Region Västernorrland

Tjänsteställe, handläggare

Datum	Dnr	Sida
2023-12-20	23REV41	1(3)

Distribution
Hälso- och sjukvårdsnämnden
Regionstyrelsen

Delges:
Regionfullmäktige

Granskning informationssäkerhet – uppföljning och skyddade personuppgifter

Vid överläggningar med Regionens revisorer den 20 december behandlades revisionsrapporten *Granskning informationssäkerhet – uppföljning och skyddade personuppgifter*.

Vi vill med anledning av vår granskning få del av Regionstyrelsens och Hälso- och sjukvårdsnämndens kommentarer samt information om planerade åtgärder inom området. Svaret bör vara oss tillhanda senast den 29 mars 2024.

Bakgrund

Revisorerna granskade år 2019 regionens informationssäkerhet. Syftet med granskningen var att bedöma om Regionstyrelsen hade tillsett att informationssäkerheten var tillräcklig. I granskningen ingick en uppföljning av 2017 års granskning av IT-säkerheten.

Den sammanfattande bedömning som gjordes utifrån 2019 års granskning var att Regionstyrelsen inte hade säkerställt att ändamålsenliga åtgärder hade vidtagits med anledning av 2017 års granskning samt att Regionstyrelsen inte hade säkerställt en tillfredsställande styrning, uppföljning och kontroll av informationssäkerheten. Bedömningen baserades på avsaknad av ett gediget ledningssystem för informationssäkerhet och tillhörande organisatorisk struktur och dokumentation, avsaknad av regelbundna rapporteringsrutiner avseende informationssäkerhetsarbetet samt brister i regionens uppföljning och vidtagande av ändamålsenliga åtgärder som följd av iakttagelserna från 2017 års granskning.

Regionen behöver i övrigt kunna hantera skyddade personuppgifter, som är ett samlingsbegrepp för åtgärder som används för att skydda personer som riskerar att utsättas för hot, våld eller förföljelse. Enligt uppgifter från Jämställdhetsmyndigheten lever i Sverige cirka 15 000 kvinnor och 10 000 män med skyddade personuppgifter.

Revisorerna har bedömt att det finns en risk för att inte tillräckliga åtgärder har vidtagits utifrån föregående granskning. Revisorerna har även bedömt att det föreligger en risk för bristande rutiner för hantering av skyddade personuppgifter.

Granskningen har utförts av Helseplan.

Postadress
871 85 Härnösand

Besöksadress
Södra vägen 3-5
Härnösand

Telefon
0611-800 00

E-post
revision@rvn.se

Iakttagelser och bedömning

Nedan framgår de samlade bedömningar som gjorts samt vad de baseras på.

- Regionstyrelsen har inte säkerställt en tillräcklig intern styrning och kontroll när det gäller hanteringen av skyddade personuppgifter och informationssäkerhet. Ett ledningssystem för informationssäkerhet (LIS) har upprättats och en virtuell informationssäkerhetsorganisation har etablerats. Inom ramen för LIS finns styrande dokument som redogör för riktlinjer och rutiner kring informationssäkerhet och skyddade personuppgifter. Däremot har Regionstyrelsen inte utifrån sitt övergripande ansvar för informationssäkerhet säkerställt att det finns strukturer för uppföljning av att rutinerna för skyddade personuppgifter efterlevs.
- Det har inte vidtagits tillräckliga åtgärder utifrån 2019 års granskning. Regionen har upprättat ett LIS på central nivå och en virtuell informationssäkerhetsorganisation har etablerats vilket skapar förutsättningar för regionens fortsatta informationssäkerhetsarbete. Därtill har även en riktlinje för säkerhetsskyddsanalys fastställts. För ett flertal av rekommendationerna har åtgärder delvis vidtagits eller att åtgärder inte vidtagits utifrån rekommendationerna från föregående granskning.
- Hälso- och sjukvårdsnämnden har utifrån sitt vårdgivaransvar inte säkerställt en tillräcklig intern styrning och kontroll för hanteringen av skyddade personuppgifter i de verksamheter som ingår i nämndens uppdrag. Det finns en regiongemensam rutin för skyddade personuppgifter men däremot saknas styrande dokument för att tillse att det sker en tillräcklig uppföljning av att rutinerna efterlevs. Av granskningen framkommer att det även saknas rutiner för rapportering av genomförd uppföljning av skyddade personuppgifter.

Rekommendationer

I revisionsrapporten framgår de rekommendationer som riktar sig till Regionstyrelsen respektive Hälso- och sjukvårdsnämnden. Dessa återges nedan.

Regionstyrelsen rekommenderas:

- att följa upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- att säkerställa och följa upp att en regiongemensam struktur för riskanalyser avseende hanteringen av skyddade personuppgifter upprättas.
- att säkerställa en ändamålsenlig struktur för förankring av styrdokument och rutiner för skyddade personuppgifter inom organisationen.
- att säkerställa en ändamålsenlig uppföljning av personalens kunskap kring gällande regelverk samt att tydliggöra vem som ansvarar för att uppföljning genomförs.

- att säkerställa tillgång till tillräckliga resurser för att regionen ska kunna upprätthålla ett ändamålsenligt arbete avseende informationssäkerhet. Avseende arbetet med skyddade personuppgifter behöver ett tydligt uppdrag och resurser ges till ansvarig enhet.
- att utreda behovet av att göra utbildning i informationssäkerhet och skyddade personuppgifter obligatorisk för berörd personal i syfte att säkerställa tillräcklig kunskap om informationssäkerhet samt hantering av skyddade personuppgifter inom organisationen.
- att säkerställa att alla medarbetare återkommande genomgår relevanta utbildningar med lämpligt intervall för att trygga bestående kunskap över tid.
- att utreda behovet av att erbjuda praktiska utbildningar i hantering av skyddade personuppgifter.
- att säkerställa att riktlinjer för hanteringen av skyddade personuppgifter tas fram samt att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.
- att säkerställa att riktlinjer för uppföljning och rapportering av skyddade personuppgifter tas fram samt att efterlevnad till riktlinjerna systematiskt och kontinuerligt följs upp i verksamheten.

Hälso- och sjukvårdsnämnden rekommenderas:

- att följa upp att de lokala rutinerna för hantering av skyddade personuppgifter utgår från regiongemensamma strukturer.
- att i dialog med Regionstyrelsen verka för att nödvändiga dokument tas fram.
- att när dokumenten är beslutade säkerställa att dessa implementeras i verksamheten inom nämndens ansvarsområde.

REGIONENS REVISORER

Ingemar Wiklander
Ordförande

Birgitta Arnberg
Revisionsdirektör