Regionens revisorer
Fördjupad granskning nr 1/2022 och nr 2/2022

Regionens arbete med IT- och informationssäkerhet

Regionstyrelsen och hälso- och sjukvårdsnämnden har inte säkerställt att GDPR efterlevs på ett ändamålsenligt sätt och det brister i arbetet med IT- och informationssäkerhet. Den interna kontrollen är inte tillräcklig.

Oroande brister, som har påtalats i flera tidigare granskningar, kvarstår. Riktlinjer och regler behöver uppdateras. Vissa styrande dokument saknas helt och styrelsen och nämnden har inte gjort tillräckligt för att göra reglerna kända. Det saknas en tillräckligt utvecklad organisation för arbetet med informationssäkerhet och en analys av vilka resurser och stöd som behövs till informationssäkerhetsansvarig och dataskyddsombud i dataskyddsarbetet. Uppföljningen och kontrollen av att regler och rutiner för IT- och informationssäkerhet följs är för svagt utvecklad.

Revisorernas rekommendationer

IT- och informationssäkerhet (1/2022)

- Se över organisationen för arbetet med IT- och informationssäkerhet. Säkerställ en tydlig ansvarsfördelning.
- Inför en standardiserad process för att identifiera risker inom IT- och informationssäkerhet.
- Säkerställ att styrdokument är aktuella över tid och kända bland verksamheterna. Säkerställ att anställda får tillräcklig utbildning inom IT-och informationssäkerhet.
- Säkerställ tillräcklig uppföljning och kontroll av verksamheternas arbete med IT- och informationssäkerhet och att policyer, riktlinjer och rutiner följs.

Efterlevnad av GDPR (2/2022)

- Tydliggör hur dataskyddsarbetet ska organiseras och genomföras i regionen. Dataskyddsarbetet bör utgå från ett övergripande styrdokument för GDPR, tydlig ansvarsfördelning och dokumenterade rollbeskrivningar. Tydliggör vilket stöd och vilka resurser som finns för informationssäkerhetsansvarig och dataskyddsombud.
- Säkerställ att styrdokument är aktuella över tid och kända bland verksamheterna. Säkerställ att anställda har tillräcklig kunskap i dataskyddsarbetet genom regelbundna utbildningar.
- Säkerställ tillräcklig uppföljning och kontroll av verksamheternas hantering av personuppgifter och att policyer, riktlinjer och rutiner följs.

För ytterligare information om granskningen kontakta Petter Bergner, petter.bergner@regionvasterbotten.se, 090-785 73 72. Rapporterna finns på regionens hemsida www.regionvasterbotten.se/revision

region västerbotten