Revisorerna

Fredrik Ljunggren
Yrkesrevisor
Certifierad kommunal revisor
040-675 30 57
fredrik.ljunggren@skane.se

Datum 2020-11-24
Dnr 2020-RG000031

Regionstyrelsen
Kollektivtrafiknämnden

Granskning av IT- och informationssäkerhet (rapport nr 6 - 2020)

Revisorerna har genomfört en granskning av IT- och informationssäkerhet i Region Skåne. EY har biträtt i granskningsarbetet och upprättat bifogad rapport. Det övergripande syftet med granskningen har varit att bedöma om Region Skånes arbete med informationssäkerhet och IT-säkerhet, bedrivs på ett systematiskt och ändamålsenligt sätt.

Den sammanfattande bedömningen är att IT- och informationssäkerhets-arbetet inom granskade nämnder till stora delar bedrivs systematiskt och ändamålsenligt men i vissa delar är otillräckligt.

I granskningen görs bedömningen att området utvecklats i en positiv riktning under de senaste åren, framför allt inom styrning och ledning med tydliggörande av ansvar och framtagande och fastställande av relevanta styrande riktlinjer och instruktioner från centralt håll. Region Skåne har även utformat en organisation för regionalt dataskyddsarbete som bedöms möjliggöra ett strukturerat och målinriktat arbete för anpassning gentemot GDPR. Granskningen har dock påvisat brister i Region Skånes arbete med IT- och informationssäkerhet vilket har påverkat bedömningen negativt. Dessa brister rör primärt:

Systematisk uppföljning, kontroll och utvärdering – Region Skåne saknar i många hänseenden lämpliga rutiner, modeller och verktyg för att följa upp att beslutade krav och riktlinjer efterlevs, dels internt inom Region Skåne men även externt gentemot molntjänstleverantörer och andra tredjeparter.

Utbildning – Utbildningsinsatser genomförs i varierande grad inom granskade nämnder. Dock påvisar granskningen att dessa inte genomförs i en omfattning som säkerställer att samtliga medarbetare genomgår grund-läggande utbildning inom området, samt nödvändig kunskapsnivå hos medarbetare i ledande befattningar.

Patientintegritet i journalsystem – Bedömningen utifrån granskningen är att patientintegriteten i journalsystem i dess nuvarande utformning och trots nuvarande rutiner för logguppföljning av journaler inte fullt kan säkerställas. EY har dock under granskningen informerats att det är en fråga som prioriteras inom ramen för införandet av Skånes Digitala Vårdsystem.

Granskningen visar på ett antal förbättringsområden varav revisorerna särskilt lyfter följande:

Regionstyrelsen och kollektivtrafiknämnden rekommenderas att

- Genomföra en kartläggning av upprättade instruktioner inom området för informationssäkerhet och utvärdera om lämpliga instruktioner i enlighet med beslutade riktlinjer för informationssäkerhet har upprättats.
- Säkerställa att rutiner och ansvar för uppföljning av avtal med molntjänstleverantörer, personuppgiftsbiträden och andra tredjeparter med ansvar för IT-säkerhet, informationssäkerhet och dataskydd är tydligt definierade.
- Införa rutiner för regelbunden och systematisk uppföljning av informationssäkerhetsarbetet inom regionen för att utvärdera om beslutade riktlinjer efterlevs. I samband med detta utvärdera behov av resurser, systemstöd, metoder, eller instruktioner för att möjliggöra en effektiv uppföljning.
- Följa upp utbildningsinsatser för att dels kontrollera om samtliga medarbetare genomgår den grundläggande e-utbildningen i säker informationshantering och dels få insikt i hur många medarbetare som genomgått kompetenshöjande men ej obligatoriska utbildningar.

Regionstyrelsen rekommenderas även att

- Årligen genomföra uppföljning av beslutade kortsiktiga mål för informationssäkerhetsarbetet i enlighet med riktlinjerna.
- Utvärdera behov och möjligheter för att tillsätta resurser med regionövergripande ansvar för ledning, kravställning, och uppföljning rörande IT-säkerhet.
- Tillse att regionövergripande process utarbetas för att tydliggöra dels hur krav på biträden som hanterar personuppgifter för Region Skånes räkning ska definieras och dels hur instruktioner för biträdenas behandling av personuppgifter ska utformas vid tecknande av avtal.
- Genomföra en översyn av nuvarande hantering av regionens registerförteckning av personuppgiftsbehandlingar i syfte att identifiera hur systemstöd kan utvecklas för att förbättra kvaliteten i registerförteckningen, samt underlätta uppföljning och kontroll av följsamheten gentemot GDPR.
- Följa upp projektet för införande av Skånes Digitala Vårdsystem avseende hur patientens integritet i det nya systemet kommer att säkerställas i enlighet med gällande lagstiftning genom exempelvis

förbättrade behörighetsstrukturer eller automatiserad logguppföljning.

Revisorskollegiet behandlade bifogad rapport vid sammanträdet 2020-11-24 och beslutade att översända rapporten för yttrande till regionstyrelsen och kollektivtrafiknämnden avseende ovan angivna rekommendationer men även avseende innehållet i rapporten i sin helhet. Regionstyrelsen och kollektivtrafiknämnden uppmanas att svara utifrån sina uppdrag och ansvarsområden.

Vi emotser svar senast 2021-02-10.

För revisorskollegiet

Louise Rehn Winsborg
Ordförande

George Smidlund
Revisionsdirektör