

Svar på revisionsrapport ”Informationssäkerhet – skyddade personuppgifter”

Regionens revisorer har i brev den 19 november 2025 bett om regionstyrelsens kommentarer och synpunkter på revisionsrapporten ”Informationssäkerhet – skyddade personuppgifter”.

Granskningen utgår från fyra revisionsfrågor vilka berör rutiner, uppföljning och övrig hantering av skyddade personuppgifter. Revisionen redovisar även en bedömning om tillräckliga åtgärder har vidtagits med anledning av de rekommendationer som lämnades i en tidigare revisionsrapport från 2023.

I det följande kommenteras de konkreta rekommendationer som lämnas till regionstyrelsen.

Den kan inledningsvis noteras att skyddade personuppgifter förekommer i ett stort antal system inom regionens verksamhet. Förekomsten av sådana uppgifter är inte begränsade till olika vårdstöds- och patientinformationssystem. Regionen har också anställda medarbetare med skyddade personuppgifter.

Regionstyrelsen delar bedömningen att hanteringen av skyddade personuppgifter är ett område som kräver tydliga och ändamålsenliga styrdokument. Regionstyrelsen vill samtidigt betona vikten av proportionalitet i uppföljningen. Hantering av sekretessbelagda uppgifter är en integrerad del av regionens verksamhet, och skyddade personuppgifter utgör endast en av flera sekretesskategorier. Det är därför viktigt att uppföljningskraven är i linje med hur andra sekretessreglerade uppgifter följs upp.

Regionstyrelsen har inte fått indikationer på att hanteringen av skyddade personuppgifter brister i större omfattning.

Regionstyrelsen konstaterar att rapporten omnämner att utifrån under 2023 genomförd revision har den planerade åtgärden att ta fram riktlinje för hantering, uppföljning och rapportering av skyddade personuppgifter inte kunnat utföras. Detta är en följd av mycket hård arbetsbelastning på informationssäkerhetsorganisationen och under 2025 varande mycket hög personalomsättning. Riktlinje avses att tas fram för detta ändamål senast under det tredje kvartalet 2026 och tillsammans med befintlig rutin utgör detta då de regiongemensamma styrdokumenterna för hantering av skyddade personuppgifter. I arbetet med framtagandet kommer både det mer renodlade informations-säkerhetsperspektivet och juristernas kompetens att nyttjas.

Regionstyrelsen instämmer i att lokala rutiner ska tas fram när det finns ett reellt behov, det vill säga när den regionövergripande rutinen inte ger tillräcklig vägledning utifrån verksamhetens specifika risker. De regiongemensamma styrdokumenterna som utvecklas bedöms i normalfallet täcka verksamheternas behov, men kompletterande lokala rutiner kan upprättas där det krävs, detta utifrån den regiongemensamma rutinen.

Regionstyrelsen delar bedömningen att det är av vikt att tillskapandet och implementeringen av lokala rutiner, där så är påkallat, genomförs. Det förutsätts att lokala rutiner följer regionens styrdokument och att efterlevnaden säkerställs genom ordinarie lednings- och styrprocesser. Regionstyrelsens framtåsyftande arbete med att stärka styrning och processägarskap kommer ytterligare att bidra till att tydliggöra ansvar och stärka uppföljningsstrukturerna.

Regionstyrelsen noterar att den i enlighet med 2023 års revision aviserade åtgärden om framtagande av rutin för hantering av tillgångars riskanalys har framtagits och fastställts – något som konstaterats i denna rapport.

Avseende rekommendationen om att säkerställa att rutin för riskanalys implementeras ser regionstyrelsen att detta säkras genom den generella information som går ut vid upprättandet av nytt respektive uppdaterat regionövergripande styrdokument. Därtill ska särskild informationsinsats via Kommunikation, med stöd av systemförvaltningsobjektet Administration och kommunikation, genomföras.

Regionstyrelsen ser positivt på revisorernas förslag om att tydliggöra processägarskapet inom informationssäkerhet och konstaterar att det kommande arbetet kring detta som redan initierats avses adressera sådant behov.

REGIONSTYRELSEN

Sara Nylund
Ordförande

Åsa Bellander
Regiondirektör