Vestland fylkeskommune

Sekretariat for kontrollutvalet
Saksframlegg

Saksnr: 2020/48610-11
Saksbehandlar: Roald Breistein

Saksgang

Utval	Utv.saksnr.	Møtedato
Kontrollutvalet		
Fylkestinget		15.12.2020

Forvaltningsrevisjon innan informasjonstryggleik - Revisjonsrapport

Forslag til innstilling

På bakgrunn av gjennomført forvaltningsrevisjon innan informasjonstryggleik ber fylkestinget fylkesrådmannen syta for at det vert sett i verk tiltak for å sikre følgjande:

1. at fylkeskommunen sitt styringssystem blir gjort ferdig og implementert i organisasjonen, og som del av dette sikre at:
   a) ansvarsforhold knytt til informasjonstryggleik blir gjort kjend og etterlevd av dei tilsette
   b) rutinar for informasjonstryggleik blir gjort ferdige, kjende og blir etterlevd av dei tilsette
   c) det blir gjennomført tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken

2. at ansvar og rutinar for å hindre uautorisert innsyn i konfidensielle opplysningar er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for at tilsette:
   a) praktiserer trygg bruk av e-post, t.d. gjennom nettfiskeforsøk
   b) nyttar sikker sone ved lagring av konfidensielle opplysningar
   c) krypterer konfidensielle opplysningar som ikkje er lagra i sikker sone

3. at ansvar og rutinar for å hindre uautorisert tilgang til informasjonssystema er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for å:
   a) sikre at tilsette har nødvendige tilgangar
   b) sikre at tilsette ikkje har tilgangar utan at det er tenestleg behov

4. at krava i personvernforordninga blir etterlevde, og som del av dette:
   a) føre protokoll over alle behandlingar av personopplysningar
   b) signere databehandlaravtalar med alle kommunen sine databehandlarar
   c) gjennomføre risikovurderingar knytt til behandlingar av personopplysningar
   d) gjennomføre vurdering av personvernkonsekvensar ved behandlingar av personopplysningar med høg risiko

5. at systemeigarar og andre med ansvar knytt til informasjonstryggleik og personvern mottek tilstrekkeleg opplæring

6. at det blir utarbeidd tilstrekkeleg med informasjon om informasjonstryggleik til dei tilsette, og sikre at dei tilsette får den naudsynte opplæringa for å kunne ivareta informasjonstryggleiken på ein tilfredsstillande måte

7. Fylkestinget ber også om at fylkesrådmannen lagar ein prioritert handlingsplan til kontrollutvalet innan 01.03.2021 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.

Samandrag

Deloitte har no gjort ferdig forvaltningsrevisjon innan informasjonstryggleik og revisjonsrapport er levert. Føremålet med denne saka er at kontrollutvalet skal handsame rapporten og vedta innstilling til fylkestinget som gjer endeleg vedtak i saka.

Hogne Haktorson
kontrollsjef

Roald Breistein
seniorrådjevar

Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift

Vedlegg
1 Forvaltningsrevisjon av informasjonstryggleik - Vestland fylkeskommune

Saksutgreiing

Bakgrunn for saka

Kontrollutvalet i Vestland fylkeskommune vedtok i møte 11.05.2020 å be Deloitte gjennomføre forvaltningsrevisjon innan informasjonstryggleik. Av den godkjende prosjektplanen går det fram at forvaltningsrevisjon innan informasjonstryggleik har slikt føremål:

«Føremålet med prosjektet har vore å undersøkje om fylkeskommunen har tilfredsstillande system og rutinar for informasjonstryggleik, og om etablerte standardar og gjeldande lovar og reglar blir følgt innanfor dette området. Det har òg vore eit føremål å undersøkje korleis fylkeskommunen praktiserer informasjonstryggleik med omsyn til konfidensialitet og tilgangsstyring, i kva grad fylkeskommunen etterlever sentrale krav i ny personvernlovgjeving, og kva kompetanse dei tilsette har på området.»

Med bakgrunn i føremålet er det utarbeidd følgjande problemstillingar som vil bli undersøkt:

1. ***I kva grad har Vestland fylkeskommune 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 fylkeskommunen system for kontroll og etterprøving av informasjonstryggleik, og blir slik kontroll og etterprøving gjennomført?*

2. ***I kva grad har Vestland fylkeskommune etablert rutinar for sikring av konfidensialitet, og i kva grad blir disse etterlevd?***
    Under dette:
    a) *Hindre uautorisert innsyn i konfidensielle opplysningar*
    b) *Sikker sone for lagring av konfidensielle opplysningar*
    c) *Kryptering av konfidensielle opplysningar*

3. ***I kva grad har Vestland fylkeskommune etablert rutinar for tilgangsstyring, og i kva grad blir disse etterlevd?***
    Under dette:
    a) *Hindre uautorisert tilgang til informasjonssystema*
    b) *Inn- og utmelding av tilsette i relevante informasjonssystema*
    c) *Vurdering av om tilsette har riktige tilgangar i informasjonssystema*
    d) *Loggføring av brukte tilgangar i informasjonssystema*

4. ***I kva grad etterlever Vestland fylkeskommune sentrale krav i personvernlovgjevinga?***
    a) *Har fylkeskommunen eit personvernombod med tilhøyrande ansvar og oppgåver som tilfredsstillar krava regelverket?*
    b) *Fører fylkeskommunen protokoll over behandlingsaktivitetar av personopplysningar i samsvar med krava i regelverket?*
    c) *Har fylkeskommunen personvernerklæring som følgjer krava i regelverket?*
    d) *I kva grad blir det gjort risiko- og konsekvensvurderingar av handsaming av personopplysningar der det er krav om dette?*
    e) *I kva grad har fylkeskommunen oversikt over avvik knytt til personvern, og i kva grad blir slike avvik meldt til Datatilsynet?*

5. ***I kva grad har dei tilsette i fylkeskommunen tilstrekkeleg kompetanse om informasjonstryggleik?***
    a) *Er det etablert rutinar for å gje tilsette opplæring i informasjonstryggleik?*
    b) *I kva grad har dei tilsette kjennskap til ev. retningsliner og rutinar for informasjonstryggleik?*
    c) *I kva grad blir ev. retningsliner og rutinar for informasjonstryggleik følgt?*

Av rapporten går det fram at Deloitte har gjort slik avgrensing i arbeidet

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 fylkeskommunen og personane som blir råka. Revisjonen har ikkje gjennomført undersøkingar, testingar eller analysar av teknisk konfigurasjon, tryggingstiltak eller operative driftsrutinar.

Vedtakskompetanse

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

Vurderingar og verknader

Deloitte har no gjort ferdig forvaltningsrevisjon innan informasjonstryggleik, revisjonsrapport er levert og ligg ved. Rapporten har vore send til uttale til fylkesrådmannen og uttalen går fram av vedlegg 1 i rapporten.

Deloitte har i denne forvaltningsrevisjonen nytta dokumentanalyse, intervju, spørjeundersøking og verifiseringsprosessar som metodar. Etter sekretariatet si vurdering har Deloitte levert ein særs god rapport som er i samsvar med kontrollutvalet si bestilling. Sekretariatet har vidare merka seg at rapporten peikar på tildels store utfordringar når det gjeld informasjonstryggleik i Vestland fylkeskommune.

Det går fram av punkt 8 i rapporten at Deloitte tilrår at Vestland fylkeskommune sett i verk tiltak for å sikre følgjande:

1. *at fylkeskommunen sitt styringssystem blir gjort ferdig og implementert i organisasjonen, og som del av dette sikre at:*
   a) *ansvarsforhold knytt til informasjonstryggleik blir gjort kjend og etterlevd av dei tilsette*
   b) *rutinar for informasjonstryggleik blir gjort ferdige, kjende og blir etterlevd av dei tilsette*
   c) *det blir gjennomført tilstrekkeleg kontroll og etterprøving av informasjonstryggleiken*

2. *at ansvar og rutinar for å hindre uautorisert innsyn i konfidensielle opplysningar er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for at tilsette:*
   a) *praktiserer trygg bruk av e-post, t.d. gjennom nettfiskeforsøk*
   b) *nyttar sikker sone ved lagring av konfidensielle opplysningar*
   c) *krypterer konfidensielle opplysningar som ikkje er lagra i sikker sone*

3. *at ansvar og rutinar for å hindre uautorisert tilgang til informasjonssystema er utfyllande, tydelege og blir etterlevd, og som del av dette gjer tiltak for å:*
   a) *sikre at tilsette har nødvendige tilgangar*
   b) *sikre at tilsette ikkje har tilgangar utan at det er tenestleg behov*

4. *at krava i personvernforordninga blir etterlevde, og som del av dette:*
   a) *føre protokoll over alle behandlingar av personopplysningar*
   b) *signere databehandlaravtalar med alle kommunen sine databehandlarar*
   c) *gjennomføre risikovurderingar knytt til behandlingar av personopplysningar*
   d) *gjennomføre vurdering av personvernkonsekvensar ved behandlingar av personopplysningar med høg risiko*

5. *at systemeigarar og andre med ansvar knytt til informasjonstryggleik og personvern mottek tilstrekkeleg opplæring*

6. *at det blir utarbeidd tilstrekkeleg med informasjon om informasjonstryggleik til dei tilsette, og sikre at dei tilsette får den naudsynte opplæringa for å kunne ivareta informasjonstryggleiken på ein tilfredsstillande måte.*

Konklusjon

Kontrollutvalet har eit særskilt ansvar for å følgje opp at fylkestinget sine vedtak i samband med handsaming av revisjonsrapportar vert følgd opp. Det vert vist til Kommunelova § 23-2, e) der det står dette:

«kontrollutvalget skal påse at

e) vedtak som kommunestyret eller fylkestinget treffer ved behandling av revisjonsrapporter, blir fulgt opp.»

Forslag til innstilling i saksframlegget, byggjer på forslag til tiltak i rapporten. Det vert dessutan tilrådd at fylkesrådmannen vert beden om å lage ein prioritert handlingsplan til kontrollutvalet innan 01.03.2021 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.