Vestland fylkeskommune

Sekretariat for kontrollutvalet
Saksframlegg

Saknr: 2020/48610-2
Saksbehandlar: Roald Breistein

Saksgang

Utval	Utv.saksnr.	Møtedato
Kontrollutvalet		

Forvaltningsrevisjon innan informasjonstryggleik - Forslag til prosjektplan

Forslag til vedtak

1. Kontrollutvalet bestiller forvaltningsrevisjon innan informasjonstryggleik frå Deloitte AS, med utgangspunkt i forslag til prosjektplan og ev. innspel under drøftinga i møtet.
2. Ev. ny korrigert prosjektplan vert å sende sekretariatet innan 25.05.2020.
3. Det vert akseptert ein samla timeressurs på inntil det timetal som ligg i forslag til prosjektplan.
4. Det vert også akseptert opsjon på ev. presentasjon av rapporten i Vestland fylkesting fakturert etter timeforbruk, inntil 6 timar.
5. Kontrollutvalet ønskjer at revisjonsrapport er klar frå Deloitte si side innan 11.11.2020, ferdig verifisert og med fylkesrådmannen sin uttale vedlagt og/eller innarbeidd, slik at den kan handsamast i kontrollutvalet 25.11.2020 og i fylkestinget 15.12.2020.

Samandrag

Føremålet med denne saka er at kontrollutvalet skal ta stilling til vedlagte forslag til prosjektplan frå Deloitte på kva forvaltningsrevisjonen innan informasjonstryggleik bør innehalde og korleis dei har tenkt å gjennomføre arbeidet.

Hogne Haktorson
Kontrollsjef

Roald Breistein
seniorrådjevar

Saksframlegget er godkjent elektronisk og har difor ingen handskriven underskrift

Vedlegg
1 Prosjektplan - forvaltningsrevisjon av informasjonstryggleik i VLFK

Saksutgreiing

Bakgrunn for saka

Kontrollutvalet handsama sak PS 35/20 Bestilling av forvaltningsrevisjon i møte 21.04.2020 og dette vart protokollert:

«Handsaming i møte
Det vart semje om at det er ønskjeleg å bestille to forvaltningsrevisjonar no.

I diskusjonen vart desse områda spelt inn som aktuelle for forvaltningsrevisjon:

- *Iril Schau Johansen – Tannhelse*
- *Klaus Iversen – Havbruk og fiskeri*
- *Renate Møgster Klepsvik – Informasjonstryggleik og internkontroll*

Etter felles diskusjon kom kontrollutvalet fram til at ein ønskjer å gjennomføre forvaltningsrevisjon innan Tannhelse og Informasjonstryggleik.

På bakgrunn av dette kom kontrollutvalet med slike problemstillingar/moment til kvart av områda:

Tannhelse:
- *Får dei som har rett på gratis tannhelseteneste det tilbodet dei skal ha?*
- *Vert frister for innkalling halde?*
- *Blir inntektssikring ivareteke?*

Informasjonstryggleik:
- *Styringssystem*
- *System og rutinar*
- *Oversikt over personopplysningar*
- *Datasikkerhet*
- *Nettfiskeforsøk*
- *Lagring av sensitive opplysningar*
- *GDPR*

Forslag til prosjektplanar vert å levere sekretraiatet innan 29.04.2020.

Med denne endringa i punkt 3 vart slikt vedtak samrøystes vedteke.

Vedtak
1. *Kontrollutvalet ønskjer at det vert gjennomført forvaltningsrevisjon innan Tannhelse og Informasjonstryggleik.*
2. *Deloitte vert beden om å levere forslag til prosjektplanar i tråd med dei føringar utvalet har gjeve, inkl. føremål, problemstillingar, ev. avgrensingar, ressursbruk og leveringstidspunkt.*
3. *Forslag til prosjektplanar bes levert sekretariatet seinast innan 29.04.2020.*
4. *Prosjektplanane skal leggjast fram til godkjenning i neste møte i kontrollutvalet.»*

Vedtakskompetanse

Kontrollutvalet har mynde til å gjennomføre forvaltningsrevisjonar medan det er fylkestinget som har mynde til å vedta revisjonsrapporten, jf. kommunelova § 23-3 og § 23-5.

Vurderingar og verknader

Med utgangspunkt i det som går fram over har Deloitte levert forslag til prosjektplan for forvaltningsrevisjon innan informasjonstryggleik. Prosjektplanen følgjer som vedlegg.

Av den føreslåtte prosjektplanen går det fram at føremålet med forvaltningsrevisjonen er:

«Føremålet med prosjektet er 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 er òg eit føremål å undersøkje korleis fylkeskommunen praktiserer informasjonstryggleik med omsyn til konfidensialitet og tilgangsstyring, å undersøkje i kva grad fylkeskommunen etterlever sentrale krav i ny personvernlovgjeving, samt å undersøkje dei tilsette sin kompetanse på området.»

Med bakgrunn i prosjektet sitt føremål har revisjonen formulert følgjande problemstillingar:

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?*

Deloitte har definert slik avgrensing

«I undersøkingane av informasjonstryggleik vil revisjonen primært fokusere 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. Ein gjennomgang av rutinar på dette området vil likevel også kunne omfatte rutinar knytt til andre sensitive eller fortrulege opplysningar.

Revisjonen vil ikkje gjennomføre undersøkingar, testingar eller analysar av teknisk konfigurasjon, tryggingstiltak eller operative driftsrutinar.»

I dette revisjonsprosjektet vil Deloitte m.a. nytta dokumentanalyse, intervju, spørjeundersøking, nettfiskeforsøk og verifisering og høyring som metode. Revisjonen ønskjer å gjennomføre 5-7 intervju med utvalde personar frå Vestland fylkeskommune som er involvert i eller har ansvar for informasjonstryggleik i ulike delar av organisasjonen.

Med utgangspunkt i det omfang som ligg i den føreslåtte prosjektplanen meiner sekretariatet at det kan forsvarast å bruke inntil det timetal som er føreslått. Sekretariatet registrerer at det går fram av prosjektplanen at ferdig revisjonsrapport kan leverast til 30.11.2020. Det vil vera ei føremon om revisjonsrapporten kan vera klar til handsaming i møte i kontrollutvalet 25.11.2020 slik at den kan handsamast i fylkestinget 15.12.2020.

Konklusjon

Sekretariatet meiner at prosjektplanen er godt gjennomarbeidd og i tråd med dei føringar som ligg i bestillinga frå kontrollutvalet. Føremål og problemstillingar synest også å vera i tråd med dette. Når det gjeld timetalet vil sekretariatet tilrå at det vert godkjend inntil det timetal som går fram av prosjektplanen. Vidare bør det aksepterast opsjon på ev. presentasjon av revisjonsrapporten for Vestland fylkesting fakturert etter timeforbruk, inntil 6 timar. Vidare bør kontrollutvalet utfordre Deloitte på om dei kan levere revisjonsrapporten slik at den kan handsamast i møte i kontrollutvalet 25.11.2020 og i fylkestinget 15.12.2020.