

SAKSGANG		
Utval	Møtedato	Saksar
Kontroll- og kvalitetsutvalget	27.01.21	3/21
Kommunestyret	22.03.21	

Saksansvarleg:	Arkivkode:	Arkivsak:
Toril Hallsjø	216	

OPPFØLGING AV FORVALTNINGSREVISJONSRAPPORTEN «PERSONVERN»

Sekretariatet sitt forslag til vedtak og innstilling til kommunestyret:

Karmøy kommunestyre tar rådmannens tilbakemelding om oppfølging av forvaltningsrevisjonsrapport «Personvern» til orientering.

Vedlegg: Rådmannens tilbakemelding, datert 18.01.21 m/ årshjul

Saksorientering

Karmøy kommunestyre behandlet i møtet 25.11.19, sak 122/19 forvaltningsrevisjonsrapport fra KPMG AS, der de fattet følgende enstemmige vedtak:

- 1. Karmøy kommunestyre tar forvaltningsrevisjonsrapporten «Personvern» fra KPMG AS til orientering.***
- 2. Rapporten oversendes rådmannen for videre oppfølging av rapportens anbefalinger.***
- 3. Rådmannen gir tilbakemelding til kommunestyret via kontroll- og kvalitetsutvalget om oppfølging av rapporten innen 12 måneder etter kommunestyrets vedtak.***

KPMGs rapport var vedlagt sak til kontroll- og kvalitetsutvalget og kommunestyret, og ligger på sekretariatets nettsider www.kontrollutvalget.no under Karmøy sine rapporter.

Rådmann har i oversendelse datert 18.01.21, oversendt tilbakemelding om oppfølging av rapportens anbefalinger.

Det gis tilbakemelding til hver av de ni anbefalingene som revisor gav i rapporten. Revisjonens anbefalinger kommer først og så tilbakemeldingen for hver av de ni punktene:

1. Kommunikasjon og opplæring

KPMG:

«Karmøy kommune holder på å implementere et nytt ledelsessystem. Denne prosessen har trolig bidratt til å hemme effektiv kommunikasjon om styrende dokumenter og krav knyttet til blant annet personvern. Det anbefales at kommunens sentraladministrasjon vurderer

hvordan den effektivt kan kommunisere styrende dokumenter og krav ut i virksomheten, og iverksetter nødvendige tiltak for å gjøre viktig personvernrelatert informasjon kjent.

Tilbakemelding:

«Styrende dokumenter og krav kommuniseres ut i organisasjonen gjennom forbedringssystemet Compilo. Alle ansatte har tilgang til disse. Enkelte dokumenter vil i tillegg sendes aktivt ut til de ansatte i forbedringssystemet for gjennomlesning og signering. Forbedringssystemet har en egen leseliste-funksjon som gjør det mulig å sette dokumentene som obligatorisk for gjennomgang, slik at de ansatte får disse på sine leselister og må signere for at de har lest og forstått dem.

I tillegg er det på Karmøy kommunes intranett (Innsiå) opprettet en egen side som omhandler personvern – her vil aktuell informasjon som ligger i forbedringssystemet bli henvist til.»

KPMG:

«Kommunen bør også vurdere å øke omfanget av opplæring i informasjonssikkerhet generelt, og i krav i personopplysningsloven spesielt. Opplæringen bør systematiseres for å sikre at alle medarbeidere får nødvendig opplæring. Det bør blant annet vurderes hvilke kanaler som egner seg for opplæring av ulike typer medarbeidere, eksempelvis ved at medarbeidere som i begrenset grad benytter epost og administrative systemer i hverdagen, tilbys fysisk opplæring i møter eller lignende for å sikre at de får nødvendig informasjon.»

Tilbakemelding:

«Karmøy kommune har gått til anskaffelse av KS læring for å kunne systematisere, følge opp og dokumentere bedre kompetansen i organisasjonen. KS-læring er en digital plattform for kompetanse som er laget av KS og er hovedsakelig for kommunene. Det som gjør KS læring spesiell i forhold til andre plattformer er muligheten for å dele kurs mellom kommuner.

I KS-læring tilbys de ansatte nanokurs innen personvern og informasjonssikkerhet. Kursprogrammet består av totalt 8 moduler i tillegg til 5 filmer. I mange av modulene blir ansatte oppfordret til å ta opp problemstillinger med sine ledere. Alle ansatte skal ikke gjennomføre alle modulene, men gjennomføre de moduler som er relevant i forhold til deres arbeidsoppgaver. Det anbefales også at ledere tilrettelegger for felles gjennomgang av moduler eller filmer i f.eks. avdelingsmøter, men pga smittevern hensyn så er selvfølgelig ikke det mulig nå.

Følgende moduler inngår i kompetansepakken:

- Grunnleggende informasjonssikkerhet - modul 1*
- Sikkerhet på mobile enheter - modul 2*
- Trusler fra IT-kriminelle - modul 3*
- Fysisk sikkerhet - modul 4*
- Grunnleggende personvern - modul 5*
- Utvidet personvern - modul 6*
- Informasjonssikkerhet for ledere - modul 7*
- Håndtering av sikkerhetshendelser - modul 8*

I tillegg inngår 5 filmer:

- *Informasjonssikkerhet for ledere*
- *Informasjonssikkerhet for ansatte*
- *Sikkerhet på mobile enheter*
- *Løsepengevirus*
- *Phishing og falske e-poster*

2. Protokoll over behandlinger og personvernerklæring

KPMG:

«Karmøy kommunes protokoll over behandlinger er mangelfull når det gjelder å konkretisere formålet med den enkelte behandlingen av personopplysninger. Det er behov for en gjennomgang og oppdatering av innholdet i protokollen.

Tilbakemelding:

«Flere av behandlingsaktivitetene i protokollen er gjennomgått og oppdatert. Resterende behandlingsaktiviteter vil bli gjennomgått iht kommunens årshjul for personvernarbeid, se vedlagt årshjul.»

KPMG:

Karmøy kommune bør videre gjennomgå personvernerklæringen, og oppdatere den slik at den tilfredsstiller kravene i personopplysningsloven. Det er særlig behov for å utbedre innholdet i personvernerklæringen når det gjelder en tydeliggjøring av formålet med kommunens behandlinger av personopplysninger, slik at den registrerte gis tilstrekkelig informasjon til å forstå hvilke behandlinger kommunen utfører. Å forstå hvilke behandlinger som utføres, er en forutsetning for å kunne ivareta egne personvernrettigheter.»

Tilbakemelding:

«Karmøy kommunes personvernerklæring er gjennomgått og oppdatert. Revidert versjon ligger på kommunens nettsider og i forbedringssystemet Compilo. Det pågår en dialog med de som leverer den tekniske løsningen hvor de ulike behandlingsaktivitetene blir kartlagt, om å kunne koble disse direkte ut til kommunenes nettside. Dette er fortsatt under utvikling.»

3. Profesjonalisering av kommunens risikostyring

KPMG:

«Det er et potensial for å profesjonalisere kommunens risikostyring, både sentralt og i helse- og omsorgsetaten. Det anbefales at ledelsen legger en plan for å sikre at det er en betryggende risikostyring. Sentrale momenter innen risikostyring omfatter:

- *avklare ledelsens risikoaksept,*
- *gjennomføre en helhetlig risikoanalyse,*

- dokumentere vurderinger,
- prioritere tiltak, tilordne ansvar og fastsette frist for lukking av det enkelte tiltak,
- etablere en rutine for å følge opp lukking av prioriterte tiltak,
- etablere en rutine for å oppdatere risikoanalysen jevnlig, samt ved vesentlige endringer som påvirker gjeldende risikovurderinger.

Planen må videre dokumenteres og innarbeides i virksomhetens årshjul for internkontroll.

Tilbakemelding:

«Profesjonalisering av kommunens risikostyring sees i sammenheng med det pågående arbeidet i kommunen vedrørende kartlegging, analyse og vurdering av risiko knyttet til arbeidsmiljøet.

Kommunens arbeidsmiljøgrupper (bestående av min leder, verneombud og ansattrepresentant på den enkelte arbeidsplass) har og vil delta på samlinger hvor de får opplæring i en metodikk innen risikostyring. Aktuelle prosedyrer og hjelpemidler i dette arbeidet er tilgjengelig i forbedringssystemet Compilo.»

4. Avklaring av personvernombudets rolle og ansvar**KPMG:**

Det anbefales at Karmøy kommune, i samarbeidet med personvernombudet, utdyper ombudets rolle og ansvar, for å sikre at det er en felles oppfatning av hva som inngår i ombudets mandat. I denne forbindelse bør det blant annet klargjøres i hvilket omfang personvernombudet skal utføre kontroller av virksomheten.

Tilbakemelding:

«Personombudets rolle og ansvar er avklart med stabsjef og fremkommer av egen avtale.»

5. Avvikshåndtering**KPMG:**

«Det er behov for å gi medarbeidere i kommunen nødvendig opplæring i rapportering av avvik i Compilo, for å legge til rette for en god rapporteringskultur. Det bør tydelig defineres hva som utgjør et avvik, og hvordan og hvor avvik skal rapporteres. Videre er det behov for å tydeliggjøre rutinen for rapportering av avvik i journalsystemet sett opp mot rutine for rapportering av avvik i det administrative systemet (Compilo), altså hvilke avvik som skal rapporteres hvor, samt om enkelte avvik skal rapporteres begge steder.»

Tilbakemelding:

«Hvordan avvik skal meldes, og til hvem, kommer frem av prosedyre for:

- Melding og håndtering av avvik
- Virksomhetens håndtering av avvik knyttet til samhandling mellom helseforetaket og kommunen.

6. Avklaring av roller og ansvar knyttet til informasjonssikkerhet**KPMG:**

Det anbefales å tydeliggjøre fordeling av roller og ansvar knyttet til informasjonssikkerhet i kommunen, og kommunisere konklusjonen ut i hele virksomheten. Dette kan med fordel gjøres i sammenheng med kommunikasjon av en handlingsplan for å sikre en betryggende praksis på området.

Tilbakemelding:

«Fordeling av roller og ansvar fremkommer av personvernombudets avtale og delegasjonsreglement.»

7. Opplæring og kommunikasjon i helse- og omsorgsetaten**KPMG:**

I Helse- og omsorgsetaten er det, tilsvarende som i kommunen sentralt, et potensial for å systematisere kommunikasjon og opplæringen om informasjonssikkerhet og personvern. Dette for å sikre at alle får nødvendig informasjon, og at det er en enhetlig tilnærming til kommunikasjon om temaet. Anbefalingen bør sees i sammenheng med anbefaling 1.

Tilbakemelding:

«Se svar under anbefaling 1.»

8. Avklaring av roller og ansvar for etterlevelse av krav i personopplysningsloven i helse- og omsorgsetaten**KPMG:**

«Det anbefales at roller og ansvar for etterlevelse av personvernregelverket i etaten tydeliggjøres, for å sikre at det er en enhetlig forståelse, og således redusere risikoen for brudd på regelverket. Det er særlig behov for å vurdere ansvarsfordeling mellom linjeledelsen og GDPR-gruppen i Etaten.»

Tilbakemelding:

«GDPR-gruppen i etatens skal veilede og gi informasjon. Mandatet til gruppen går på å kartlegge og bistå – ikke ift oppfølging. Gruppen jobber overordnet for å sikre/bidra til etatens etterlevelse av lovverket.»

9. Profesjonalisering av helse- og omsorgsetatens risikostyring**KPMG:**

«Det er et potensial for å profesjonalisere etatens risikostyring. Anbefalingen bør sees i sammenheng med anbefaling 3.»

Tilbakemelding:

«Profesjonalisering av etatens risikostyring sees i sammenheng med det pågående arbeidet i kommunen vedrørende kartlegging, analyse og vurdering av risiko knyttet til arbeidsmiljøet. Etatens arbeidsmiljøgrupper (bestående av min leder, verneombud og ansattrepresentant på den enkelte arbeidsplass) har deltatt

på samlinger hvor de har fått opplæring i en metodikk innen risikostyring. Aktuelle prosedyrer og hjelpemidler i dette arbeidet er tilgjengelig i forbedringssystemet Compilo.»

Samlet tilbakemelding:**Sammendrag**

Som nevnt i rådmannens tilbakemelding på rapporten etter forvaltningsrevisjonen ville Karmøy kommune legge vekt på alle anbefalingene i rapporten, men ha et økt fokus på tre sentrale prinsipper som ble trukket frem i rapporten:

- *Kommunikasjon og opplæring*
- *Protokoll over behandlinger*
- *Risikostyring*

Rapporten fremhever behovet for bedre kommunikasjon i kommunen. Dette har vært en kjent utfordring som det har jobbet kontinuerlig med over lengre tid i Karmøy kommune og hvor det fra 1.1.20 ble opprettet en egen kommunikasjonsavdeling som skal støtte opp om dette arbeidet.

Sekretariatets kommentarer

I følge kontrollutvalgsforskriften tilligger det kontrollutvalget å se til at rådmannen følger opp rapporter. Dette skal sikre at kontroll og tilsyn får effekt og bidra til forbedring. Utvalget skal også gi rapport til kommunestyret hvordan merknadene er fulgt opp.

Det ligger ikke til kontrollutvalget å fastsette hvordan administrasjonen skal følge opp påviste avvik/svakheter i det konkrete tilfellet, da dette er rådmannens ansvar. Kontrollutvalget kan rapportere om tidligere saker til kommunestyret, dersom kontrollutvalget mener saker ikke er fulgt opp på en tilfredsstillende måte.

Sekretariatet mener rådmannen i denne saken har gitt en utfyllende tilbakemelding og at de anbefalte tiltakene er det tatt tak i gjennom nye rutiner og prosedyrer.

Det har vært praksis for at administrasjonen møter i utvalget og orienterer om oppfølgingen eller svarer på spørsmål, i tillegg til den skriftlige oversendelsen.

Aksdal, 19.01.21

Toril Hallsjø (sign.)
Daglig leder/utvalgssekretær