Region Kalmar län

Regionrevisorerna

Datum
2022-10-21

Ärendenummer RR 2022/1

Till regionstyrelsen
Kopia för kännedom till fullmäktiges presidium

Granskning av informationssäkerheten i Region Kalmar län

Revisorerna har låtit granska huruvida regionstyrelsen säkerställer att det bedrivs ett tillfredsställande arbete för att skydda och säkra information utifrån lagstiftning, mål och riktlinjer.

Den sammanfattande bedömningen är att regionstyrelsen inte helt säkerställer att det bedrivs ett tillfredsställande arbete för att skydda och säkra information utifrån lagstiftning och mål och riktlinjer.

Bedömningen grundas på att ett flertal områden har identifierats där det saknas en dokumenterad och/eller formaliserad process för att säkerställa att säkerhets- och informationsarbetet bedrivs enligt såväl interna riktlinjer som externa lagkrav. Exempelvis är utbildningsplanen ej beslutad och det saknas kontinuerlig och formaliserad kommunikation av riktlinjer. Därtill saknas en dokumenterad process för kontinuerlig och formaliserad uppföljning av leverantörsavtal samt registerförteckning över personuppgiftsbehandlingar.

Det saknas en dokumenterad process för att säkerställa efterlevnad av styrdokument avseende dataskydd. Därtill finns ett behov av kontinuerlig rapportering till regionstyrelsen avseende hur dataskyddsarbetet fortlöper.

Regionstyrelsens övergripande mognadsgrad bedöms vara över genomsnittet för IT- och informationssäkerhet jämfört med en offentlig verksamhet av motsvarande storlek och karaktär. Granskningsresultatet indikerar att regionens mognadsgrad är högst inom hantering av programförändringar och lägst inom hantering av personuppgifter. Trots att mognadsgraden för Region Kalmar län är hög i jämförelse med annan offentlig verksamhet är det revisorernas bedömning att mognadsgraden bör vara högre sett till den storlek, riskbild samt den mängd informationstillgångar av känslig karaktär som regionstyrelsen är ansvarig för.

I granskningen har ett flertal rekommendationer till såväl regionstyrelsen som regionledningen identifierats. Samtliga rekommendationer återfinns i den bifogade rapporten över granskningen.

Revisorerna rekommenderar regionstyrelsen att:

- upprättade styrdokument avseende utbildningar och molntjänsthantering blir beslutade och implementerade.
- en plan för regelbunden kommunikation av styrande dokument upprättas, beslutas och implementeras.
- se till att dataskyddsarbetet kontinuerligt rapporteras till regionstyrelsen.
- analys genomförs över vilka delar i regionens säkerhets- och informationsarbete som verkligen är av nationellt säkerhetsintresse och således faller under säkerhetsskyddslagen.

Mot bakgrund av vad som framkommit önskar revisorerna svar från regionstyrelsen med uppgift om vilka åtgärder som planeras respektive vidtagits för att tillvarata rekommendationerna i granskningen. Detta svar önskar revisorerna ha tillhanda senast den 16 februari 2023.

Granskningen presenteras i bilagd rapport som härmed överlämnas till regionstyrelsen.

På revisorernas vägnar

Klaus Leidecker
Ordförande

Joakim Klasa
Revisionschef

Bilaga:
Rapport över granskning, EY