§ 45/24 Yttrande över revisionens granskning Hantering av personuppgifter enligt Dataskyddsförordningen, GDPR

Diarienummer: RS-LED23-2806

Regionstyrelsens beslut

Yttrandet godkänns.

Proposition

Ordförande Christoffer Öqvist (M) ställer förvaltningens förslag under proposition och finner att det bifalls.

Ärendet

Region Sörmlands revisionskontor har, på uppdrag av regionens revisorer, genomfört en fördjupad granskning av hantering av personuppgifter enligt dataskyddsförordningen, GDPR. Den övergripande revisionsfrågan är om regionstyrelsen och regionens nämnder säkerställer en ändamålsenlig hantering av personuppgifter. Granskningen omfattar regionstyrelsen och regionens nämnder och avser om regionen säkerställer att regionen följer dataskyddsförordningen, att regelverket är känt och tillämpas.

Revisorernas sammanfattande bedömning är att regionstyrelsen inte helt har säkerställt förutsättningar för en ändamålsenlig hantering av regionens personuppgifter utifrån dataskyddsförordningen.

Revisorerna har framfört synpunkter gällande brister i organisation av dataskyddsarbetet, oklara ansvarsförhållanden och behov av justeringar och förtydliganden i styrande dokument, informationsmaterial och utbildningar. Revisorerna pekar särskilt på den organisationsförändring som genomfördes under första halvåret 2023 som ett skäl till den oklara ansvarsfördelning, vilket har åtgärdats genom beslut om att sammanföra informationssäkerhet och dataskyddsarbetet under Informationssäkerhetschefens ledning.

Regionstyrelsen ställer sig bakom revisorernas rekommendationer och de i yttrandet föreslagna aktiviteterna, vilka stämmer överens med styrelsens ambitioner gällande informationssäkerhet och dataskydd. I regionstyrelsens yttrande framförs vikten av att regionen uppfyller de regler som Dataskyddsförordningen (2018:218) föreskriver.

Sammanfattningsvis avser Region Sörmland att utveckla dataskyddsarbetet tillsammans med det systematiska och riskbaserade IT- och informationssäkerhetsarbetet samt stärka styrning, kontroll och uppföljning på området

Beslutsunderlag

Tjänsteutlåtande Revisionens granskning Hantering av personuppgifter enligt Dataskyddsförordningen, GDPR, RS-LED23-2806-3
Yttrande över revisionens granskning av ”Hantering av personuppgifter enligt dataskydds-förordningen, GDPR”, RS-LED23-2806-3
Granskningsrapport - Hantering av personuppgifter enligt dataskyddsförordningen, GDPR, RE-REV23-0037-1
Regiondirektörens verkställighetsbeslut 1/24 – Beslut om att omorganisera Utvecklingsenheten, Staben för demokrati och insyn samt RS IT, RS-LED24-0018-1

Beslutet expedieras till

Revisionen
Magnus Johansson, regiondirektör
Urban Petrén, IT-direktör
Mats Olsson, informationssäkerhetschef
Akten

REGION SÖRMLAND

Handläggare
Mats Olsson
Region Sörmland IT

Datum
2024-03-06

Dokumentnummer
RS-LED23-2806-3

Yttrande över revisionens granskning Hantering av personuppgifter enligt Dataskyddsförordningen, GDPR

Regionstyrelsen har mottagit en granskningsrapport (RE-REV23-0037-1) från revisionen gällande ”Hantering av personuppgifter enligt dataskydds-förordningen, GDPR”. Regionstyrelsen ska yttra sig senast den 12 april 2024.

Regionstyrelsen ser positivt på granskningen och ställer sig bakom revisionens rekommendationer. Region Sörmland har ambitionen att leva upp till lagstiftarens krav gällande hantering av personuppgifter och övriga informationstillgångar.

Revisionens samlade bedömning är att regionstyrelsen inte helt har säkerställt förutsättningar för en ändamålsenlig hantering i regionen av personuppgifter utifrån dataskyddsförordningen.

De organisationsförändringar som genomfördes i juni 2023 medförde uppdelade och oklara ansvarsområden gällande informationssäkerhet och dataskydd, vilket har omhändertagits genom beslut RS-LED24-0018-1. Av beslutet framgår att informationssäkerhet och dataskydd sammanförs under informationssäkerhetschefens ledning liksom ansvaret för det externa dataskyddsombudet och det praktiska informationssäkerhetsarbetet som tidigare utförts av Säkerhetsenheten.

De brister som identifierats gällande hantering av nämndernas personuppgiftsansvar och avsaknaden av dataskyddsombud kommer att hanteras av informationssäkerhetschefen med inriktning mot gemensamma lösningar så lång det är möjligt.

De rekommendationer som lämnas i rapporten ska inkorporeras i den verksamhetsplan som har utarbetats inom RSIT för informationssäkerhets- och dataskyddsarbetet. Aktiviteter i verksamhetsplanen som kommer att omhänderta påpekade brister i dataskyddet är:

- styrande dokument, skriftliga rutiner och informationsmaterial kommer att uppdateras och kompletteras där regleringar saknas
- regionens e-utbildningar kommer att kompletteras enligt givna rekommendationer och föreslås bli obligatoriska för anställda och uppdragstagare att genomföra med jämna mellanrum.

- genomförande av konsekvensanalyser kommer att uppdras åt respektive förvaltningsobjekt att svara för.

För genomförande av informationssäkerhets- och dataskyddsarbetet behöver regionstyrelsen överväga ifall resurstilldelningen behöver öka för att möta lagstiftarens krav gällande nämnda områden. Frågan kommer att hanteras inom ramen för budgetberedning för de kommande åren.

Christofer Öqvist (M)
Regionstyrelsens ordförande

Magnus Johansson
Regiondirektör