



Dato: 18.01.2021
Dokumentnummer: 20/5493-20
Deres referanse:
Saksbehandler: Beathe Andreassen

Karmøy kontroll- og kvalitetsutvalg
v/Haugaland Kontrollutvalgssekretariat lks
Postboks 57
5575 AKSDAL

Oppfølging av forvaltningsrevisjonsrapporten "Personvern"

Det vises til kommunestyrevedtak 25.11.19, sak 122/19:

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.

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.

Tilbakemelding på anbefalinger

Anbefaling 1. Kommunikasjon og opplæring

Det er behov for å 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.

Det anbefales å øke omfanget av opplæring i informasjonssikkerhet generelt og i krav i personopplysningsloven spesielt. Opplæringen bør systematiseres og sikres at alle medarbeidere får nødvendig opplæring.

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.

Protokoll over behandlinger er mangelfull når det gjelder å konkretisere formålet med en enkeltbehandling 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.

Karmøy kommune bør gjennomgår personvernerklæringen og oppdatere denne slik at den tilfredsstille kravene i personopplysningsloven.

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

Det er potensial for å profesjonalisere kommunens risikostyring, både sentralt og i etaten. Det anbefales at ledelsen legger en plan for å sikre at det er en betryggende risikostyring.

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 PVO rolle og ansvar

Det anbefales at Karmøy kommune, i samarbeid med personvernombudet, utdyper ombudets rolle og ansvar, for å sikre felles oppfatning av hva som inngår i ombudet sitt 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

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 er et avvik og hvordan og hvor avvik skal rapporteres.

Behov for å tydeliggjøre rutine for rapportering av avvik i profil sett opp mot 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

Tydeliggjøre fordeling av roller og ansvar knyttet til informasjonssikkerhet – og kommunisere dette ut.

Tilbakemelding:

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

7. Opplæring og kommunikasjon i helse-og omsorgsetaten

Behov for å systematisere kommunikasjon og opplæring av informasjonssikkerhet og personvern. Dette for å sikre at alle får nødvendig informasjon og at det er en enhetlig tilnærming til temaet.

Tilbakemelding:

Se svar under anbefaling 1.

8. Avklaring av roller og ansvar for etterlevelse av krav i personopplysningsloven i Helse- og omsorgsetaten

Tilbakemelding:

GDPR-gruppen i etaten 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 omsorgsetaten risikostyring

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.

Med hilsen

Vibeke Vikse Johnsen
Rådmann

Beathe Andreassen
Kvalitetsrådgiver

Dokumentet er godkjent elektronisk.

Vedlegg 1: Årshjul GDPR

