
Bankgiro: 3525.07.00340
Org.nr: 959412340

Vedlegg 2: Utvida høyringsuttale

Tysnes kommune

Sentraladministrasjonen - stab

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

Kjersti Gjuvsland

Utvida uttale til rapport - forvaltningsrevisjon informasjonstryggleik og personvern
Det vert vist til epost av 13. desember d.å., her følgjer endeleg uttale.

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

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

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

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

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

Tysnes kommune
Uggdalsvegen 301
5685 UGGDAL
e-post: post@tysnes.kommune.no
Telefon:53437000
Bankgiro: 3525.07.00340
Org.nr: 959412340

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

Styringssystem og informasjonstryggleik

3.3.1 Omsynet til ISO/IEC 27001

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

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

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

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

Revisjonen skriv på s. 10 i rapporten at:

> «Digdir tilrår at offentlege verksemder baserer seg på ISO/IEC 27001…»

Det vert her vist til note 5 der revisjonen skriv:

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

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

3.3.2 Vurdering

Under vurdering skriv revisjonen mellom anna:

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

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

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

eForvaltningsforskrifta § 15 har slik ordlyd:

§ 15.*Internkontroll på informasjonssikkerhetsområdet*

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

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

Omfang og innretning på internkontrollen skal være tilpasset risiko.

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

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

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

> «Gjennomgangen til leiinga skal haldast årleg for leiargruppa til rådmannen.
>
> I møte skal det samanfattast status for informasjonstryggleiksarbeidet i kommunen, og dessutan avdekkast om tryggleiken blir vareteken i høve mål, strategiar og prosedyrar og vedtakast tiltak for det vidare sikkerhetsarbeidet. Tiltak skal sikra at sikkerhetsmål, strategi og organisering av informasjonstryggleikssystemet er oppdaterte og i samsvar med behovet til kommunen.
>
> I gjennomgangen til leiinga skal m.a. følgjande punkt gåast gjennom og bli vurderte:
>
> • Resultat og hovudkonklusjonar frå informasjonstryggleiksrevisjonar
>
> • Registrerte avvik
>
> • Rapporter frå offentlege og interne tilsyn
>
> • Endringar i lover, forskrifter og offentlege sikkerhetskrav
>
> • Endringar i dei personopplysningane som verksemda skal behandla
>
> • Endringar i trusselbiletet som kjem fram i gjennomførte risikovurderingar
>
> • Status på hendingar rundt teknisk informasjonstryggleik
>
> • Organisatoriske endringar
>
> • Bygningsmessige endringar
>
> • Planar og framdrift for å ivareta intern kontroll og informasjonstryggleik.»

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

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

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

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

3.5.2

Revisjonen skriv under dette punktet:

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

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

Konklusjon og tilrådingar

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

Tysnes kommune har ikkje etablert styringssystem for tilfredsstiller krav i sentrale føresegner:

- Kulepunkt 1: Her er det eit spørsmål om tolking av eForvaltningsforskriften § 15. Er problemstillinga her at styrande dokument ikkje eksplisitt viser til standard, eller er avviket at styrande dokument ikkje tar opp i seg innhaldet av etablerte standardar. Ein meir nøytral konklusjon vil her vera:

- Kommunen sine styrande dokument må vise til kva standard dei byggjer på.

- Kulepunkt 2: Ein konklusjon som er langt meir i tråd med rapporten er at Tysnes kommune langt på veg har skildra ansvarsforhold knyt til informasjonstryggleik. Undersøkinga viser tilsvarande at ansvarsforhold ennå ikkje er fullt ut implementert og forstått i alle deler av organisasjonen.
- Det må presiserast i ansvarsskildringa at rådmannen er behandlingsansvarleg, dei funksjonar som er lagt til rådmannen særskilt må skildrast nærare.
- Det må sikrast at rollefordelinga vert forstått og etterlevd på alle nivå i organisasjonen.
- Det bør særskilt gjerast ei vurdering knytt til det som ser ut til å vera avvikande praksis innanfor oppvekst.

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

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

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

- Revisjonen tilrår at rapport knytt til leiinga sin årlege gjennomgang også vert sendt til kommunestyre for informasjon.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Revisjonen sine tilrådingar:

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

Avslutning:

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

Med helsing

Steinar Dalland
rådmann

Brevet er elektronisk godkjent.

Kopi til:

Vedlegg 3: Kommentar til utvida høyringsuttale

Innleiing

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Vedlegg 4: Revisjonskriterier

Informasjonstryggleik

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

Å sørgje for *konfidensialitet* inneber å hindre ikkje-autorisert innsyn i informasjon som ikkje skal vere tilgjengeleg for alle; å sørgje for *integritet* inneber å hindre ikkje-autorisert endring og sletting av informasjon; å sørgje 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.[52] Denne tredde i kraft 20. juli 2018, og gjennomfører EU si personvernforordning – kjend som GDPR[53] – 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.[54] Databehandlarar er eventuelle tenesteleverandørar til kommunen som behandlar personopplysningar, som til dømes leverandør av løn- og personalsystem. Forordninga artikkel 28 nr. 3 stiller krav om at behandling av personopplysningar utført av ein databehandlar skal vere underlagt ein avtale med nærare spesifisert innhald (bokstav a til h).

Internkontroll og styringssystem for informasjonstryggleik

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

---

[52] Lov om behandling av personopplysninger (personopplysningsloven)
[53] General Data Protection Regulation
[54] Jf. *En veiledning om internkontroll og informasjonssikkerhet* (Datatilsynet 2009, s. 11).

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

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

> Forvaltningsorgan som benytter elektronisk kommunikasjon skal ha beskrevet mål og strategi for informasjonssikkerhet i virksomheten (sikkerhetsmål og sikkerhetsstrategi). Disse skal danne grunnlaget for forvaltningsorganets internkontroll (styring og kontroll) på informasjonssikkerhetsområdet. Sikkerhetsstrategien og internkontrollen skal inkludere relevante krav som er fastsatt i annen lov, forskrift eller instruks.
>
> Forvaltningsorganet skal ha en internkontroll (styring og kontroll) på informasjonssikkerhetsområdet som baserer seg på anerkjente standarder for styringssystem for informasjonssikkerhet. Internkontrollen bør være en integrert del av virksomhetens helhetlige styringssystem. Det organet departementet peker ut skal gi anbefalinger på området.

I rettleiar til e-forvaltingsforskrifta går det fram følgande når det gjeld § 15 andre ledd:

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

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 rettleiingsmateriell 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 rådigheit 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 personvernkonsekvensar (bokstav c), og samarbeide med Datatilsynet (bokstav d).

---

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

Forordninga stiller vidare krav til kva avvik som skal meldast til Datatilsynet. Hovudregelen slik denne går fram i artikkel 33 er at alle avvik som skuldast brot på personopplysningstryggleiken (utilsikta sletting, tap, endring, ulovleg spreiing 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 personopplysingar 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[56] omhandlar mellom anna oppfølging og opplæring. Her går det fram at målet med brukaropplæring er å syte for at brukarane er merksame på trugslar mot personvernet og informasjonstryggleiken generelt, og at dei er gitt høve til å etterleve dette i sitt daglege arbeid. Opplæringa bør vere tilpassa dei ulike målgruppene sitt behov for opplæring og fordelast over tid. Brukarane bør få opplæring i rutinar, tryggleiksprosedyrar og riktig bruk av informasjonssystem for å redusere potensielle risikoar.

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

[56] *Internkontroll og informasjonssikkerhet*. Datatilsynet. Publisert 23.06.2018. Sist endra 30.10. 2018. https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/internkontroll-og-informasjonssikkerhet/

Anna regelverk

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

Vedlegg 5: Sentrale dokument og litteratur

Lov og forskrift

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

Førearbeider, rundskriv, rettleiarar mv.

- Diverse rettleiingsmateriell frå Digitaliseringsdirektoratet
- Diverse rettleiingsmateriell frå Datatilsynet

Dokument frå kommunen

- Tysnes kommune. *Handbok i informasjonssikkerhet*. 2022. Ikkje datert
- Tysnes kommune. *IKT-strategi i Tysnes kommune 2022-2025*. Ikkje datert
- Tysnes kommune. *Årsmelding 2021*. 31.03.2021.
- Tysnes kommune. *Agresso UBW – instruks for behandling av elektroniske document*. Ikkje datert.
- Tysnes kommune. *Cosdoc – instruks for behandling av elektroniske arkivdokument*. Ikkje datert.
- Tysnes kommune. *DIPS – Sosial – instruks for behandling av elektroniske system tysnes.arkivplan.no*. Ikkje datert.
- Tysnes kommune. *ESA – instruks for behandling av elektroniske dokument tysnes.arkivplan.no*. Ikkje datert.
- Tysnes kommune. *GIS – Line instruks for behandling av elektroniske dokument*. Ikkje datert.
- Tysnes kommune. *HelseCERT – Avtale om deltakelse i HelseCERTs nasjonalt beskyttelsesprogram*. 20.01.2023.
- Tysnes kommune. *HelseCERT – Informasjon om Nasjonalt Beskyttelsesprogram*. Ikkje datert.
- Tysnes kommune. *HelseCERT – Skjema – Deltakelse i nasjonalt beskyttelsesprogram*. 20.01.2023.
- Tysnes kommune. *HelseCERT Sårbarhetsoversikt*. Ikkje datert.
- Tysnes kommune. *Infrastruktur – informasjonstryggleik*. Ikkje datert.
- Tysnes kommune. *Krisehandtering IT – eksterne ressursar – eksterne som kan yta akutt hjelp*. Ikkje datert.
- Tysnes kommune. *Medlemskap i HelseCERT*. 20.01.2023.
- Tysnes kommune. *Sjekkliste 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 Innreiseoppfolgning*. Datert 08.06.2021
- Tysnes kommune. *DPIA Fiks vaksinestatus*. Datert 21.09.2021

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

Deloitte.

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2023/406-6
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**2/24**	**07.03.2024**

Plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024-2028 - prosessmøte 1

Forslag til vedtak

Kontrollutvalet tek, på bakgrunn av prosessmøte 1, risiko- og vesentlegvurdering (ROV) gjeldande forvaltningsrevisjon og eigarskapskontroll så langt til orientering.

Samandrag

Føremålet med saka er å gje kontrollutvalet moglegheit til å diskutera og vurdera risiko innanfor kommunen sine ansvarsområde og selskapa der kommunen har eigarinteresser, og gjere greie for neste trinn i kontrollutvalet sitt arbeid med risiko- og vesentlegvurdering (ROV). ROV skal leggjast til grunn for plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024 - 2028.

Hogne Haktorson
kontrollsjef

Helge Inge Johansen
spesialrådgjevar

Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift

Saksutgreiing

Bakgrunn for saka

Kontrollutvalet gjorde slikt vedtak i PS 32/23, i møte 23.11.2023:

1. Kontrollutvalet ber Deloitte AS gjennomføre risiko- og vesentlegvurderingar (ROV) av verksemda i Tysnes kommune, verksemda i kommunen sine selskap og av Tysnes kommune sin eigarskap i selskap.
2. Vidare ber kontrollutvalet Deloitte AS utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024 – 2028.
3. Det er ei målsetting at prosessmøte 1 skal gjennomførast i første møte i kontrollutvalet i 2024 og at prosessmøte 2 skal gjennomførast i kontrollutvalet i mai 2024.
4. Det er videre ei målsetting at forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for 2024 – 2028 skal leggast fram for kommunestyret i juni 2024.

Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse for å starte opp og gjennomføra planprosessen, mellom anna gjennom vedtak i denne saka.

Når utkast til plan for forvaltningsrevisjon og plan for eigarskapskontroll 2024 - 2028 ligg føre, etter at prosess er gjennomført, skal kontrollutvalet innstilla til kommunestyret, som vedtek plan for forvaltningsrevisjon og plan for eigarskapskontroll, jf. kommunelova §§ 23-3 og 23-4.

Vurderingar og verknader

I dette møte skal Deloitte gjennomføra «Prosessmøte 1». I prosjektplanen som blei vedteken i møte 23.11.2023 vart «Prosessmøte 1» omtala slik:

«I det første prosessmøtet vil kontrollutvalet få høve til å diskutere og vurdere risikoar innanfor kommunen sine ansvarsområder og knytt til drifta i selskapa der kommunen har eigarinteresser, basert på eiga erfaring frå arbeidet i kontrollutvalet.

I denne prosessen nytter vi eit «risikospel» som har ei oversikt over dei ulike tenesteområda i kommunen. Ved bruk av farga spelbrikker får kontrollutvalsmedlemmane høve til å vurdere risiko knytt til ulike tenesteområde.»

Konklusjon

Sekretariatet rår til at kontrollutvalet med bakgrunn i prosessmøte 1, tek risiko og vesentlegvurderinga (ROV) gjeldane forvaltningsrevisjon og eigarskapskontroll så langt til orientering.

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2024/32-1
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**3/24**	**07.03.2024**

Årsmelding 2023 for kontrollutvalet

Forslag til innstilling

Kommunestyret godkjenner årsmelding 2023 for kontrollutvalet.

Samandrag

Sekretariatet har laga forslag til utvalet si årsmelding for 2023. Årsmeldinga frå kontrollutvalet må reknast som ein del av den lovpålagte rapporteringa frå utvalet til kommunestyret.

Hogne Haktorson
kontrollsjef

Helge Inge Johansen
spesialrådgjevar

Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift

Vedlegg
1 Årsmelding 2023 for kontrollutvalet

Saksutgreiing

Bakgrunn for saka

Sekretariatet har utarbeida forslag til årsmelding for kontrollutvalet 2023. Årsmeldinga er ein lekk i rapporteringa frå utvalet til kommunestyret. Sjå kommunelova § 23-5 som seier:

«Kontrollutvalget skal rapportere resultatene av sitt arbeid til kommunestyret eller fylkestinget. I saker som skal oversendes til kommunestyret eller fylkestinget, skal kommunedirektøren gis anledning til å uttale seg før kontrollutvalget behandler saken.»

Vedtakskompetanse

Det er kommunestyret som har vedtakskompetanse i saker som vert rapportert frå kontrollutvalet, jf. kommunelova § 23-5 der det står dette:

«Kontrollutvalget skal rapportere resultatene av sitt arbeid til kommunestyret eller fylkestinget.»

Vurderingar og verknader

Årsmelding for 2023 er vedlagt saka. Ettersom årsmeldinga også fungerar som ei rapportering til kommunestyret, vert det lagt opp til endeleg handsaming av årsmeldinga der, slik det og har vore gjort i ei årrekke.

Konklusjon

Kontrollutvalet tilrår at kommunestyret godkjenner årsmeldinga.

TYSNES KOMMUNE

ÅRSMELDING 2023

FOR

KONTROLLUTVALET

1 Føremål og oppgåver for kontrollutvalet

Føremålet med kontrollutvalet sitt arbeid er å medverke til at det vert allmenn tillit til at kommunen sine oppgåver vert løyst på best mogleg måte, og i samsvar med gjeldande lover og forskrifter.

I kommunelova § 23-1 står det m.a.:

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. at kommunen har en forsvarlig revisjonsordning.

2 Samansetjing av kontrollutvalet

Kontrollutvalet for valperioden 2019 – 2023 var slik samansett:

Medlemmer :	**Varamedlemmer :**
Lorentz Lunde, (Krf), leiar	1. Lars Enes 2. Monica Lavik Frøkedal
Britt Ersvær (Ap), nestleiar	1.Gerhard Stoltz
Lars Heine Kåsa (Sp)	1. Linn Frøkendal 2. Helge Hauge
Kåre Haugland (Frp)	1. Marit Gunn Daland
Sigvard Michael Madsen (H)	1. Egil Bjarne Berge 2. Ingrid Sunde 3. Kirsten Gunn Epland

I følgje lova skal minst ein av medlemmane i kontrollutvalet og vera medlem av kommunestyret. Sigvard Michael Madsen var kommunestyremedlem.

Kontrollutvalet for valperioden 2023 – 2027 er slik samansett:

Medlemmer :	**Varamedlemmer :**
Anne Kristi Alfstad (H), leiar	1. Bjørn Lande 2. Egil Bjarne Berge
Lars Heine Kåsa (Sp), nestleiar	1. Helge Hauge 2. Kristin Teigland Gjerstad Kleppe
Lorentz Lunde (Krf)	1. Arild Frøyseth
Asbjørn Myklestad (Ap)	1. Rolf Simonsen
Tor Magnus Hauge (Inp)	1. Terje Dalsgård

I denne valperioden er Asbjørn Myklestad (Ap) som er kommunestyremedlem.

3 Om verksemda til kontrollutvalet i 2023

- Kontrollutvalet hadde 4 møter og handsama 34 politiske saker og 6 referatsaker i 2023.
- Ordførar har møterett i kontrollutvalet.
- Rådmann og andre tilsette i kommunen har møtt for å informera til kontrollutvalet, når dei har vorte innkalla.
- Revisjonen har og møtt på møta i kontrollutvalet.
- Kontrollutvalet har fått tilgang til den informasjonen det har vorte bede om.

4 Sekretariatsordninga

I kommunelova § 23-7 Sekretariatet står det dette:

Kommunestyret og fylkestinget skal sørge for at kontrollutvalget får sekretariatsbistand som tilfredsstiller utvalgets behov.

Sekretariatet skal påse at de sakene som behandles av kontrollutvalget, er forsvarlig utredet, og at utvalgets vedtak blir iverksatt.

Sekretariatet skal være uavhengig av kommunens eller fylkeskommunens administrasjon og av den eller dem som utfører revisjon for kommunen eller fylkeskommunen.

Sekretariatsfunksjonen kan ikke legges til
a) ansatte i kommunen eller fylkeskommunen som har andre arbeidsoppgaver enn å være sekretær for kontrollutvalget
b) den som utfører revisjon for den aktuelle kommunen eller fylkeskommunen
c) medlemmer av kontrollutvalget, kommunestyret eller fylkestinget i den aktuelle kommunen eller fylkeskommunen.

Den som utfører sekretariatsoppgaver for kontrollutvalget, er direkte underordnet kontrollutvalget og skal følge de retningslinjer og pålegg som utvalget gir.

Kommunestyret og fylkestinget velger selv sekretariat for kontrollutvalget etter innstilling fra kontrollutvalget.

Sekretariat for kontrollutvalet i Vestland fylkeskommune utfører sekretariatstenesta for kontrollutvalet i Tysnes kommune. Helge Inge Johansen har utført sekretæroppgåver på kontrollutvalsmøta i 2023.

Sekretariat for kontrollutvalet i Vestland fylkeskommune er også sekretariat for kontrollutvalet i fylkeskommunen, samt kontrollutvala i desse kommunane: Askøy, Austevoll, Bjørnafjorden, Bømlo, Eidfjord, Fitjar, Kvam, Kvinnherad, Samnanger, Stord, Ullensvang, Ulvik, Vaksdal og Øygarden. I tillegg til dette har sekretariatet også vore settesekretariat for Møre og Romsdal fylkeskommune sitt kontrollutval i heile 2023. Vestland fylkeskommune/Hordaland fylkeskommune har utført sekretariatstenester for Tysnes kommune sidan 2008. Det er gjennomført konkurranse gjeldande sekretariatstenester for kommunane i Sunnhordland andre halvår 2022. Vestland fylkeskommune held fram som sekretariat for Tysnes kommune sitt kontrollutval. Ny avtale gjeld frå 01.01.2023 til 01.01.2025, med opsjon på 1 + 1 år.

5 Revisjonstenesta

Kontrollutvalet skal på vegne av kommunestyret ha tilsyn med den kommunale forvaltninga. Utvalet må halda seg orientert om kva saker revisjonen arbeider med og føra tilsyn med at revisjonsarbeidet er à jour og føregår i samsvar med forskrift og vedtak.

På grunnlag av revisjonen sine rapportar, rekneskapsplan og annan informasjon, har utvalet ført tilsyn med at forvaltninga er i samsvar med gjeldande lover, forskrifter og vedtak. Utvalet skal vidare i samarbeid med revisjonen gjennomføra ei systematisk vurdering av bruk og forvaltning av dei kommunale midlar, med utgangspunkt i oppgåver, ressursbruk og oppnådde resultat (forvaltningsrevisjon).

Deloitte AS er revisor for Tysnes kommune. Noverande avtale er gjeldande frå 01.07.2020 og gjeld fram til og med 30.06.2024. Deloitte har lagt fram revisjonsmelding, slik kravet er, samt rapportar og annan informasjon om revisjonen sitt arbeid. Kontrollutvalet har starta arbeidet med ny konkurranseutsetjing av revisjonstenester.

Til dagleg er det den valde revisor som utfører tilsynet og kontrollen mot kommunen, men kontrollutvalet har eit eige ansvar med å sjå til at arbeidet vert tilfredsstillande utført. Kommunelova stiller krav om at utvalet sjølv må visa ei aktiv haldning. For å få utført det arbeid utvalet er pålagt, er ein avhengig av god kommunikasjon med kommunestyret, administrasjonen i kommunen og revisor. Samarbeidet har vore godt med dei aktuelle aktørar. Ansvarleg revisor har vore partner i Deloitte Unni-Renate Moe, som i tråd med regelverket har lagt fram eigenvurdering for at Deloitte er uavhengig i høve til Tysnes kommune.

Utanom revisjon av årsrekneskapen, har revisor og gjennomført forenkla etterlevingskontroll, laga revisjonsplan og lagt fram interimsrevisjonsrapport, som alle er handsama i kontrollutvalet.

6 Arbeid med forvaltningsrevisjon.

Kommunelova § 23-2. Kontrollutvalgets ansvar og myndighet punkt c lyd slik:

«Kontrollutvalget skal påse at:

c) det utføres forvaltningsrevisjon av kommunens eller fylkeskommunens virksomhet, og av selskaper kommunen eller fylkeskommunen har eierinteresser i.»

Vidare går det fram av kommunelova § 23-3. Forvaltningsrevisjon dette:

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

Kontrollutvalet vurderer m.a. kvaliteten i sakshandsaminga og om vedtak og premisser er tilstrekkeleg klårt utforma til at vedtaka kan effektuerast. I den nye kommunelova gjeld dette også internt i selskap som kommunen har eigarinteresser i. I punkta nedanfor kjem kort omtale av dei revisjonane innan dette feltet som kontrollutvalet har handsama i 2023.

6.1 Plan for forvaltningsrevisjon

Kommunelova § 23-3 Forvaltningsrevisjon lyd m.a. slik:

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 delegere til kontrollutvalget å gjøre endringer i planen.

Plan for forvaltningsrevisjon for perioden 2020 - 2024

Kontrollutvalet har i 2020, med god bistand frå Deloitte AS, gjennomført ei slik risiko- og vesentlegvurdering av kommunen si verksemd og av verksemda i kommunen sine selskap.

På bakgrunn av dette er det vidare utarbeidd ein plan for forvaltningsrevisjon som vart handsama i kommunestyret 15.12.2020 der det vart gjort slikt vedtak etter innstilling frå kontrollutvalet:

«Vedtak:
1. Forslag til plan for forvaltningsrevisjon for perioden 2020 – 2024 for Tysnes kommune vert vedteken slik den ligg føre, med endring ved at prioritet nr. 2 vert skyvd over til prioritet nr. 1 og omvendt.
2. Planen erstattar plan for forvaltningsrevisjon for perioden 2016 – 2020.

3. Planen gjeld for resten av valperioden og fram til ny plan etter intensjonen vert vedteken i 2024.
4. Kommunestyret delegerer mynde til kontrollutvalet til å føreta endringar og omprioriteringar i planen, samt til å kunna definera og avgrensa konkrete prosjekt innafor dei utvalde områda i planen
5. Planen skal evaluerast minst ein gong i valperioden. Kommunestyret delegerer mynde til kontrollutvalet til å gjera denne evalueringa.
6. Kontrollutvalet skal rapportere resultatet av forvaltningsrevisjonar til kommunestyret etter kvart.»

I den vedtekne planen er desse prosjekta sett opp i slik prioritert rekkefølge etter at kommunestyret har endra på prioriteringa:

1. Sjukefråvær og personalforvaltning
2. Plan og byggesak
3. Informasjonstryggleik, personvern og GDPR
4. Styring av investeringsprosjekt
5. Barnevern
6. Kontrakt og leverandøroppfølging
7. Internkontroll og kvalitetsarbeid
8. Journalføring og arkivering
9. Innkjøp
10. Opplæringstilbodet til minoritetsspråklege

Rullering av plan for forvaltningsrevisjon for perioden 2020 - 2024

Kontrollutvalet vedtok i møte 13.10.2022 å ikkje gjennomføra rullering av plan for forvaltningsrevisjon for perioden 2020 – 2024.

Plan for forvaltningsrevisjon for perioden 2024-2028

Kontrollutvalet bestilte i møte 23.11.2023 oppstart av ROV for ny planperiode, der forslag til prosjektplan vart handsama. Dette vart mellom anna vedteke:

1. Kontrollutvalet ber Deloitte AS gjennomføre risiko- og vesentlegvurderingar (ROV) av verksemda i Tysnes kommune, verksemda i kommunen sine selskap og av Tysnes kommune sin eigarskap i selskap.
2. Vidare ber kontrollutvalet Deloitte AS utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024 – 2028.
3. Det er ei målsetting at prosessmøte 1 skal gjennomførast i første møte i kontrollutvalet i 2024 og at prosessmøte 2 skal gjennomførast i kontrollutvalet i mai 2024.
4. Det er videre ei målsetting at forslag til plan for forvaltningsrevisjon og plan for

eigarskapskontroll for 2024 – 2028 skal leggast fram for kommunestyret i juni 2024.

6.2 Gjennomførte forvaltningsrevisjonar

Forvaltningsrevisjon av informasjonstryggleik og personvern

Kontrollutvalet bestilte ny forvaltningsrevisjon Informasjonstryggleik og personvern i møte 13.10.2022 og prosjektplanen vart vedteke i møte 24.11.2022.

«Vedtak:

1. Kontrollutvalet ber Deloitte AS gjennomføra forvaltningsrevisjon av informasjons-Tryggleik 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.»

Føremål med denne forvaltningsrevisjonen:

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 tilfredsstiller 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?

Kontrollutvalet handsama revisjonsrapporten i møte 05.10.2023, men grunna at rådmannen og revisjonen var ueinig i ein del fakta slik det kjem fram av rapporten, vart saka utsett til første møte i kontrollutvalet i 2024.

6.3 Tidlegare gjennomførte forvaltningsrevisjonsprosjekt og oppfølging av desse.

Forvaltningsrevisjon av sjukefråvær og personalforvaltning

Kontrollutvalet handsama rapporten i møte 24.02.2022 og innstillinga frå kontrollutvalet vart vedteke av kommunestyret i møte 05.04.2022 (PS 10/2022) utan endingar.

«Kommunestyret ber rådmannen om å:

1. Vurdere å etablere differensierte måltal for sjukefråværet, herunder årlege sjukefråværsmål og mål for den enkelte eining
2. Sørge for at leiarar med ansvar for oppfølging av sjukefråvær jamleg får tilsendt sjukefråværsstatistikk og at statistikken blir brukt på arbeidsplassen
3. Vurdere å utvide registreringa av arbeidsrelatert sjukdom til meir enn arbeidsrelaterte personskadar og godkjent yrkessjukdom, til bruk i det førebyggjande arbeidet
4. Arbeide ytterlegare med å redusere sjukefråvær. Kommunen bør vurdere tiltak eller endringar i tiltak i einingar med høgt sjukefråvær over tid. Tiltaka må tilpassast situasjonen i den enkelte eining, og tilsette bør vere tett involvert i arbeidet for å sikre forankring og målretta tiltak.
5. Sørge for at leiarar får tilstrekkeleg opplæring når det gjeld sjukefråværsarbeid
6. Sørge for at alle medarbeidarar får tilbod om medarbeidarsamtalar
7. Vurdere – saman med verneomboda – om dei har fått tilstrekkeleg opplæring og tid for å kunne utføre vernearbeidet på ein forsvarleg måte, jf. arbeidsmiljølova
8. Sørge for at tiltak etter gjennomførte arbeidsmiljøkartleggingar i tilstrekkeleg grad blir følgt opp/evaluert
9. Etablere ein tilfredsstillande kultur og eit tilfredsstilllande system for å melde og følgje opp avvik
10. Tydeleggjere eller vurdere endringar rundt dokumentasjonskrava for visse typar permisjonar
11. Kommunestyret ber om at det vert gjeve tilbakemelding (handlingsplan) til kontrollutvalet innan 25.april, om korleis vedtaka vert følgt opp, når tilaka vert sett i verk og kven som har ansvar for iverksettinga»

Handlingsplanen vart handsama av kontrollutvalet i møte 12.05.2022. Kontrollutvalet handsama så oppfølging etter denne forvaltningsrevisjonen i møte 09.02 2023, og valde å lukke saka. Kontrollutvalet er ferdig med dette oppfølgingsarbeidet etter denne forvaltningsrevisjonen.

Forvaltningsrevisjon av Plan- og byggesakshandsaming

Kontrollutvalet handsama rapporten i møte 13.10.2022 og innstillinga frå kontrollutvalet vart vedteke av kommunestyret i møte 15.12.2022 (PS 34/2022) utan endringar.

«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 byggjesakshandsaming.
4. 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.
5. 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.
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 byggjesaker
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 byggjesaksavdelinga 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 byggjesaksområdet, 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 har handsama oppfølging etter denne forvaltningsrevisjonen i to møter i 2023. Dette oppfølgingsarbeidet vert vidareført til neste år.

7 Arbeid med eigarskapskontroll

I gamal kommunelov var dette omtala som selskapskontroll som innebar både forvaltningsrevisjon i kommunen sine selskap og kommunen si eigaroppfølging av selskapa.

Etter ny kommunelov er det no slik at forvaltningsrevisjon i kommunen sine selskap skal inngå i plan for forvaltningsrevisjon som er omtala i punkt 6 framanfor.

Kommunelova § 23-2. Kontrollutvalgets ansvar og myndighet punkt d lyd slik:

«Kontrollutvalget skal påse at:

d) det føres kontroll med forvaltningen av kommunens eller fylkeskommunens eierinteresser i selskaper mv. (eierskapskontroll).»

Vidare går det fram av kommunelova § 23-4. Eierskapskontroll dette:

«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.»

7.1 Plan for eigarskapskontroll

Kommunelova § 23-4 Eigarskapskontroll lyd slik:

«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 delegere til kontrollutvalget å gjøre endringer i planen.»

Kontrollutvalet har i 2020, med god bistand frå Deloitte AS, gjennomført ei slik risiko- og vesentlegvurdering av kommunen sin eigarskap i selskap.

På bakgrunn av dette er det vidare utarbeidd ein plan for eigarskapskontroll som vart handsama i kommunestyret 15.12.2020 der det vart gjort slikt vedtak etter innstilling frå kontrollutvalet:

«Vedtak:

1. Forslag til plan for eigarskapskontroll for perioden 2020 – 2024 for Tysnes kommune vert vedteken slik den ligg føre.
2. Planen erstattar plan for selskapskontroll for perioden 2016 – 2020.
3. Planen gjeld for resten av valperioden og fram til ny plan etter intensjonen vert vedteken i 2024.
4. Kommunestyret delegerer mynde til kontrollutvalet til å foreta endringar og omprioriteringar i planen, samt til å kunna definera og avgrensa konkrete prosjekt innanfor dei utvalde områda i planen.
5. Planen skal evaluerast minst ein gong i valperioden. Kommunestyret delegerer mynde til kontrollutvalet å gjera denne evalueringa.
6. Kontrollutvalet skal rapportera resultatet av eigarskapskontrollar til kommunestyret.»

I den vedtekne planen er dette prosjektet sett opp under prioritert prosjekt:

1. Overordna eigarskapsforvaltning i kommunen

Rullering av plan for eigarskapskontroll for perioden 2020 - 2024

Kontrollutvalet vedtok i møte 13.10.2022 å ikkje gjennomføra rullering av plan for eigarskapskontroll for perioden 2020 – 2024.

Plan for eigarskapskontroll for perioden 2024 – 2028

Kontrollutvalet bestilte i møte 23.11.2023 oppstart av ROV for ny planperiode, der forslag til prosjektplan vart handsama. Dette vart mellom anna vedteke:

1. Kontrollutvalet ber Deloitte AS gjennomføre risiko- og vesentlegvurderingar (ROV) av verksemda i Tysnes kommune, verksemda i kommunen sine selskap og av Tysnes kommune sin eigarskap i selskap.
2. Vidare ber kontrollutvalet Deloitte AS utarbeide forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for perioden 2024 – 2028.
3. Det er ei målsetting at prosessmøte 1 skal gjennomførast i første møte i kontrollutvalet i 2024 og at prosessmøte 2 skal gjennomførast i kontrollutvalet i mai 2024.
4. Det er videre ei målsetting at forslag til plan for forvaltningsrevisjon og plan for eigarskapskontroll for 2024 – 2028 skal leggast fram for kommunestyret i juni 2024.

7.2 Gjennomførte eigarskapskontrollar

Det er ikkje gjennomført eigarskapskontroll eller bedriftsbesøk i 2023, i nokon av dei selskap som kommunen har eigarskap i.

8 Arbeid med rekneskapsrevisjon

Kontrollutvalet handsama sak om årsrekneskap og årsmelding i maimøtet, der kontrollutvalet som ein del av saka gjev ein uttale til årsrekneskapen.

Dette vart mellom anna omtalt i saksframlegg og uttale:

Av rekneskapen for 2022 har sekretariatet merka seg eit netto positivt driftsresultat med kr 14.696.555 som utgjer eit netto resultatgrad på 3,96 % (Sett opp mot sum driftsinntekter).

Gjennomsnitt for alle kommunane i Norge ligg ifølge opplysningar fra SSB på netto resultatgrad på 3,0 % i 2022. Teknisk beregningsutvalg for kommunal og fylkeskommunal økonomi (TBU) tilrår at ein over tid bør ha netto resultatgrad på 1,75 % for å ha ei forsvarleg økonomisk drift.

For Tysnes kommune har netto resultatgrad vore slik dei siste 5 åra: 2018 (+ 3,51 %), 2019 (+1,86 %), 2020 (+ 0,48 %), 2021 (3,13 %) og 2022 (3,96%) sjå graf nedanfor. Som vi ser av desse tala har kommunen eit resultat som i 2022 er positivt. Det er sterkare enn tilrådingane frå TBU og litt sterkara enn snittet i kommunane. Netto driftsresultat viser kva ein har igjen etter at alle drifts-utgifter, inklusive renter og avdrag er dekka. Driftsresultatet påverkar i stor grad kommunen sin handlefridom og evne til å tåle svingningar i økonomien.

Riksrevisjonen la 16.02.2015 fram Dokument 3:5 (2014 – 2015) «Riksrevisjonens undersøkelse av kommunenes låneopptak og gjeldsbelastning». Her er det undersøkt samanhengen mellom høg lånegjeld i kommunane, sum driftsinntekter og disposisjonsfond. Riksrevisjonen tilrår at kommunane ikkje bør ha meir enn 75 % av driftsinntektene i lånegjeld. Ved å nytte Riksrevisjonen si tilnærming kjem ein fram til at Tysnes kommune har ei lånegjeld i 2022 tilsvarende 65 % av sum driftsinntekter, altså noko betre enn tilrådinga frå Riksrevisjonen. Tilsvarende tal var 62,5 % i 2020 og 76 % i 2021.Tilsvarande er disposisjonsfondet på 22,78 % av driftsinntektene. Riksrevisjonen tilrår her minst 5%.

Kommunen si gjeldsbelastning finn ein ved å sjå på netto rente og avdragsutgifter i prosent av driftsinntektene. I 2022 finn vi at denne gjeldsbelastninga er på 8,57 %. Sekretariatet er ikkje kjent med om Tysnes kommune har eit eige måltal her, men statsforvaltaren i Nordland meinar dette bør vera under 5%. Men Tysnes kommune har betalt ekstra høgt avdrag for å reusere gjelda og denne kjem derfor innanfor akseptabelt nivå.

Rådmann har lagt fram ei årsmelding som gjev ei god skildring av drifta av kommunen i 2022.

Oppsummering/tilråding frå kontrollutvalet

- Netto driftsresultat er på 3,96 % av driftsinntektene, tilrådinga frå TBU er minst 1,75%
- Gjeldsgrad er berekna til 65 % av driftsinntektene, Riksrevisjonen tilrår maks 75%
- Gjeldsbelastning er berekna til 8,57 % av driftsinntektene. Statsforvaltataren i Nordland tilrår at gjeldsgraden ikkje overstig 5 %. Men Tysnes kommune har derimot betalt ekstra høgt avdrag for å reusere gjelda og denne kjem derfor innanfor akseptabelt nivå.
- Disposisjonsfond er berekna til 22,78 % av driftsinntektene, Riksrevisjonen si tilråding er på minst 5%

9 Forum for Kontroll og Tilsyn (FKT)

FKT er ein landsomfattande organisasjon som har som oppgåve å vera møte- og kompetanseplass for kontrollutvala og deira sekretariat. Kontrollutvalet i Tysnes kommune er medlem i FKT. FKT arrangerar fagkonferansar, samt utarbeidar ulike vegleiarar, bl.a. om «Kva kan ein forvente av oppgåveutføring og kompetanse frå sekretariatet». Nyheitsbrev frå FKT med aktuelle tema for kontrollutvalet sitt arbeid er og lagt fram som meldingar til kontrollutvalet.

10 Opplæring

Det er gjennomført kurs for det nye kontrollutvalet i Roller og rolleavklaring i møte 23.11.23.

11 Kontrollutvalet på kommune si heimeside.

Informasjon om kontrollutvalet på heimesida er lagt til rette på ein god måte, men det er noko manglande informasjon om kontrollutvalet og møta. Dette har og vore diskutert på nokre av møta. Administrasjonen har starta opp eit forbetringsarbeid.

Kommunestyret, alle hovudutval, og også kontrollutvalet brukar lesebrett på møta, og får innkalling til møter elektronisk. For å nytta denne arbeidsmåten i politiske utval er det ein føresetnad at heimesida er godt tilrettelagt og at innkallingar og protokollar vert lagt ut.

12 Tilsyn frå Statsforvaltaren.

Når til dømes Statsforvaltaren gjennomfører tilsyn i kommunane, vert det utarbeida rapport etter tilsynet, som vert sendt til kommunen. I rapportar etter slik gjennomgang av tenesteområde, gjev Statsforvaltaren tilråding, melding eller pålegg til kommunen om kva som bør følgjast opp innanfor saksfeltet. Når påpeikingane er følgd opp og utført på ein tilfredsstillande måte, sender Statsforvaltaren melding om at tilsynssaka er avslutta.

Kontrollutvalet har ikkje handsama tilsynsrapportar i 2023.

13 Andre saker handsama av kontrollutvalet

Døme på andre saker kontrollutvalet har handsama i 2023, lista er ikkje uttømmande:

- Årsmelding 2022 for kontrollutvalet
- Kommunaløkonomisk berekraft i Tysnes kommune
- Konkurranseutsetting av revisjonstenester
- Budsjett 2024 for kontrollutvalet
- Etikk og misleg framferd
- Kontrollutvalet si rolle i varslingssaker

Tysnes 7. mars 2024.

Anne Kristi Alfstad
leiar i kontrollutvalet

Tysnes kommune

Kontrollutvalet
c/o Sekretariat for kontrollutvalet
Vestland fylkeskommune
Postboks 7900, 5020 Bergen

telefon: 05557

e-post: hogne.haktorson@vlfk.no
e-post: roald.breistein@vlfk.no
e-post: kjartan.haugsnes@vlfk.no
e-post: helge.inge.johansen@vlfk.no
e-post: einar.kare.ulla@vlfk.no
e-post: kontrollutvalet@vlfk.no

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2023/479-2
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**4/24**	**07.03.2024**

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 Tysnes 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 i møte 23.11.23, sak PS 33/23, gjort vedtak om at ansvar for gjennomgang av møteprotokollar skal fordelast slik:

Politisk organ:	Kontrollutvalsmedlem:
Kommunestyret	Asbjørn Myklestad
Formannskapet	Lars Heine Kåsa
Tenesteutvalet	Lorentz Lunde
Utval for landbruk og teknisk	Tor Magnus Hauge

Vedtakskompetanse

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

Vurderingar og verknader

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

- Kommunestyret 14.12.2023 og 25.01.2024
- Formannskapet 28.11.2023, 06.12.2023, 10.01.2024, 25.01.2024 og 22.02.2024
- Tenesteutvalet 21.11.2023 og 20.02.2024
- Utval for landbruk og teknisk 05.12.2023 og 23.01.2024

Konklusjon

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

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2024/30-1
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**5/24**	**07.03.2024**

Møteplan 2024 for kontrollutvalet

Forslag til vedtak

Kontrollutvalet vedtek slik møteplan for 2024:
07.03.2024
18.04.2024
15.05.2024
26.09.2024
21.11.2024

Samandrag

I dette møtet skal kontrollutvalet vedta møteplan for 2024. Møta må tilpassast ut i frå om sakene skal vidare til formannskapet og kommunestyret.

Hogne Haktorson
kontrollsjef

Helge Inge Johansen
spesialrådgjevar

Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift

Saksutgreiing

Bakgrunn for saka

Det er praktisk at møtetider i kontrollutvalet er tilpassa saker som eventuelt skal vidare til formannskap og kommunestyre. I utgangspunktet er det planlagt med 5 møter, men kontrollutvalet vel sjølv ut i frå aktivitet kor mange møter ein må ha.

Kommunestyret har vedteke møteplanen for første halvår i 2024. Sekretariatet tilrår at kontrollutvalet vedtek møteplan også for andre halvår.

Vedtakskompetanse

Det er kontrollutvalet som har vedtakskompetanse til å vedta eigen møteplan, jf. Kommunelova § 23-2.

Vurderingar og verknader

Deler av møteplanen for Tysnes kommune for 2024 er lagt inn i tabellen.

Utkast til møteplan for KUV	Aktuelle saker å ta opp:	Aktuelle møter, dersom saker skal vidare til:	
		Formannskapet	Kommunestyret
07.03.2024	Årsmelding 2023 for kontrollutvalet ROV prosessmøte 1 Konkurranse av revisjonstenester – innkomne tilbod		07.05.2024
18.04.2024	ROV prosessmøte 2 Konkurranse revisjonstenester – val av leverandør		07.05.2024
15.05.2024	Uttale til kommunerekneskapen	06.06.2024	20.06.2024
26.09.2024	Budsjett 2025 – for kontrollutvalet		
21.11.2024			

Konklusjon

Kontrollutvalet vedtek møteplanen for 2024 slik den ligg føre.

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2023/478-2
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**6/24**	**07.03.2024**

Eventuelt

Forslag til vedtak

Saka vert lagt fram utan forslag til vedtak.

Samandrag

Det er lagt opp til å ha eventuelt på saklista for å ivareta det enkelte medlem i utvalet sin moglegheit til å sjølv å ta opp saker som ikkje er på sakslista.

Hogne Haktorson
kontrollsjef

Helge Inge Johansen
spesialrådgjevar

Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift

Saksutgreiing

Bakgrunn for saka

Denne saka er å sjå på som ei formalisering av kommunelova § 11-2 siste avsnitt som seier:
«Alle medlemmer kan stille spørsmål til lederen, også om saker som ikke står på sakslisten»

Vedtakskompetanse

Kontrollutvalet har vedtakskompetanse til å handsama sak om eventuelt, 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 er å gje opning for å få nærare utgreiing av saker som kontrollutvalet ynskjer å få utgreidd til neste møte, eventuelt få ei orientering frå rådmannen eller andre i eit seinare møte.

Tysnes kommune

Sekretariat for kontrollutvalet

Saksframlegg

Saksnr: 2023/371-6
Saksbehandlar: Helge Inge Johansen

Saksgang

Utval	Utv.saksnr.	Møtedato
Tysnes kommune, Kontrollutvalet	**7/24**	**07.03.2024**

Konkurranseutsetting av revisjonstenestene for Tysnes kommune

Forslag til vedtak

Kontrollutvalet vurderer evalueringa frå sekretariatet som eit godt grunnlag til vidare arbeid til sak i neste møte.

Samandrag

Føremålet med denne saka er å presentere og drøfte sekretariatet sitt forslag til evaluering av innkomne tilbod på kjøp av revisjonstenester for Tysnes kommune for perioden 01.07.2024 til 30.06.2028.

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.

Kommunestyret gjorde slik vedtak i møte 15.06.2023 etter innstilling frå kontrollutvalet:

1. Kommunestyret gjev 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 omfattar gjennomføring av heile prosessen, herunder:

    - Utarbeiding og godkjenning av tilbodsdokument
    - Knytte til seg naudsynt hjelp.
    - Vurdere mottekne tilbod og innstilla overfor kommunestyret på val av revisor.

Forslag til konkurransegrunnlag vart lagt fram for kontrollutvalet i møte 05.10.2023 der det vart gjort slikt vedtak:

1. Forslag til konkurransegrunnlag vert vedteke.
2. Sekretariatet får fullmakt til å gjera naudsynte redaksjonelle og strukturelle endringar i konkurransegrunnlaget før det vert send ut.

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

Anbodsfristen gjekk ut 26.01.2023 kl. 12.00 for tilbod på kjøp av revisjonstenester for Tysnes kommune for perioden 01.07.2024 til 30.06.2028. Sekretariatet har gjennomgått og evaluert dei innkomne tilboda og førebudd arbeidsmøtet ut frå det. I dette arbeidet har sekretariatet nytta jurist i innkjøpsseksjonen i Vestland fylkeskommune som rådgjevar. Denne juristen rapporterer i denne saka til sekretariatet og ikkje til fylkesdirektør.

Tanken er at vårt forslag til evaluering skal presenterast for kontrollutvalet i dette møtet. På bakgrunn av denne presentasjonen bør utvalet i møtet gjera si eiga vurdering av tilboda. Resultatet av arbeidsmøtet skal vidare danne grunnlag fram mot innstillinga til kommunestyret på val av revisor, som skal handsamast i neste møte i kontrollutvalet.

Konklusjon

Sidan tilboda inneheld informasjon av konkurransemessig betydning for tilbydarane er informasjonen unnateke offentleggjering, jf. offl.13, jf. forvl. § 13. Møtet må difor lukkast med heimel i kommunelova § 11-5 under handsaming av denne saka.

Det vert tilrådd at kontrollutvalet vurderer evalueringa frå sekretariatet som eit godt grunnlag til vidare arbeid til sak i neste møte.

Konto	Konto (T)	BUDSJETT 2024	Endring budsjett i kr	Endring budsjett i %	Rev. Budsjett 2023	Budsjett 2023	Rekneskap 2022	Rev. Budsjett 2022	Budsjett 2022
10800	Godtgjersle folkevalde	43 574	13 840	46,5 %	29 734	29 734	0	24 448	24 448
10990	Arbeidsgjevaravgift	4 619	1 467	46,5 %	3 152	3 152	0	2 592	2 592
11001	Abonnement og faglitteratur	12 000	500	4,3 %	11 500	11 500	425	11 500	11 500
11150	Matvarer/servering	3 000	-	0,0 %	3 000	3 000	4 860	3 000	3 000
11500	Opplæring/ kursutgifter	35 000	20 000	133,3 %	15 000	15 000	2 446	35 000	35 000
11600	skyss- og kostgodtgjering	5 000	-	0,0 %	5 000	5 000	0	5 000	5 000
11955	Kontingentar	4 000	300	8,1 %	3 700	3 700	3 700	3 700	3 700
12700	Konsulentteneste	25 000	-	0,0 %	25 000	25 000	54 164	25 000	25 000
13300	Kjøp frå fylkeskommunen	192 310	27 435	16,6 %	164 875	164 875	136 205	158 725	158 725
13700	Kjøp frå andre, kjøp som erstatter eigenproduksjon	855 529	232 221	37,3 %	623 308	623 308	699 141	583 570	583 570
14290	Betalt mva - momskompensasjon	282 010	70 114	33,1 %	211 896	211 896	164 762	197 759	197 759
17290	Momsrefusjon drift	-282 010	- 70 114	33,1 %	-211 896	-211 896	-164 762	-197 759	-197 759
	Sum	1 180 032	295 763	33,4 %	884 269	884 269	900 940	852 535	852 535

Fra: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]
Sendt: 22.12.2023 09:36:59
Til: Helge Inge Johansen[Helge.Inge.Johansen@vlfk.no]
Tittel: VS: FKT - medlemsinformasjon desember 2023

Fra: Forum for Kontroll og Tilsyn <fkt@fkt.no>
Sendt: onsdag 20. desember 2023 12:31
Til: Forum for Kontroll og Tilsyn <fkt@fkt.no>
Emne: FKT - medlemsinformasjon desember 2023

Til FKTs medlemmer

Se vedlagte brev

Med vennlig hilsen

Anne-Karin Femanger Pettersen
Generalsekretær

Forum for kontroll og tilsyn / Postboks 41 Sentrum, 0101 Oslo / fkt@fkt.no / +47 414 71 166 / www.fkt.no

Hold deg oppdatert med vårt nyhetsbrev

Forum for
kontroll og tilsyn

20. desember 2023

Kjære medlemmer

Nå er tiden her for å reflektere over året som har gått og det som skal komme. Mange av dere er nye i kontrollutvalget og har forhåpentligvis ambisjoner om å gjøre en god jobb der. Forum for kontroll og tilsyn har som nyttårsforsett å bistå dere godt med det.

I høst gjennomførte vi Kontrollutvalgslederskolen del 1 på Teams. Interessen var stor med over 200 påmeldte. Nå er vi godt i gang med å planlegge vårens aktiviteter:

FAGLIGE SAMLINGER FØRSTE HALVÅR 2024

Kontrollutvalsdagane, 23. – 24. januar

Sted: Hotel Alexandra, Loen

Sammen med sekretariatene arrangerer Forum for kontroll og tilsyn og kommunerevisorforbundets lokalforening i Vestland en 2-dagers samling for kontrollutvalgene i Sogn og Fjordane og Søre Sunnmøre. 130 er påmeldt.

Kontrollutvalgslederskolen del 2, 5. – 6. februar

Sted: Clarion Oslo Airport, Gardermoen

Kontrollutvalgslederskolen har som mål å gjøre lederne tryggere i rollen. Skolen gir rom for faglige diskusjoner utover det som kan tilbys i ordinære konferanser. Her er også god anledning for leder til å bygge nettverk med andre ledere rundt om i landet. Til glede for oss er det stor interesse og samlingen er fullbooket. Det er mulig å stå på venteliste for de som er interessert.

Sekretariatskonferansen, 19. - 20. mars

Sted: Quality Airport Hotel, Gardermoen

Vi håper å treffe mange av kontrollutvalgssekretærene på Gardermoen i mars (ikke Lillestrøm der vi vanligvis har brukt å være).

Her kan dere blant annet lære mer om kontrollutvalget sin rolle med å forebygge og avdekke misligheter og hvordan vi kan følge opp en risiko- og vesentlighetsanalyse med andre kontrollhandlinger enn forvaltningsrevisjon og eierskapskontroll.

Andre tema er gode og forsvarlige saksutredninger – kan kunstig intelligens (KI) hjelpe oss? Det vi skriver skal være leservennlig, konkret, forståelig og oppdatert. For å få til det er KI et verktøy – som kanskje utfordrer både faglig forsvarlighet og sikkerhet?

Vi legger opp til gode diskusjoner både i plenum og i grupper. Vi lover et nyttig, konkret, strukturert og interessant opplegg for gruppearbeidet.

Vi sender ut en invitasjon på nyåret, men det er åpent for påmelding allerede nå.

Fagkonferanse og årsmøte, 4. – 5. juni

Sted: Quality Airport Hotel, Gardermoen

Fagkonferansen 2024 tar høyde for at nyvalgte kontrollutvalgsmedlemmer har behov for kunnskap om kontrollutvalgets rolle og samspillet med andre aktører i den kommunale egenkontrollen. Selv om dere har fått opplæring lokalt, har dere sannsynligvis behov for mer faglig påfyll.

Sikkert ikke uventet er tillitt og habilitet et av hovedtemaene for vårens fagkonferanse.

Dere som er nye i kontrollutvalget vil sannsynligvis etter hvert erfare å ta imot henvendelser om mer eller mindre konkrete kritikkverdige forhold. Hvordan skal kontrollutvalget håndtere slike henvendelser? Og hva med varsling – har kontrollutvalget noe med det å gjøre?

Vi sender ut en invitasjon på nyåret, men det er åpent for påmelding allerede nå.

I forbindelse med fagkonferansen, har vi også årsmøte 4. juni. Her kommer vi tilbake mer informasjon.

PROSJEKTER

Forum for kontroll og tilsyn og NKRF – kontroll og revisjon i kommunene samarbeider om et prosjekt om utvikling av veiledere for sekretariatene. Daglig leder Arnar Helgheim, SEKOM-sekretariat og generalsekretær Anne-Karin Femanger Pettersen utgjør i styringsgruppen sammen med NKRFs kontrollutvalgskomite.

Like over nyttår skal styringsgruppen behandle høringssvar på anbefalinger om risiko- og vesentlighetsvurdering, plan for forvaltningsrevisjon og plan for eierskapskontroll. Du kan lese mer om dette her.

5. oktober ble styringsgruppen enige om at de to neste temaene for veiledning skal være hvordan sekretariatet og kontrollutvalget kan planlegge og følge opp orienteringer fra kommunedirektøren og besøk hos avdelinger, tjenestesteder og selskaper.

NYE MEDLEMMER

Etter valget i høst startet vi en rekrutteringskampanje som allerede har gitt gode resultater. I løpet av høsten har vi fått ti nye medlemmer. VELKOMMEN til alle dere som er nye!

Vi håper denne trenden fortsetter i 2024.

STYRET

Dere finner styreprotokollene på medlemssiden (krever pålogging). Send e-post til fkt@fkt.no hvis dere ønsker å få tilsendt brukernavn og passord.

Styrets møtekalender for våren 2024: 5. februar, 18. mars, 24. april og 3. juni.

NYHETSBREV OG MEDLEMSINFORMASJON

Personvernreglene krever samtykke for at vi kan sende ut nyhetsbrev. De som er interessert i nyhetsbrevet «Nytt fra FKT» kan melde seg på her:

Hold deg oppdatert med vårt nyhetsbrev Alle interesserte - også de utenfor organisasjonen - kan abonnere på nyhetsbrevet.

Informasjon som er forbeholdt medlemmer (medlemsbrev) blir sendt ut når vi mener vi har informasjon som bør nå medlemmene. Flere av dere har mottatt dette julebrevet direkte til personlig e-post. Hvis dere ikke ønsker å motta medlemsinformasjon direkte, kan dere gi beskjed til sekretariatet eller til FKT. Da skal vi slette adressen fra medlemslisten.

Følg oss gjerne på facebook og på twitter

Med ønske om en riktig god jul!

Anne-Karin Femanger Pettersen

Generalsekretær

Årsmelding 2022-23
Mobbeombodet i Vestland

Vestland fylkeskommune

Innhald

Forord

Årsmeldinga til mobbeombodet i Vestland er skriven med utgangspunkt i dei førespurnadane vi har fått og arbeid vi har gjort i løpet av barnehage- og skuleåret 2022–2023. Erfaringar og observasjonar frå enkeltsaker og systemarbeid er inkludert. Samtaler med barn, unge, foreldre og tilsette er viktige informasjonskjelder. Årsmeldinga vår er ikkje ein tilstandsrapport om alt som går føre seg i barnehagar og skular i Vestland. Meldinga rommar nyansar og perspektiv som supplerer det eksisterande datagrunnlaget som kommunane og andre barnehage- og skuleeigarar har. Erfaringane våre er først og fremst viktige for å tydeleggjere svakheiter og forbetringspotensial i det vidare arbeidet. Mobbeombodet rapporterer til fylkestinget i Vestland.

Vi takkar alle som har tatt kontakt med oss, og dei vi har samarbeidd med. Vi håpar vi har vore til hjelp i sakene de har tatt kontakt om, og vi tek med oss alle tilbakemeldingar vidare. Vi er også takksame for samarbeidspartnarar som utfordrar oss på arbeidet vårt. Det bidreg til at vi utviklar både rolla vår og tenesta vi leverer.

Vi ber særleg om at ansvarlege politikarar, administrasjon og tilsette i skule og barnehage løftar og bruker årsmeldinga. Les ho, lytt til erfaringane frå elevar, foreldre og tilsette, og kontakt oss gjerne om du vil høyre meir!

Aina Drage og Hildegunn Hodneland, mobbeombod i Vestland

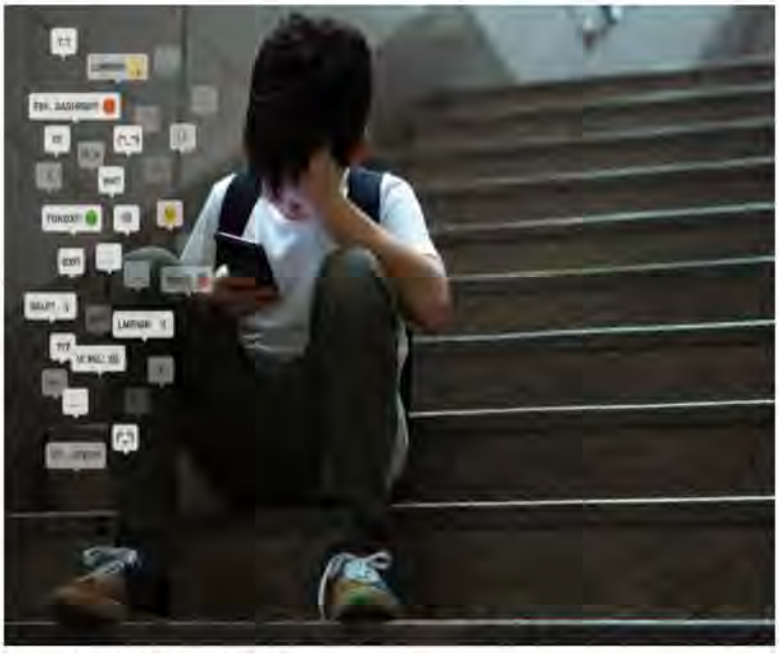


Foto: https://pixabay.com/no/

Samandrag

Gjennom året har vi fått 223 førespurnader. Dei fleste kjem frå føresette til barn i grunnskulen, men også føresette til barnehageborn og tilsette i skule- og barnehage tek kontakt. Vi opplever òg at andre vaksne rundt barnet, som t.d. idrettsleiarar og besteforeldre ynskjer råd og hjelp frå mobbeombodet når dei er uroa for eit barn dei kjenner.

Komplekse saker

Vi høyrer oftast om barn som ikkje har det trygt og godt på skule eller i barnehage når nokon tek kontakt. Vi får innsyn i opplevingar av å ikkje høyre til, og ikkje vere ein del av laget. Vi ser òg korleis det eine påverkar det andre, og at problema ofte er komplekse. I mange av sakene mobbeombodet blir gjort kjende med, vil ikkje eit barn eller ein elev få det betre før heile gruppa og fellesskapet får det betre saman. Det handlar om komplekse sosiale prosessar og negative gruppedynamikkar. Det handlar om systemsvikt – og det handlar om å prøve å løyse dette med for enkle middel.

Gode intensjonar utan god nok kunnskap er ikkje nok. Vi ser at fleire av sakene vi blir bedne om råd i har vart lenge og har blitt for komplekse og vanskelege å løyse for skule/barnehage. Dette kan handle både om at det tek tid før skule/barnehage opplever at aktivitetsplikta er utløyst, og at situasjonen dermed kan ha blitt verre for barnet det handlar om. Dersom skule/barnehage ikkje lyttar til dei som melder frå, manglar kunnskap om trygge miljø, eller ikkje tek styringa i prosessen med aktivitetsplanen for barnet, blir tilliten frå barn og foreldre tynnsliten. Alt dette er faktorar som gjer det vanskelegare å hjelpe barnet.

Informer!

Fleire som tek kontakt med oss fortel at dei ikkje har fått informasjon om rettar i samband med trygt skule- og barnehagemiljø. Difor oppmodar vi skular og barnehagar til å informere slik at informasjonen vert tilgjengeleg for alle aktuelle. Det kan bety å informere på andre måtar, fleire gonger, på fleire språk og fleire stader slik at ingen er i tvil om kva rettar dei har, og kven dei kan kontakte for å få hjelp.

Ingen må bli gløymde

Fleire barn som ikkje har det trygt og godt på skulen utviklar også ufrivillig skulefråvær. Ei følgje av dette er at svært mange av dei heller ikkje får oppfylt retten til opplæring. Her ser vi ein tendens til at elevar som ikkje er på skulen lett kan bli gløymde av skulen, og at tiltak for å trygge blir sett på vent til eleven er tilbake. Vi er òg kjende med saker der elevar som i periodar blir skjerma frå medelevar, ikkje får undervisninga dei skal ha. Å bli gløymt fagleg – og miste relasjonen til lærar – blir då ei ekstra belastning for ein elev som har det vanskeleg sosialt. I tillegg til å miste retten til trygt skulemiljø, mister eleven også retten til undervisning og til å høyre til i ei gruppe.

Når vi samtidig veit at mange kommunar har dårleg økonomi og må kutte i budsjetta til barn og unge, vert vi uroa. Dette er alvorleg. Som mobbeombodet møter vi ofte dei kortsiktige

følgjene, men vi veit at det også får følgjer på lang sikt når barn og unge ikkje får oppfylt rettane til eit trygt miljø og opplæring.

Kunnskap og kapasitet

Mobbeombodet opplever også ein «strekk i laget» blant skuleleiingar når det handlar om kompetanse om sosialt samspel og mobbing. Nokre stader er det vanskeleg å få tak i kvalifisert personale, både på leiarnivå og som lærar/barnehagelærar. Det går ut over både forståinga av forebyggande arbeid og handtering når saker oppstår. På skular og i barnehagar som har mange og krevjande miljøsaker, kan det også ofte bli stort gjennomtrekk av personale, noko som igjen svekker kontinuiteten i arbeidet. I tillegg til kompetanse, handlar det også om å ha nok «folk på dekk». Vi ser til dømes ein auke i barnehagestyrarar som fortel at det no også er vanskeleg å få tak i ufaglært personale.
I den politiske debatten om mobbing og trygt skulemiljø, registrerer vi at det ofte vert løfta fram at fleire miljøarbeidarar kan vere eit godt tiltak. Det støttar sjølvsagt mobbeombodet også, men vi vil understreke at ein enkeltperson aldri kan erstatte god kunnskap om klasseleiing, mobbing, førebygging, undersøking, avdekking og tiltak i alle ledd på skulen, frå skuleeigar til lærar. I tillegg til kunnskap, er det viktig at det også er kapasitet i skule og barnehage til å møte elev og føresette på ein god måte og til å arbeide grundig med sakene.

> Enkeltpersonar i skulen kan ikkje ha eineansvar for å skape trygge miljø. Kompetanse om mobbing, både førebygging og handtering, må finnast i alle ledd i skulesystemet. Frå miljøarbeidarar til skuleeigar. Vi snakker ikkje om «mitt» og «ditt barn», men om «våre barn».
>
> - Mobbeombodet i Vestland

Den viktige vaksenrolla

Vi ser og vi veit også at det blir gjort uendeleg mykje godt arbeid kvar einaste dag på alle skular og i alle barnehagar. Vi ser tilsette som strekk seg langt og har vilje, evne og varme til å sjå kvart einaste barn. Arbeidet med å sikre barn trygge og gode miljø har fleire nivå som vi må evne å sjå: frå individ- og mikronivå, til system-, samfunns- og makronivå. Som vaksne har vi ulike roller, noko det er viktig at vi er medvitne om, sidan rolla vi trer inn i gir ulik posisjon til å påverke. Som forelder, tilsett, barnehage-og skuleeigar, tilsynsmynde og politikar har vi særlege ansvar, eigne plikter og ulike handlingsrom. Det er opp til den enkelte å vurdere korleis ein best nyttar handlingsrommet.

Mobbeombodet held fram arbeid for at barn og elevar skal få tatt i vare rettane sine til trygge og gode barnehage- og skulemiljø. I tillegg til å hjelpe den einskilde som tek kontakt med oss, vil vi òg vere pådrivar for at systema rundt barn og unge blir gode. Vi vil jobbe for at inkludering stadig er ein faktor og eit kjenneteikn, på gode miljø/samfunn. Sist i årsmeldinga kan du lese korleis mobbeombodet i Vestland meir konkret ser på vegen vidare.

Mobbeombodet i Vestland

Kven er vi og kva gjer vi?

Mobbeombodet i Vestland er eit lågterskeltilbod for barn i barnehage og grunnskule, og for deira føresette. Vi skal bidra til at barn og unge får oppfylt rettane sine til trygge og gode barnehage- og skulemiljø. Det inneber at alle kan spørje ombodet om råd i saker som gjeld barnehage- og skulemiljø. Mobbeombodet har teieplikt.

Aina Drage og Hildegunn Hodneland er mobbeombod i Vestland.

I Vestland er vi to mobbeombod; Aina Drage og Hildegunn Hodneland, begge tilsette i 100 % stillingar. Frå august 2022 til januar 2023 var det berre tilsett eitt mobbeombod. Hildegunn Hodneland starta i jobben 4.januar 2023.

Barnekonvensjonen sin art. 3 om vurdering av barnets beste ligg til grunn for alle vurderingane våre.

Mobbeombodet har god kjennskap til lovar og regelverk knytt til barn og unge sine rettar. Vi har lang og relevant utdanning og praksis knytt til felta vi arbeider med. Som ombod er vi uavhengige av politiske og administrative myndigheiter. Saman med elev- og lærlingombodet er vi plasserte i fylkesdirektøren sin stab, i avdeling for organisasjon og økonomi. Vi har kontorstad ved fylkeshusa i Bergen og Førde.

Fylkestinget i Vestland vedtok 10.6.2020 mandatet som mobbeombodet arbeider ut frå. Først og fremst gir vi støtte, råd og rettleiing til foreldre til enkelte barn. Vi samarbeider også med foreldregrupper og tilsette i barnehage og skule, og vi bidreg med faglege innspel til barnehage- og skuleleiing og til lokalpolitikarar i kommunestyre. Vi arbeider med både førebygging, handtering og oppfølging av utrygge miljø og mobbing.

Her kan du kontakte oss:

Telefon: 57 30 03 33

E-post: mobbeombod@vlfk.no

Nettside: vlfk.no/mobbeombodet

Vårt kunnskapsgrunnlag og verdiplattform

Mobbeombodet har ei relasjonell og systemisk tilnærming til mobbing. Det vil seie at vi ser på mobbehandlingar som meir enn berre uønskt åtferd i seg sjølv. Vi arbeider ut frå definisjonar knytt opp til at mobbing handlar om sosiale prosessar på avvege. Der eitt barn ikkje har det bra, er det ofte fleire i same klasse/gruppe som også kjenner på utanforskap eller mobbing. Mobbing skjer i kontekst, og kan til dømes handle om kultur og relasjonar.

Årsakene til åtferd kan også vere samansette, og vi meiner ein må sjå åtferda i samanheng med omgjevnadane til barnet. Samtidig er vi også opptekne av at mobbeåtferd må stoppast. Å involvere dei vaksne rundt barnet er viktig, og vi samarbeider difor også med tilsette i skule og barnehage, der vi mellom anna kan vere med å diskutere og analysere utfordringar med enkeltelevar og i barne-/elevgruppa.

Ein kjent og viktig indikator på skulemiljø er den årlege Elevundersøkinga, som òg er ein del av kunnskapsgrunnlaget i arbeidet for trygge og gode skulemiljø. Undersøkinga kartlegg sentrale sider ved elevane sine læringsmiljø, også mobbing. Når undersøkinga konkret spør om eleven har opplevd mobbing, vert det utdjupa: *Med mobbing meiner vi gjentekne negative handlingar frå ein eller fleire saman, mot ein elev som kan ha vanskeleg for å forsvare seg. Mobbing kan vere å kalle ein annan for stygge ting og erte, halde ein annan utanfor, baksnakke eller slå, dytte og halde fast.*

Denne definisjonen på mobbing er i tråd med Dan Olweus sin definisjon[1] frå 1992, som også er internasjonalt anerkjent. Vi veit på same tid at nyare definisjonar på mobbing veks fram. Ingrid Lund [2] har saman med fleire kollegaer utvikla følgjande definisjon: *«Mobbing av barn og unge er handlingar frå vaksne og/eller barn som hindrar opplevinga av å høyre til, å vere ein betydingsfull person i fellesskapet og moglegheita til medverknad."*

Definisjonen på mobbing kan hjelpe oss til å forstå kva som skjer mellom barn, og til å komme i posisjon til å hjelpe. Uavhengig av definisjon er det samstundes slik at aktivitetsplikta i opplæringslova tek utgangspunkt i **eleven si oppleving** av eige skulemiljø og om eleven har det trygt og godt, uavhengig om mobbing er ein faktor.

Mobbeombodet arbeider heile tida med å oppdatere oss fagleg og har jamleg møte med elev- og lærlingombodet i Vestland. Vi diskuterer aktuelle problemstillingar og reflekterer rundt omgrep og praksis. Vi deltek også på både regionale og nasjonale kompetansehevingar saman med andre mobbeombod i Noreg.

Foto: Vestland fylkeskommune.

---

[1] Den tradisjonelle definisjonen av mobbing er utvikla av forskaren Dan Olweus, som definerer mobbing slik:
"Ein person er mobba eller plaga når han eller ho, gjentatte gonger og over ei viss tid, blir utsett for negative handlingar frå ein eller fleire andre personar."

[2] Helgeland A. & Lund I. (2020) Mobbing i barnehage og skole-nye perspektiver

Mobbeombodet sitt arbeid 2022 – 2023

Kven har fortalt til oss og kva gjer vi med det vi får vite?

Mobbeombodet har mottatt 223 førespurnader som gjeld barnehage- og/eller skulemiljø i Vestland. Generelt ser vi at talet på førespurnader til oss aukar jamt. Gjennom dei tre siste barnehage- og skuleåra har talet på førespurnader auka frå 201 til no 223.

Dei fleste som har tatt kontakt er foreldre med barn som opplever utrygt barnehage- eller skulemiljø. Tilsette i barnehage og skule har òg tatt kontakt, ofte for å få rettleiing eller råd i ei sak. Tabellane under syner korleis førespurnadane fordeler seg på felt/alder, og kven som har tatt kontakt med oss.

Dei fleste, og totalt 192 førespurnader, har kome frå skulefeltet.

Det er færrast førespurnader som gjeld barnehage, totalt 13.

Vi har motteke 18 førespurnader som gjeld situasjonar utanfor barnehage og skule.

Tilsette som har kontakta oss har vore leiarar i skule og barnehage, og lærarar og assistentar i klasse og avdeling.

Med «støttesystem» meiner vi mellom anna PPT, skulehelseteneste, BUP og fritidsleiarar.

«Andre» som har tatt kontakt inkluderer FAU-representant, sambygdingar, slekt og venner av familie.

Vi mottek flest førespurnadar som gjeld mellomtrinn, deretter ungdomstrinn.

For barnhagefeltet er det flest førespurnader som gjeld dei eldste barna.

Ikkje alle fortel kva for trinn meldinga gjeld.

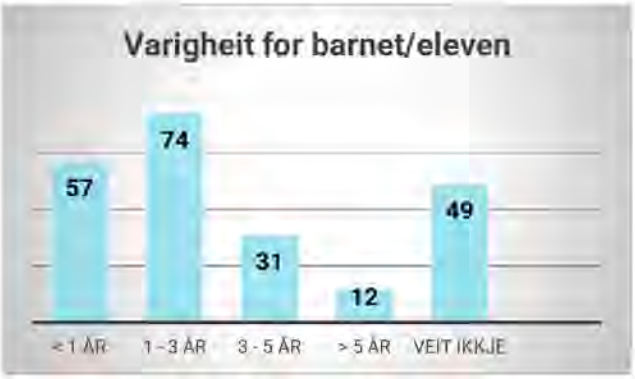
Fordeling mellom kjønn er tilnærma lik, men også her er det ikkje alle som informerer om kjønn.

Etter mandatet vårt skal vi bidra til at barn og unge får teke i vare rettane sine til trygge og gode barnehage- og skulemiljø. I praksis handlar det i stor grad om å gi råd og rettleiing ut frå lovverk og faglege perspektiv, og i tillegg yte emosjonell og sosial støtte.

Når vi vert kontakta av elevar og foreldre, prøver vi difor

1) å lytte og møte den som tek kontakt med oss slik at den kjenner seg forstått og teke på alvor,
2) gjennom fagleg og emosjonell støtte å ruste elev/foreldre til å handtere sin eigen situasjon, vite kva ein kan gjere og kva ein skal kunne forvente av barnehage, skule og eigar, og
3) gi sosial støtte når elev/foreldre har behov for det i møte med barnehage/skule.

Når vi er urolege for ein situasjon/prosess som ikkje fører fram eller for kvaliteten på oppfølginga, seier vi i frå til ansvarlege, som regel styrar, rektor eller barnehage- og skuleeigar. Ofte skjer dette parallelt med at foreldre sjølve seier i frå. For at barn og elevar skal ha det trygt og godt, er det avgjerande at barnehage og skule har god kapasitet til å hjelpe når det først har gått gale, når førebygging likevel ikkje er nok. Mange gonger ønskjer også tilsette råd, nokon å tenke høgt med, for å prøve få auge på det ein sjølv ikkje ser.



Av dei som tek kontakt med oss fortel dei fleste at situasjonen har vart 1 – 3 år. Det høyrer òg med at dei aller fleste av desse allereie har gitt beskjed eller vore i kontakt med barnehagen eller skulen.

Vi merkar oss at om lag 20 % av dei som tek kontakt har opplevd utrygt barnehage-/skulemiljø i meir enn 3 år.

Om lag 22 % har ikkje fortalt noko om varigheit.

Når eit barn ikkje har det trygt og godt, kan barn og føresette bli redde. Frykt for å ikkje høyre til gjer fysisk vondt. Smerter i kroppen kan oppstå og andre symptom som endra matlyst og søvnvanskar kan også vise seg. Over tid høyrer vi om barn som utagerer eller som resignerer. Nokre utviklar angst/depresjon. Vi høyrer òg om barn som uttrykker at dei ikkje vil leve lenger.

Om ein vanskeleg situasjon ikkje vert betre, kjenner vi til at dei fleste barn etter kvart vegrar seg for å vere i barnehagen eller på skulen. Mange mobiliserer og går dit likevel, men etter kvart kan det bli for vanskeleg. Ufrivillig skulefråvær blir dermed ei ny utfordring, og mange av desse mister både retten til å høyre til i ei gruppe og retten til opplæring.

Dessverre er det også slik at barn i norske skular også kan utvikle posttraumatisk stressliding av å stå i utrygge skulemiljø.

Vi meiner det er svært viktig å vere god i å handtere når førebygging ikkje er nok. Som kjent blir ein god på det ein øver på, og når det kjem til handtering av utrygge barnehage- og skulemiljø (vere seg mobbing eller ikkje) – må ein vere god både kollektivt og individuelt.

Å vere synlege for dei vi er sett til å hjelpe

Tidlegare evalueringar av mobbeombodstenesta har vist at ordninga har effekt, men har vore lite kjent.[3] Også dette året har vi jobba for å vere synlege og gjere tenesta betre kjent.

Årleg sender vi ut informasjonsplakatar til aktuelle aktørar i kommunar, med mål om å gjere informasjonen lett tilgjengeleg for barn og foreldre. Vi ser at mange kommunar, skular og barnehagar i Vestland informerer om tenesta på sine nettsider. Vestland fylkeskommune sine tannklinikkar informerer òg om tenesta.

Vi erfarer òg at mange elevar og foreldre ikkje har visst om tenesta vår før saka deira har vart ei stund, og dei etter kvart har fått eit tips om å ta kontakt med oss. Det er viktig at barnehagar, skular og kommunar sikrar seg at informasjonen når ut til barn, elevar og foreldre. Også Mobbeombodet arbeider for å informere på fleire måtar:

a) Gjennom eigen profil på Facebook[4] rettar vi oss mot foreldre og deler aktuell informasjon.
b) I fysiske og digitale besøk i klasserom og på foreldremøte presenterer vi oss sjølve og mobbeombodstenesta.
c) Med jamne mellom skriv vi debattinnlegg og stiller opp til intervju i aktuelle saker i media. Føregåande skuleår har vi bidratt til totalt 9 slike innlegg/intervju fordelt på lokalaviser, regionaviser, lokalradio og TV.

Innlegg og føredrag som gjeld barnehage- og skulemiljø

Mobbeombodet har gjennom skuleåret delteke med 47 innlegg og føredrag i ulike fora.

Ved invitasjon, og med omsyn til kapasitet, har mobbeombodet halde føredrag og innlegg for aktuelle og ansvarlege i barn sine miljø.

Å treffe elevar og foreldre har vore viktig med omsyn til å gjere mobbeombodet kjend.

Foreldremøte i skule og barnehage og klassemøte med elevar har vore viktige treffpunkt for oss. Her har vi snakka både generelt og konkret om tema *trygge fellesskap, å høyre til, sosiale prosessar* og *korleis foreldre kan vere med å bygge gode og trygge miljø*.

[3] Seland, I., I.M. Eriksen, M. Løvgren og M.A. Sletten (2020): Evaluering av ordning med fylkesvise mobbeombud for barnehage og grunnskole. Oslo: NOVA, OsloMet.

[4] https://www.facebook.com/mobbeombod

Vi har òg gjennomført temaøkter og føredrag med tilsette på ulike nivå i barnehage, skule og SFO. Tilbakemeldingar fortel at det er nyttig å sette av tid til å snakke om leik- og læringsmiljø, utryggheit, mobbing, sårbarheit og om kulturen vi skaper. Like viktig har det vore å dvele ved kva som konkret ligg i ansvaret til barnehagen og skulen, og korleis fullt ut oppfylle alle delane av aktivitetsplikta.

Nokre kommunar har invitert mobbeombodet til politiske møte der vi har fått legge fram årsmeldinga vår og fått høve til å snakke om mobbing og utrygge miljø som samfunnsproblem og samfunnsansvar. I desse møta har vi lagt vekt på kva barns opplevingar handlar om, og vi har delt våre tankar om kva som hemmar og fremmar løysing i saker.

Politisk handsaming av årsmeldinga

Årsmeldinga til mobbeombodet gjeld barn i barnehage og elevar i grunnskulen og er aktuell og viktig lesnad for kommunen, politikarar, administrasjon og tilsette i oppvekst. Fylkestinget oppmoda i vedtak 28.09.2022 kommunane om å handsame årsmeldinga vår. På vegne av barn og unge er vi takksame for dei 12 kommunane i Vestland som hausten 2022 følgde oppmodinga og handsama den.

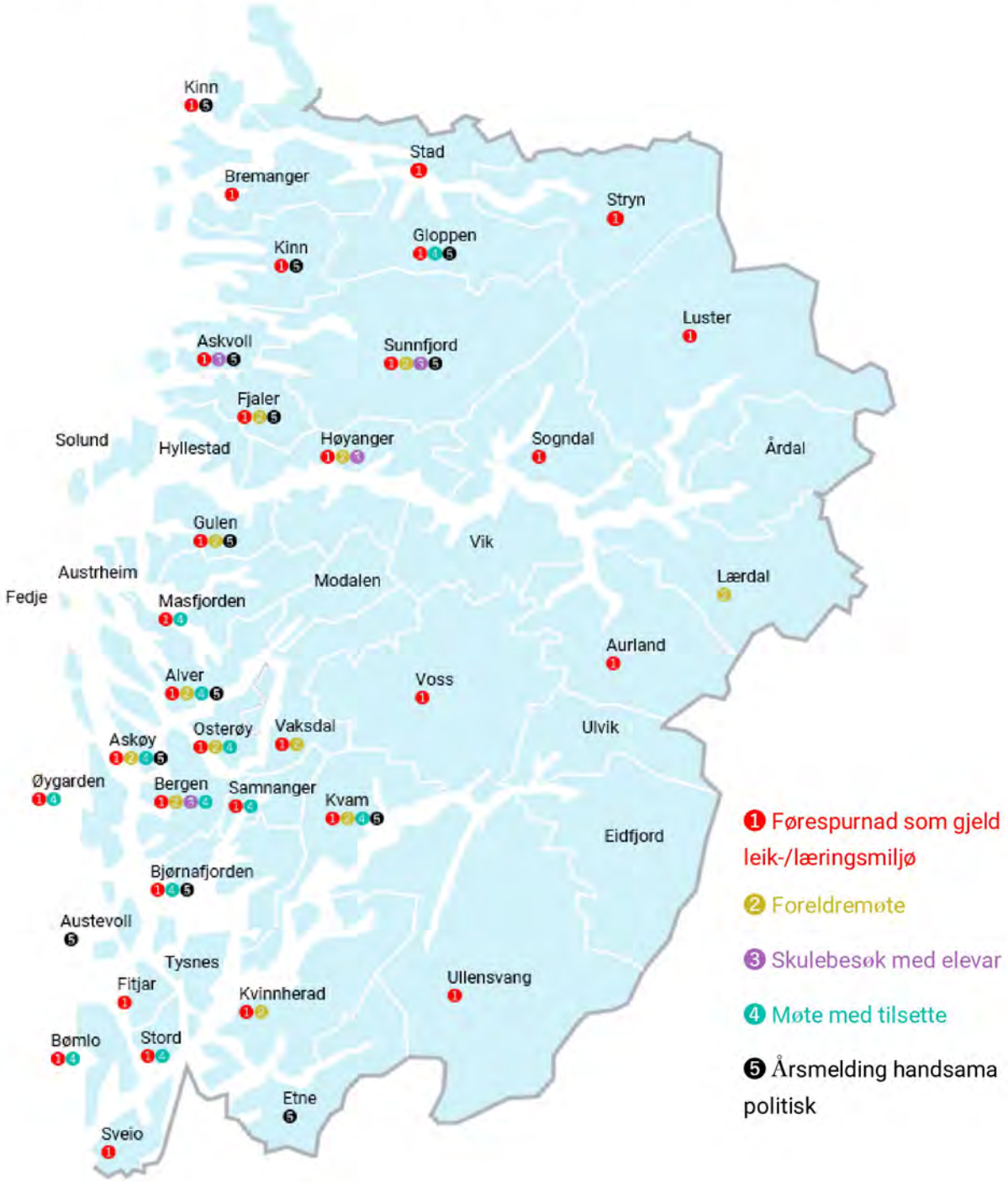
Ved gjennomgang kan vi sjå at årsmeldinga stort sett har vorte handsama som referatsak, altså orientering om vedtak treft av Fylkestinget. *Ein* kommune har handsama årsmeldinga politisk, og denne har vedteke at årsmeldinga frå Mobbeombodet i Vestland skal inngå som eit av fleire kunnskapsgrunnlag som kommunen har i arbeidet mot mobbing i barnehage og skule.

Årsmeldinga er handsama i ulike organ; utval for oppvekst, kommunestyre, kontrollutval, formannskap, rådet for menneske med nedsett funksjonsevne og i ungdomsråd. Seks kommunar har handsama den i fleire enn eitt organ, og sju kommunar har hatt den på saklista i kommunestyret.

foto: https://www.pexels.com/

Engasjementskart

For mobbeomboda er det viktig å vere synlege både for dei vi skal hjelpe og på arenaer der vi kan påverke barn sine leik- og læringsmiljø på konstruktive måtar. Oversikta under syner kva for kommunar vi på ulike måtar har hatt kontakt med dette året. Her kjem òg fram kva for 12 kommunar som har handsama årsmeldinga vår politisk.



Kva skal til for å lukkast med handtering?

Mobbeombodet blir ofte kontakta fordi barn ikkje har det bra i skule eller barnehage. I tillegg har noko svikta i handteringa av saka, og vi får tilgang til informasjon om kva som har gått gale. Skuleåret 2022-2023 ser vi i stor grad dei same problemstillingane i handteringa som tidlegare. Vi meiner det er viktig å trekke desse fram og vise korleis dei påverkar ei sak. Problemstillingane som oftast går igjen er:

- bagatellisering
- skulen/barnehagen tek ikkje (synleg) tak i saka
- manglande kommunikasjon og samarbeid
- krenkande kommunikasjon/sakshandsaming
- tiltak blir ikkje sett i verk, vert ikkje opplevd som treffsikre eller gjer vondt verre
- enkeltbarn blir gjort ansvarlege

Når ein familie opplever alt dette i ei og same sak, kjennest det ofte svært krevjande. Når handtering feilar tidleg i prosessen, pregar det ofte saka vidare. Det krev tid og energi å rette og bygge opp att tillit. For å prøve å vise problemstillingane som går att, og kva som påverkar prosessen, har vi laga ein fiktiv case som vi no presenterer.

Eskil- ein case om handtering av skulemiljøsak

«Eskil» er 11 år og går i 5. klasse. Han har hatt det vanskeleg på skulen i over eitt år. Han har fortalt til kontaktlæraren sin at han ofte kvir seg til å gå på skulen fordi det er mykje uro i klassen, og fordi han ofte blir sitjande aleine i friminutt. Han opplever også kommentarar og blikk frå andre som gjer han meir utrygg, men han vil ikkje at kontaktlærar skal gjere noko. Han er redd for konsekvensar frå medelevar om han fortel lærar kven som seier stygge ting til han. Foreldra til Eskil har tatt sonen sin skulesituasjon opp på utviklingssamtalar. Dei har også sendt e-post til kontaktlærar fordi dei er urolege for einsemda til Eskil og for at han ikkje er trygg på klassekameratane sine. Kontaktlærar seier klassen kan vere litt uroleg av og til, men at ho ofte ser Eskil smile og i samtale med medelevar i timane. Ho seier at det er lett å bli usikker på kva andre meiner med det dei seier når ein ikkje kjenner dei så godt. Ho har ikkje sjølv sett blikka eller oppfatta kommentarane Eskil fortel om.

Kontaktlærar oppfordrar han til å spørje medelevar om å få vere med dei i friminutt, og seier at ho vil lage eit nytt klassekart for at Eskil skal få høve til å bli kjent med fleire elevar i klassen. Ho meiner ho har god oversikt over situasjonen i klassen, og at dette ikkje er noko ein treng å melde vidare til rektor.

Vi oppfattar ikkje Eskil som spesielt utrygg, og sidan vi set inn ekstra ressursar for heile gruppa, ser vi ikkje behovet for ein eigen aktivitetsplan for Eskil no.

-avdelingsleiar

Vi ser at:

- **Barn og foreldre har meldt frå ved fleire høve, ofte over år, utan å oppleve varig endring.**
- **Barn kan også vere redde for represaliar frå medelevar dersom dei seier frå til vaksne.**
- **Tilsette får ikkje med seg og klarer ikkje å sjå det barna fortel om.**
- **Skule/barnehage og barn/foreldre har ulik forståing av det som går føre seg.**
- **I mange av sakene har ikkje barnet fått ein god og klar aktivitetsplan**
- **Ein del tilsette uttrykker at det må handle om mobbing for at aktivitetsplikta skal gjelde.[5] Usikkerheit om lovverk fører til gjentekne lovbrot.**

Krevjande kommunikasjon

Foreldra til Eskil meiner dei får lite informasjon frå skulen, og Eskil seier framleis at han kvir seg til å gå på skulen. Fråværet aukar også, då han ofte blir kvalm og får vondt i magen når han skal på skulen. Over nyttår i 5. klasse sender foreldra ei melding til rektor kor dei viser til kapittel 9A i opplæringslova.

Dei blir kalla inn til møte på skulen nokre dagar etter. I e-posten er det ingen informasjon om kor på skulen møtet skal vere, kva som er agenda for møtet, kor lang tid som er sett av og om kven som skal delta. Foreldra kvir seg allereie. Det å ikkje vere kjent med møteagenda eller deltakarar, er eit ekstra stressmoment i ein allereie krevjande situasjon.

Avdelingsleiar og kontaktlærar deltek på møtet. Eskil er ikkje invitert. Foreldra fortel ein gong til om dei viktigaste hendingane og historikken sidan 4. klasse. Avdelingsleiar seier at han har følgt med Eskil sjølv den siste veka, og sjølv om han ikkje er av dei mest utåtvente i klassen, kan han ikkje sjå at han er spesielt uttrygg. Eskil er også ein del borte frå skulen, så det er vanskeleg å få observert han så ofte som dei skulle ønske, seier avdelingsleiar. Skulen arbeider fortløpande med uroa som er i klassen, og har miljøarbeidar til stades fleire timar i veka. Kontaktlærar seier at dei planlegg å starte aktivitetsgrupper i friminutta etter vinterferien og at dei arbeider med sosial kompetanse heile tida.

Etter møtet ventar foreldra på referat, men dei får ikkje noko tilsendt. Dei er usikre på kva skulen og dei sjølve skal gjere vidare.

Vi høyrer at:

- **Barnet si stemme ofte manglar i møte og i saker som gjeld dei sjølve.**
- **Foreldre må etterspørje informasjon og etterlyse framdrift. I nokre sakar er det foreldra sjølve som sørger for framdrift. Dei kjenner seg som ei byrde for skulen/barnehagen.**

[5] § 9 A-4: Kva skal skulen gjere? https://www.udir.no/regelverkstolkninger/opplaring/Laringsmiljo/skolemiljo-udir-3-2017/6.-hva-skal-skolen-gjore-aktivitetsplikten/

- **Foreldre får lite informasjon om korleis skulen/barnehagen har gjort undersøkingar. Då er det vanskeleg å vere trygg på at det er undersøkt godt nok.**
- **Skular vegrar seg for å setje i verk tiltak for elevar med stort fråvær, og vil vente til eleven er meir på skulen før dei gjer noko.**
- **Uryddig forvaltningsskikk går igjen; Å ikkje få skriftleg innkalling med tilstrekkeleg informasjon i forkant av møte, manglande referat frå møte, at ein ikkje får høve til å godkjenne referat, osb.**

Samarbeid

Foreldra opplever at skulen ikkje tek problema til Eskil på alvor. Samstundes er dei ikkje til stades på skulen og kan sjå korleis Eskil har det saman med medelevane sine. Foreldra likar kontaktlærar, og opplever at samarbeidet med henne fram til no har vore godt. Dei vil ikkje kritisere jobben ho gjer, og Eskil likar henne også. Kanskje blir situasjonen til Eskil verre om dei tek kontakt med skulen fleire gongar, eller klagar på oppfølginga dei har fått til no?

Dei prøver å støtte og oppmuntre Eskil, og få han til å legge meir vekt på positive opplevingar på skulen enn på det som er negativt. Samstundes er dei redde for å bagatellisere forteljingane til Eskil om det som ikkje er bra på skulen. Eskil blir også meir og meir klar på at han ikkje ser nokon vits i å snakke meir med vaksne på skulen om det han opplever. Dei vaksne held fram med å seie at han må prøve å vere meir på skulen enn han er, og at han må vere meir frampå og sjølv ta kontakt med andre når han kjem på skulen.

Eg kvir meg til å kontakte skulen att, eg er så lei av å vere «ho masete mora...».

-mor

Vi ser at:

- **Foreldre er avhengige av eit godt samarbeid med skulen, og at dei fleste redde for å bli sett på som «masete» eller forelderen som «aldri blir nøgd».**
- **Foreldre er i ein sårbar situasjon, saman med barnet sitt. Nokre blir sjukmelde av å følgje opp barnet sitt/kommunisere med skulen i langvarige skulemiljøsaker.**
- **Foreldre kjenner seg pressa til å sjølv ta ansvar og styring når dei opplever at skulen/barnehagen ikkje gjer det. Det er ikkje alltid til barnas beste.**
- **Barn som opplever at dei ikkje blir lytta til eller at det ikkje har nokon effekt å fortelje (sjølv om den vaksne er empatisk og lyttande) vil ofte slutte å fortelje.**

Sakshandsaming og tillit

Det går mot vår i 5. klasse, og Eskil mobiliserer kvar dag for å klare å møte opp på skulen. Fleire gongar i veka klarer han det ikkje, og han opplever ofte negative kommentarar frå andre elevar dei dagane han er på skulen. Han heldt seg mykje på rommet når han er heime, og det blir vanskeleg å få han med på fritidsaktivitetar som han før har likt. Foreldra er uroa for helsa til Eskil, og dei opplever at han ofte er nedstemt og lei seg. Mor sender e-post til

kontaktlærar kvar gong Eskil er borte, og får innimellom svar på e-postane. Ho blir usikker når ho ikkje får svar på e-postar, og når ho får svar, kvir ho seg nokre gonger til å opne dei.

På skulen får Eskil innimellom tilbod om å vere på grupperom når han synest det er vanskeleg å vere inne i klasserommet. Han opplever sjeldan at læraren har tid til å komme inn til han. Nokre gongar sit han aleine og andre gongar får han med seg ein assistent som prøver å hjelpe han med oppgåvene.

Foreldra er uroa for skulen sine rutinar, og er usikker på kompetansen deira når det gjeld arbeid for trygt skulemiljø. «Er det slik at dei ikkje vil sjå, eller klarer dei ikkje å sjå...?» Begge delar gjev grunn til uro og tilliten til skulen vert broten ned. Foreldra ynsker likevel ikkje å melde saka til Statsforvaltaren då dei er redde for at ei slik melding vil ta bort tid og energi dei og skulen treng for å hjelpe Eskil. I tillegg er dei redde for at samarbeidet med skulen skal bli dårlegare. Dei tek kontakt med rektor, og set mobbeombodet i kopi i e-posten. Rektor set i gang undersøkingar etter opplæringslova sin § 9A og læringsmiljøteamet som kommunen har blir kopla på. Undersøkingane viser at det er fleire elevar i klassen, i tillegg til Eskil, som ikkje har det trygt på skulen, og at det finst eit hierarki i klassen der Eskil er nedst.

Vi erfarer at:

- **Det som vert sagt, ord og formuleringar skulen/barnehagen vel å bruke har svært mykje å seie. Orda blir tolka i lys av eigne opplevingar av situasjonen, i lys av relasjonen til tilsette og i lys av tidlegare erfaringar med barnehagen/skulen. «Kva meiner dei med det?» Kva betyr dette?» Foreldre treng å vere trygge på kva barnehage/skule tenkjer, og kjenne at dei vil barnet deira vel.**
- **Born som ikkje opplever å ha det trygt og godt på skulen, får ofte fleire rettar brotne. Det kan t.d. vere retten til undervisning og retten til tilhøyrsle til gruppe/klasse.[6]**
- **Når kommunikasjon og samarbeid i seg sjølve krev energi frå foreldra, blir det ofte ei tilleggsbelastning og tilleggskonflikt til sjølve saka. Det er ikkje til det beste for barnet.**
- **Når tilliten er tynnsliten, krev det god og tett oppfølging for å bygge han opp att.**

Tiltak

Skulen utarbeider ein aktivitetsplan etter undersøkingane. Eskil og foreldra får uttale seg om tiltaka i planen. Det er ikkje sett opp dato for evaluering av planen, men når foreldra ber om det, blir dei kalla inn til møte. Eskil er med på delar av møtet, og seier at det går litt betre.

---

[6] Opplæringslova § 8-2: *Organisering av elevane i klassar eller basisgrupper* I opplæringa skal elevane delast i klassar eller basisgrupper som skal vareta deira behov for sosialt tilhøyr. For delar av opplæringa kan elevane delast i andre grupper etter behov.

Nokre av tiltaka i planen ser ut til å ha effekt. Det er mykje fokus på samarbeid og venskap i klassen, og skulen set opp fleire timar der miljøarbeidar er saman med kontaktlærar i klasserommet. Eitt av tiltaka i planen er at Eskil skal ha samtale med miljøarbeidar ein gong om dagen. Sjølv om han likar å ha ein vaksen som lyttar til han, er det også ubehageleg når dei andre i klassen ser at han ofte går ut av klasserommet saman med ein vaksen.

Andre tiltak som styrte aktivitetar i nokre av friminutta fungerer ikkje alltid. Eskil opplever at dei vaksne som skulle ha ansvar for aktivitetar må steppe inn andre stader, og at han blir ståande aleine slik som før. Han opplever også negative kommentarar frå medelevar som ikkje har lyst til å vere på lag med han i fotball. Nokre av tiltaka blir justerte etter tilbakemelding frå foreldra. Dei er redde for at Eskil byrjar å bli lei av møter og «mas» og at han ikkje lenger seier korleis han har det.

Kvifor skal det heile tida vere opp til guten vår å gi beskjed når noko skjer på skulen? Det burde vere dei vaksne sin jobb å følgje med.

-far

Barn og foreldre fortel:

- **Dei får ikkje bidra i arbeidet med tiltak**[7]
- **Aktivitetsplanar har lite konkrete tiltak. Dei kan også vere utydelege på kven som er ansvarlege, på tidsperiode for tiltak og på dato for evaluering.**
- **Tiltak vert ikkje gjennomførte, har ikkje effekt, eller gjer vondt verre.**
- **Dei opplever ein forventning om at barnet heile tida skal halde dei vaksne underretta om korleis det går, meir enn at dei vaksne sjølv tar dette ansvaret og hentar inn informasjon.**
- **Vaksne grip ikkje inn i krenkingar.**
- **Dei saknar informasjon om kva tiltak som vert sett inn mot andre involverte barn.**[8]

Skulen klarer i løpet av våren i 5. klasse å gjere skulekvardagen trygg for Eskil ved at dei legg til rette for ein føreseieleg skulekvardag med trygge aktivitetar, og ved å stoppe krenkingane han opplever. Dei arbeider framleis aktivt med å bygge opp relasjonar, både mellom elevar i klassen og mellom lærarar og enkeltelevar. Eskil seier at det går betre, og skulen lukker saka før sommaren. Eskil og foreldra tenkjer at det er godt å starte 6. klasse med å legge bak seg alt som har skjedd.

---

[7] Barn og foreldre skal aldri ha ansvaret for å finne tiltak. Det er heller ikkje slik at barn/foreldre kan «bestille» eller krevje tiltak, det skal ligge ei fagleg og pedagogisk vurdering til grunn for tiltaka.

[8] Skule og barnehage har teieplikt om tiltak for andre barn. Likevel kan dei dele noko informasjon. Til dømes kan ein vise til skulen sine rutinar for handtering av krenkingar – at dei «alltid i alle saker følgjer opp slik». Ansvarlege kan be om samtykke til å dele informasjon med andre foreldre. Det er òg mogleg å utarbeidde aktivitetsplanar på gruppenivå, kor ein har tiltak som blir satt inn i heile klassen eller gruppa.

Det er mange som kjenner det slik som Eskil og foreldra hans når dei opplever betring i vanskelege situasjonar dei har stått i lenge. Det har vi stor forståing for, og vi ser ofte at gode forandringar kan vare ved. Likevel vil vi understreke at det er viktig å følgje opp i lang tid etter at eit barn har det trygt og godt. Vi veit også at feriar, overgang til ny klasse, lærarbyte etc. skapar sosiale «vakuum», og tilrår difor at tiltak blir vidareført inn i nytt skuleår, sjølv om eleven opplever å ha det trygt her og no.

Kva med barnehage?

Historia om Eskil går føre seg over nokre år på barneskulen. Mange som tek kontakt med mobbeombodet fortel om at dei har opplevd utrygt skulemiljø i fleire år, at det har eskalert frå tid til anna, og at det heile starta i barnehagen.

Vi møter mange av dei same problemstillingane (t.d. bagatellisering, manglande undersøking, tiltak som ikkje vert gjennomførte eller har effekt) når barnehageforeldre tek kontakt som dei vi har skildra i skule-casen over, men i tillegg spør barnehageforeldre ofte om korleis og til kven ein skal løfte saka når tiltak i barnehagen ikkje fungerer. I motsetnad til opplæringslova, gjennom § 9 A–6, gir ikkje barnehagelova same individuelle klagerett. For barnehagen er det kommunen som er tilsynsmyndigheit og fører tilsyn etter barnehagelova.

Barnehagelova sitt kapittel 8 liknar mykje på kapittel 9A i opplæringslova, og her går det tydeleg fram kva plikter barnehagen har når barn ikkje har eit trygt og godt psykososialt miljø.

Vi ser ei auke i førespurnader, både frå tilsette og føresette i barnehage. Vi er glade for at trygt barnehagemiljø har fått auka fokus, og med meir systematisk arbeid vil vi kunne plukke opp fleire saker og hindre at dei følgjer barna inn i skulen. Oppmodingar frå mobbeombodet

Foto: Pixabay.com

Å lukkast med både førebygging og handtering

Saka om Eskil er fiktiv, men laga på bakgrunn av dei problemstillingane vi oftast høyrer om i førespurnadene vi får frå barn og føresette. Vi ser at det er skilnad på korleis barnehagar og skular handterer saker som gjeld barnehage- og skulemiljø; nokre er trygge medan andre er meir usikre. Frå vår ståstad kan vi i noko grad sjå kva som skal til for å praktisere god handtering. Basert på erfaringane våre gjennom året som har gått, rettar vi følgjande oppmodingar til ansvarlege i barnehage og skule:

System

Barnehage- og skuleleiing og- eigar må:

- **Vurdere** eigen kultur jamleg saman med tilsette. Sjå på både majoritetssamfunnet og skulen/barnehagen sine eigne normer og haldningar.
- Ha **rutinar** for gjennomføring av kartlegging og risikovurdering og for registrering av fråvær og om dette heng saman med barnehage- eller skulemiljø.
- **Invitere foreldre** aktivt til å melde frå om motstand mot skule eller fråvær kan setjast i samanheng med barnehage- eller skulemiljø.

Barnehage og skuleeigar må sørge for:

- **Rettleiing** på alle nivå i ei sak. Sørg for at det finst spisskompetanse i kommunen/organisasjonen som kan tilby dette.
- Ha **system for registrering av fråvær** og om det heng saman med barnehage/skulemiljø.

Informasjon

Barnehageleiing- og eigar:

- **Informer** barn og føresette å ein måte som sikrar at dei får nødvendig informasjon om barna sine rettar i barnehagen. Foreldra må vite *heilt konkret* kor dei skal melde saka vidare til barnehageeigar om dei meiner at barnehagen ikkje har oppfylt aktivitetsplikta.

Barnehagemyndigheit:

- **Informer** om kor og korleis foreldre kan melde inn sak. Informasjonen må vere **lett å finne, lett å forstå og lett å bruke.**
- Foreldre må også få ***informasjon om kva ein kan forvente*** og korleis **prosessen** går føre seg når ein har meldt inn sak.

Kunnskap og kompetanse

- **Tru på barn**. Alle tilsette må ha kompetanse og ressursar til å ta imot barn som fortel at dei ikkje har det bra. Dette inneber å kunne møte barnet og foreldre sine behov – her og no, òg på sikt. Å trygge barnet sine foreldre, bidrar til trygg og god handtering frå alle partar. Det er til barnet sitt beste. Å tru på barn og ta i mot barnet si oppleving er særleg viktig i situasjonar der den tilsette les situasjonen barnet står i på ein annan måte enn barnet sjølv.

- **Godt foreldresamarbeid.**
  Foreldre må bli sett på som ein likeverdig partnar og verdifull bidragsytar. Foreldresamarbeid må vere ein integrert del av barnehagen/skulen sin aktivitet. Leiinga må sørgje for at alle tilsette er klar over kva han/ho skal gjere for å fremme eit godt samarbeid med alle foreldre. Vidare må leiinga sørgje for at ein har strategiar når samarbeidet blir vanskeleg.

- **Kjenn barn sine rettar**. Tilsette som arbeider med barn må ha kunnskap om barn sine rettar og korleis gjere vurdering av *barnets beste*. Tilsette må vidare gjennomføre pliktene sine etter lovverket ovanfor barn. Dei må særleg ha inngåande kompetanse om *aktivitetsplikta,* med delplikter, etter *barnehagelova* og *opplæringslova*. Det gjeld både kva lova betyr, men og kjennskap til eigne lokale retningslinjer.

  Tilsette i barnehage og skule må i alt arbeid utøve *god forvaltningsskikk*, - som til dømes å svare på e-post og førespurnadar, gi god informasjon og rettleiing, og gi moglegheit til medverknad.

- **Forstå**. Alle tilsette i barnehage og skule må ha god kompetanse om *grupper, gruppedynamikk, sosialt samspel* og *felles forståing* av kva krenking og mobbing er. Dei må også ha god kunnskap om korleis *sårbarheit* kan vere ein risikofaktor. Dei må òg kunne gjere *risikovurdering*; kven er dei særleg sårbare barna i år, kva kan vi gjere for å fjerne risiko og auke beskyttelse i miljøet.

  Den tilsette må ha kompetanse og i tillegg anerkjenne at dei ikkje veit alt ein situasjon, og at involverte kan ha svært ulike opplevingar. Avgjerande faktorar for å lukkast med handtering av miljøsaker, er at den som handterer saka er trygg i arbeidet sitt, veit kva lovverket krev, og kva som vert forventa i møte med barn og foreldre. I tillegg må tilsette ha kapasitet til å handtere. Dette må barnehage- og skuleeigar ta ansvar for.

- **Øv.** Vi vert gode på det vi øver på. Skuleeigar og barnehagemyndigheit må legge til rette for at leiarar i barnehage og skule får arbeide med og øve på å løyse saker som omhandlar barn sitt psykososiale miljø i «fredstid». Det same gjeld for leiarar i barnehage- og skule; Bruk planleggingsdagar og fellesmøte til å diskutere og arbeide med aktivitetsplikt og delplikter frå § 9A i opplæringslova og kapittel 8 i barnehagelova. Bruk tid på å analysere tidlegare saker. *Kva fekk vi godt til, og kva kan vi bli betre på til neste gong?*

- **Be om hjelp**. Tilsette må vite når dei kan og bør be om hjelp. Dei må òg ha naudsynt kompetanse tilgjengeleg når dei har behov for hjelp. Spisskompetanse, til dømes gjennom læringsmiljøteam eller kommunale innsatsteam, kan vere eit døme på ein måte å løyse behovet for fagleg hjelp og støtte.

Vegen vidare

Mobbeombodet held fram arbeidet for at barn og elevar skal få tatt i vare rettane sine til trygge og gode barnehage- og skulemiljø. Vi skal også i komande år først og fremst vere eit lågterskeltilbod for barn, elevar og deira foreldre. Det inneber at **vi skal vere synlege, ha rask responstid og tilby fagleg, emosjonell og sosial støtte** i saker som gjeld barn i barnehage og elevar i grunnskulen. Førespurnader som gjeld utrygge barnehage- og skulemiljø har høg prioritet, og vi erfarer stor nytte i å gi støtte til barn og foreldre i slike situasjonar.

Ombodstenesta i Vestland vil vi gjere kjend gjennom ulike oppdrag for foreldre og tilsette i barnehage og skule, og gjennom digitale treffpunkt som informasjon på nett, aktuelle innlegg i sosiale medium og via webinar. Kvart år sender vi også ut informasjon om mobbeombodsordninga til kommunar, barnehagar og skular i Vestland.

I Vestland fylkeskommune sin langsiktige mål- og strategiplan har vi sett oss mål om *å vere pådrivar for å utvikle godt foreldresamarbeid i skule og barnehage, for at barns rettar vert gjort kjende for både dei sjølve og for tilsette, og for at tilsette rundt barn har kompetanse om skule- og barnehagemiljø.* Dette gjer vi kontinuerleg, men har som mål å gjere dette systematiske slik at vi har kontakt med alle kommunar kvart år.

Komande år vil vi ha særleg fokus på

- **Å komme i kontakt og bli kjende med kommunar** vi ikkje har hatt kontakt med tidlegare/føregåande år. Vi vil ta initiativ til å delta på mellom anna foreldremøte, politiske møte og administrasjonsmøte.
- **Å samle ressursteam** i fylket, vere pådrivar for at alle kommunar bygger seg og brukar slik kompetanse til beste for barn i barnehage og elevar i grunnskulen. God og tilgjengeleg kompetanse er ein viktig faktor i å ha kapasitet.
- **Å etterspørje god praksis** på korleis barns rettar vert gjort kjende.

Å lukkast med handtering gir fleire gevinstar ut over det at barn får det trygt og godt att. Mellom anna ser vi at foreldre sin tillit til barnehagen og skulen aukar, og at leiing og tilsette vert tryggare i arbeid med handtering. Å støtte barn, foreldre og tilsette i arbeid med å skape trygge miljø for alle, tenkjer vi er ein viktig del av ansvaret til kommunane.

Vidare vil vi også **halde fram med andre viktige samarbeid som vi har etablert, som med politiske utval og interessegrupper**. Gjennom jamleg kontakt med utval for opplæring og kompetanse, Rådet for menneske med nedsett funksjonsevne og med Elevorganisasjonen får vi aktuelle innspel å ta med vidare.

Saman for trygge og gode barnehage- og skulemiljø!

Kjeldeliste

Barnehagelova, kap. VIII: https://lovdata.no/nav/lov/2005-06-17-64/kapVIII

Breivik, K., Bru, E., Hancock, C., Idsøe, E. C., Idsøe, T., & Solberg, M. E. (2017). *Å bli utsatt for mobbing. En kunnskapsoppsummering om konsekvenser og tiltak*. Henta 01.12.2020 frå https://www.udir.no/tall-og-forskning/finn-forskning/rapporter/a-bli-utsatt-for-mobbing--en-kunnskapsoppsummering-om-konsekvenser-og-tiltak/

Drugli, M.B. & Onsøien, R. (2010) *Vanskelige foreldresamtaler – gode dialoger*. Cappelen Akademisk Forlag.

Elevundersøkinga 2022:
https://www.udir.no/tall-og-forskning/brukerundersokelser/elevundersokelsen/

FNs konvensjon om barns rettigheter:
https://www.regjeringen.no/globalassets/upload/kilde/bfd/bro/2004/0004/ddd/pdfv/178931-fns_barnekonvensjon

Helgeland A. & Lund I. (2020) Mobbing i barnehage og skole-nye perspektiver. Cappelen Damm Akademisk.
Lund, G. E. (2020). Responsivt forældresamarbejde i skolen. *Tema: Forældresamarbejde – en udfordring for læreruddannelsen og et vilkår for skolen. Studier i Læreruddannelse og Profession*. 5(1) (s. 52-72). Henta 01.12.2020, frå https://tidsskrift.dk/SLP/issue/view/8790/1160?fbclid=IwAR0X-VZabvXReLGLC0Bu4oMpH7qUSSowZ3Fzq9513Dlg0MppEsFwctwYxtc

Olweus, D. (1992). *Mobbing i skolen, hva vi vet og hva vi kan gjøre*. Universitetsforlaget

Opplæringslova kap. 9 A: https://lovdata.no/nav/lov/1998-07-17-61/kap9a#:~:text=Alle%20som%20arbeider%20p%C3%A5%20skolen,trakassering%20dersom%20det%20er%20mogleg.

Seland, I., I.M. Eriksen, M. Løvgren og M.A. Sletten (2020): Evaluering av ordning med fylkesvise mobbeombud for barnehage og grunnskole. Oslo: NOVA, OsloMet.

Årsmelding frå mobbeombodet i Vestland 2020-2021:
https://www.vestlandfylke.no/globalassets/utdanning-og-karriere/hjelp/mobbeombud/arsmelding-mobbeombod-2020-2021.pdf

Årsmelding frå mobbeombodet i Vestland 2021-2022:
https://www.vestlandfylke.no/globalassets/utdanning-og-karriere/hjelp/mobbeombud/arsmelding-mobbeombodet--2021-2022.pdf

vestlandfylke.no