Vestland fylkeskommune

Sekretariat for kontrollutvalet
Saksframlegg

Saksnr: 2020/48610-6
Saksbehandlar: Roald Breistein

Saksgang

Utval	Utv.saksnr.	Møtedato
Kontrollutvalet		

Forvaltningsrevisjon innan informasjonstryggleik - Status i arbeidet ved Deloitte

Forslag til vedtak

Kontrollutvalet tek informasjonen til orientering.

Samandrag

Føremålet med denne saka er at Deloitte skal gjera greie for status i arbeidet med den pågåande forvaltningsrevisjonen innan informasjonstryggleik.

Hogne Haktorson
kontrollsjef

Roald Breistein
seniorrådjevar

Saksframlegget er godkjent elektronisk og har difor inga handskriven underskrift

Saksutgreiing

Bakgrunn for saka

I møte i kontrollutvalet i Vestland fylkeskommune 11.05.2020 vart det gjort slikt vedtak:

1. *Kontrollutvalet bestiller forvaltningsrevisjon innan informasjonstryggleik frå Deloitte AS, med utgangspunkt i forslag til prosjektplan og ev. innspel under drøftinga i møtet.*
2. *Det vert akseptert ein samla timeressurs på inntil det timetal som ligg i forslag til prosjektplan.*
3. *Det vert også akseptert opsjon på ev. presentasjon av rapporten i Vestland fylkesting fakturert etter timeforbruk, inntil 6 timar.*
4. *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.*

I den godkjende prosjektplan går det fram at forvaltningsrevisjon innan informasjonstryggleik har slikt føremål:

«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 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?*

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.»

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 vil i møtet orientere om status og framdrift i prosjektet. Dei vert også utfordra på å ta opp med kontrollutvalet dersom dei ser tilhøve (raude eller gule flagg) som gjer at det bør gjerast endringar i bestillinga.

Konklusjon

Dersom det ikkje kjem fram særskilte opplysningar, som t.d. krev justering ift. godkjend prosjektplan, vert det tilrådd at kontrollutvalet tar informasjonen til orientering.