Grong kommune
Kommunedirektøren

KONSEK TRØNDELAG IKS
Att.Jorunn Sund
Postboks 2564

7735 STEINKJER

Vår ref	Deres ref:	Dato:
2022/392	3353/2023	10.05.2023

Rapport til kontrollutvalget om oppfølging av punkt 4 i vedtak i PS 16/2022

Viser til vedtak i Grong kommunestyre der pkt 4 sier at: *Administrasjonen bes om å sørge for at dokumentasjonen av behandling av personopplysninger og datasikkerhet er i samsvar med lovverket.*

Sikkerhetsansvarlig, personvernombud og kommunedirektør har gjennomgått dokumentasjonen som er tilgjengelig i vårt kvalitetssystem Compilo. I denne gjennomgangen har vi sett på både rutiner og strukturen det er bygd opp rundt.

Etter vår vurdering er det ikke mangel på rutiner, men heller at rutinene er av et slikt omfang, samt inngripende i hverandre, at det trengs en opprydding og forenkling for at systemet skal kunne fungere bedre enn i dag. I tillegg så vi behov for en struktur der internkontroll har hovedfokuset og ulike vurderinger av informasjonssikkerhet og personvern får en mer naturlig del av rapporteringsrutinene.

Det har ligget planer for en slik gjennomgang tidligere, men med pandemien og alle de ekstra oppgaver som kom med pandemien, ble gjennomgangen utsatt. Samtidig må en også bemerke at antall avvik på dette området ikke er i et slikt omfang, at det er her vi har identifisert de største risikoene. Med dette bakteppe ble gjennomgangen utsatt, men er nå tatt opp igjen og jobbet med dette i en god periode.

Tiltak som er gjort, innbefatter:

- Ledelsens gjennomgang med følgende rutiner som ligger til grunn:
  - Ansvarsmatrise og Sikkerhetsorganisasjonen
  - Sikkerhetsstrategi
  - Sikkerhetsmål
  - Akseptabel risiko

Postadresse:
Grong kommune
Postboks 162
7871 GRONG

Sentralbord: 74312100
Saksbehandlers tlf:
91748370

Bankgiro: 4448.06.00050
Organisasjonsnummer: 940010853
Epost:
postmottak@grong.kommune.no
www.grong.kommune.no

        - Akseptert risikonivå på informasjonssikkerhet legges på 9 ved f.eks anskaffelse av nytt programvare eller drift. Ved risiko over 9 må dette godkjennes av kommunaldirektør før investering eller drifta videreføres.

Det ble også benyttet rutinen «Mal for egenkontroll» som verktøy, selv om det er i større grad tiltenkt enheter og avdelinger. Men det ble et verktøy for vurdering av situasjonen og dokumentert i vårt referatsystem for ledermøter.

- Systemendringer foretatt i Compilo.
    - Struktur er gjennomgått og endret og bygd opp i stor grad etter Datatilsynets forslag til struktur for internkontroll - se link: https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/informasjonssikkerhet-internkontroll/etablere-internkontroll/internkontrollens-struktur/
- Gjennomgang av rutiner med revidering av de viktigste
    - Tatt ut og/eller tilpasset rutiner som ligger tett opp mot hverandre
- Lagt plan for videre revidering og tilpasning for resten av året. Dette omfatter blant annet:
    - Revisjon av protokoll for behandlingsaktiviteter (behandlingsoversikt)
        - Behandlingsprotokoll er i dag utarbeidet og revidert. Men en ser at det er behov for en mer strukturell tilpasning, bl.a. om dette kan bakes inn i «orden i eget hus» programvaren.
    - Lage rutine for utarbeiding av protokoll for behandling av personopplysninger
    - Lage sjekkliste ved innkjøp av programvare, applikasjoner. Hva skal en huske på?
    - Gjennomføre et utvidet søk etter databehandleravtaler i historisk og produksjonsbasen, og oppdatere oversikten i Compilo.
    - Lage en rutine med beskrivelse av DPIA, når det gjøres, lagring osv.
    - Skrive inn søkeord for hvert enkelt dokument for senere gjenfinning under Personvern og informasjonssikkerhet.
    - Vurdere bruken av Orden i eget hus opp mot øvrige systemer vi allerede bruker
    - Informasjon til alle leder om nytt system - videre info på ansattnivå.

- Egen fagdag Personvern for PVO og ledere og saksbehandlere ble gjennomført 23.03.2023

For å få dette systemet mer naturlig inn i ordinært årshjul, legges det opp til å implementere dette området i større grad opp mot ny rutine for rapportering og risikovurdering.
Dette startet vi med i 2022 på slutten av året, og første rapport på driftsros ble lagt fram for kommunestyret ved siste møtet her i mai.

Strukturen bli å implementere mer konkret områder som for eksempel informasjonssikkerhet, personvern og HMS i denne prosessen, som vil gå kontinuering opp mot ulike milepæler som er allerede fastsatt.

Prosessen vil utartes slik:
I løpet av året skal alle avdelinger gjennomføre ulike ROS'er på fagnivå. I dette skal også Informasjonssikkerhet og personvern være egen del. Lokale samarbeidsmøter har avvik og behandling av disse som et obligatorisk punkt som skal gjennomgås. Det presiseres i rutinen at informasjonssikkerhet og personvern skal nevnes der spesifikt slik at det minner deltagerne på en slik gjennomgang.

I løpet av første kvartal skal det utarbeides en driftsROS basert på fagROS'er fra avdelingene. Der skal enkelte tema være obligatoriske, slik som informasjonssikkerhet og flere til. Disse opplysningene skal til slutt genereres til en driftsROS for Grong kommune som leveres til kommunestyret ved Budsjettmøte i mai. Dette i hh til økonomireglementet.
Da blir dette innbakt i drøftinger rundt budsjettpremissene for kommende budsjettbehandling. Samtidig kan resultatet kreve at det iverksettes mer øyeblikkelige tiltak som kan løses innenfor ordinære driftsrammer.

Andre tiltak bakes inn i egne kapitler for budsjett og handlingsplan for kommende budsjettår, og vil derav også forankres politisk.

Dette danner igjen grunnlag for tertialrapportering som da skal rapportere ut på valgte områder. For å sikre fokus på dette med informasjonssikkerhet, skal personvernombudet ha sitt eget avsnitt i tertialrapportene. Disse tapportene vil da være grunnlag for årsmelding, der årsmeldingen er oppbygd rundt samme mal som tertialrapportene. Så vil samme syklus gjentas, slik at vi får en kontinuerlig prosess rundt dette i større grad.

Med dette mener kommunedirektøren at vi har tatt revisjonens innspill til etterretning, og iverksatt konkrete tiltak for å sikre både prosesser og handlinger i henhold til rutinene. Personvernombudet vil stille til møtet i kontrollutvalget, og gi en uavhengig vurdering av tiltak.

Med hilsen

Bjørn Ståle Aalberg
kommunedirektør

Dokumentet er elektronisk godkjent og har derfor ingen underskrift

Intern kopimottakere:
Tore Kirkedam KOMMDIR - Kommunedirektøren