Region Västmanland

Regionkontoret

Datum
2023-01-09

vår beteckning
RV220707-4

Regionens revisorer

YTTRANDE ÖVER UPPFÖLJANDE OCH FORTSATT GRANSKNING AV INFORMATIONSSÄKERHET OCH GDPR

Regionens revisorer har överlämnat sin granskningsrapport ”uppföljande och fortsatt granskning av informationssäkerhet och GDPR” till regionstyrelsen för yttrande.

Granskningen syftar till att bedöma om regionstyrelsen har säkerställt att tidigare (2019) identifierade brister kopplat till informationssäkerhetsarbetet har åtgärdats samt säkerställt en ändamålsenlig personuppgiftshantering.

Revisorernas sammanfattande bedömning är att regionstyrelsen inte helt har säkerställt att tidigare identifierade brister kopplat till informations-säkerhetsarbetet har åtgärdats. Vidare bedömer revisionen att regionstyrelsen ej har säkerställt en ändamålsenlig personuppgiftshantering.

Nedan följer beskrivning av planerade åtgärder och kommentarer till de rekommendationer och synpunkter som lyfts fram i rapporten.

Som ett led i att lyfta regionens informationssäkerhets- och dataskyddsarbetet har, efter framtagandet av revisionsrapporten, informationssäkerhetsorganisationen förstärkts med en samordnare. Resursförstärkningen gör att både det operativa verksamhetsstödet i form av t ex utbildning, rådgivning och uppföljning och det strategiska arbetet inom informationssäkerhet och dataskydd kan intensifieras. Ett område som kommer att prioriteras är en översyn och uppdatering av befintliga styrdokument och framtagande av nya dokument inom GDPR-området för att därigenom öka effekten i arbetet med dataskydd med syfte att säkerställa en ändamålsenlig personuppgiftshantering. Ett exempel på nytt styrdokument är den mall för registerförteckning som publicerades i november. Ledningssystem för informationssäkerhet och GDPR kommer att tillgängliggöras bl.a. genom intranätet och inom områdets utbildningspaket.

Revisorerna rekommenderar att regionens organisation för systematiskt säkerhetsarbete 29043-2, SSO:n, uppdateras och att informationssäkerhetsrådets syfte och ansvar då förtydligas. Därutöver framhålls att verksamhetsplan 2022 blir en formellt beslutad verksamhetsplan och att planerade aktiviteter är budgeterade. Styrdokument för den systematiska säkerhetsorganisationen (SSO) och informationssäkerhetsrådet kommer att uppdateras. Övergripande verksamhetsplan för områdena inom SSO:n (bl. a. informationssäkerhetsrådet) fastställdes av riskkommittén 2022-09-19. Vad gäller budgetering av aktiviteter för SSO:ns verksamhetsområden (informationssäkerhet, katastrofmedicinsk beredskap och allmän säkerhet) så sker finansiering inom ramen för verksamheternas ordinarie budget.

Inom informationssäkerhetsområdet finns en obligatorisk e-utbildning (beslutad av regiondirektören 2019-11-13. En uppdatering av innehållet med bl.a. material om dataskydd och verksamhetschefernas ansvar för dataskyddsfrågor planeras publicera till första halvåret 2023. Uppföljning av utbildningens genomförande görs i samband

med framtagande av årsrapport för informationssäkerhet (Q1). Som komplement till e-utbildningen kommer det fr.o.m. 2023, införas två utbildningstillfällen per år inom informationssäkerhet och dataskydd i utbildningsenheten ordinarie utbud.

Revisionen rekommenderar även att metoder och riktlinjer för upphandlingsprocessen tas fram. 2019 togs ett stödmaterial fram för upphandling av IT-relaterade tjänster, kallat ”Analyshäftet”. Under 2022 har ett gemensamt arbete mellan informationssäkerhetsfunktionerna i Västmanland och Sörmland samt den gemensamma inköpsorganisationen Sörmland/Västmanland resulterat i nya rutiner och instruktioner som stöd för informationssäkerhetskrav i upphandling.

En förstudie som syftar till att förbättra behörighetsantering i vårdsystem har pågått sedan 2021. En projektgrupp är tillsatt av Hälso- och sjukvårdsförvaltning för att under 2023 genomföra en behovs- och riskanalys gällande behörighetshantering.

Ytterligare en rekommendation är att, så snart som möjligt, återstarta en systematisk internkontroll av verksamheternas dataskyddsarbete. Informationssäkerhet och dataskydd kommer, inom ramen för regionens nya modell, att lyftas upp som ett prioriterat område för intern kontroll 2023.

Revisionen föreslår att det antingen utses lokalt ansvariga inom förvaltningarna för dataskyddsfrågor, t.ex. i form av en roll som dataskyddssamordnare, eller att verksamhetschefernas ansvar tydliggörs. Att avsätta administrativa resurser i verksamheterna för dataskydd bedöms inte som ett förstahandsalternativ. En första åtgärd blir att ta fram ett informationsmaterial om dataskyddsfrågor som är riktat till regionens verksamhetschefer.

Vad gäller förtydligandet av ansvar och roller i PM:3-modellen kopplat till säkerhetsåtgärder ligger ansvaret ytterst hos respektive objektägare verksamhet/IT.

De synpunkter som i övrigt framkommit i rapporten kommer att vara vägledande i det fortsatta utvecklingsarbetet inom området.

Regionstyrelsen avser att särskilt följa det fortsatta arbetet med att säkerställa en ändamålsenlig personuppgiftshantering.

FÖR REGION VÄSTMANLAND

Mikael Andersson Elfgren
Regionstyrelsens ordförande

Anders Åhlund
Regiondirektör