

Till
Regionstyrelsen för svar
Regionfullmäktige för kännedom

Uppföljande och fortsatt granskning av informationssäkerhet och GDPR

PwC har på uppdrag av Region Västmanlands revisorer genomfört en uppföljning och fortsatt granskning av informationssäkerhet och GDPR. Granskningen syftar till att bedöma om regionstyrelsen har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats samt säkerställt en ändamålsenlig personuppgiftshantering.

Vi bedömer sammantaget att regionstyrelsen inte helt har säkerställt att tidigare identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats. Vidare bedömer vi att regionstyrelsen ej har säkerställt en ändamålsenlig personuppgiftshantering.

Utifrån vår uppföljning av tidigare granskning rekommenderas regionstyrelsen att säkerställa att:

- Region Västmanlands Organisation för systematiskt säkerhetsarbete 29043-2, SSO:n, uppdateras och förtydligar Informations säkerhetsrådets syfte och ansvar.
- Tydliggöra kopplingen mellan ansvar och roll, exempelvis för informationssäkerhetssamordnaren och informationssäkerhetsstrategen.
- Förtydliga ansvar och roller i PM3-modellen kopplat till säkerhetsåtgärder som riskanalyser, konsekvensanalyser, händelse- och avvikelseanalyser, kontinuitetshantering samt sårbarhetsanalyser.
- Intensifiera planen med att införa obligatoriska, regelbundna utbildningsmoment för samtliga medarbetare inom regionen. I sammanhanget bör rutin tas fram för att säkerställa genomförande av framtagna utbildningar.
- Genomföra projekt med målsättningen att förbättra behörighetshantering i journal-systemet. Fokusområden bör vara genomförande av riskanalys vid behörighetstilldelning, tydliggöra gallringsrutiner samt säkerställa godtagbar följsamhet av interna rutiner inkluderat kontinuerliga stickprov i patientjournalssystemet.
- Verksamhetsplan 2022 blir en formellt beslutad verksamhetsplan och att planerade aktiviteter är budgeterade.
- Metoder och riktlinjer för upphandlingsprocessen tas fram.

Gällande Region Västmanlands arbete med GDPR rekommenderar vi regionstyrelsen att säkerställa att:

- Framtagna riktlinjer och policies är uppdaterade och att kontinuerlig revidering införs, samt tydlig märkning med datum vilket kommer skapa en tydlighet för medarbetare och öka spårbarhet av ändringar.
- Utforma fler riktlinjer kopplat till GDPR, exempelvis rutin för konsekvensbedömning, för att standardisera regionens arbetssätt.
- Tydliggöra hur organisationen ska ta del av styrdokumentationen kring GDPR.

- Prioritera utbildningsinsatser kring dataskydd.
- Framtagande av en registerförteckning av personuppgiftsbehandlingar genomförs.
- Det utses lokalt ansvariga inom förvaltningarna för dataskyddsfrågor, t.ex. i form av en roll som dataskyddssamordnare, eller tydliggöra för verksamhetschefer om vilket ansvar de faktiskt har över sina förvaltningar då denna insikt är låg i dagsläget.
- En systematisk internkontroll av verksamheternas dataskyddsarbete återstartas så snart som möjligt.

Iakttagelser i sin helhet framgår i bifogad rapport som har godkänts vid revisorernas sammanträde 2022-10-12. Revisorerna översänder rapporten till regionstyrelsen och önskar svar senast 2023-01-11.

FÖR REGIONENS REVISORER

Hans Strandlund
Ordförande

Elisabeth Löf
Revisor