VÄSTRA GÖTALANDSREGIONEN
REVISIONSENHETEN

2022-12-14

Till regionstyrelsen

Granskning av regionens dataskyddsarbete (REV 2022-00038)

Revisionen har granskat efterlevnaden av dataskyddsförordningen inom Koncernkontoret vilket ingår i regionstyrelsens personuppgiftsansvar. Syftet med granskningen har varit att bedöma om regionstyrelsen bedriver ett ändamålsenligt arbete utifrån dataskyddsförordningens krav.

Granskningens visar att regionstyrelsen har en bristande efterlevnad av dataskyddsförordningen.

Vår bedömning är att regionstyrelsen inte har säkerställt att den inom sitt personuppgiftsansvar bedriver ett ändamålsenligt arbete utifrån dataskydds-förordningens krav. De dokument som i dag är styrande är alltför övergripande för att säkerställa efterlevnad av dataskyddsförordningen.

Vi konstaterar även att det saknas en regelbunden rapportering av dataskydds-arbetet från dataskyddsombud till regionstyrelsen. Regionstyrelsen har genom detta brustit i sin kontroll och uppföljning av arbetet.

På nästa sida finns de rekommendationer som vi lämnar med anledning av granskningen.

Vi önskar få ett yttrande från er senast den 30 april 2023. Av yttrandet ska framgå vilka åtgärder som ni har gjort eller planerar att göra med anledning av de rekommendationer som vi lämnar. Yttrandet skickar ni till revision@vgregion.se.

Revisionsrapporten översänds för yttrande till regionstyrelsen och för kännedom till regionfullmäktiges presidium samt övriga nämnder och styrelser i regionen.

För revisorskollegiet,

Birgitta Eriksson,
ordförande

Krister Stensson,
vice ordförande

Rekommendationer

Revisionen rekommenderar regionstyrelsen att:

- etablera en dataskyddsorganisation med tillräckliga resurser att stödja dataskyddsombud i utförande av de uppgifter som dataskydds-förordningen ställer krav på.

- komplettera nuvarande riktlinje och rutiner med ansvarsbeskrivningar för nyckelroller.

- integrera dataskyddsarbetet i ledningssystemet för informationssäkerhet genom att komplettera styrdokument med krav avseende personuppgifts-hanteringen.

- upprätta registerförteckning för samtliga personuppgiftsbehandlingar inom regionstyrelsens personuppgiftsansvar.

- erbjuda regelbunden utbildning till samtliga medarbetare som hanterar personuppgifter, samt avväga vilka kompletterande utbildningar som bör erbjudas nyckelfunktioner och ansvariga i dataskyddsarbetet.

- tydliggöra incidenthanteringsrutiner med instruktioner om när personuppgiftsansvariga ska informeras.

- tillse att dataskyddsombud genomför årlig granskning av dataskydds-arbetet med bedömning av efterlevnad av dataskyddsförordningen och att uppföljning rapporteras till regionstyrelsen.

*