Revisonsskrivelse 2022-02-16

Till: Kommunstyrelsen
För kännedom: Fullmäktiges presidium

Uppföljande granskning av stadens informationssäkerhet samt följsamhet gentemot GDPR

EY har på uppdrag av de förtroendevalda revisorerna i Sundbybergs stad följt upp två fördjupade granskningar och en uppföljning som genomfördes under revisionsåren 2019 och 2020. Syftet med uppföljningen är att bedöma om de åtgärder som vidtagits inom identifierade förbättringsområden samt resultaten som uppnåtts är tillräckliga utifrån revisorernas givna rekommendationer. Granskningen omfattar uppföljning av följande fördjupade granskningar:

- Granskning av stadens arbete med informationssäkerhet med fokus på styrning, organisation och incidenthantering
- Granskning av efterlevnad - Dataskyddsförordningen GDPR

Granskningen omfattar även uppföljning av stadens åtgärder med anledning av Schrems II (C311/18) ”Överföring av personuppgifter till tredjeland”.

Vår sammanfattade bedömning är att kommunstyrelsen inte har nått tillräckligt långt i arbetet vad gäller informationssäkerhet mot bakgrund av tidigare lämnade rekommendationer. Detta även fast relativt lång tid har förflutit sedan tidigare granskningar. I flera fall konstaterar vi att ett arbete pågår och en del rekommendationer därför inte har beaktats fullt ut. I flera fall har revisorernas rekommendationer varken beaktats eller åtgärdats, däribland kvarstår vissa brister som vi bedömer vara av allvarlig karaktär.

Bland kvarstående brister vill vi bland annat lyfta fram att vi anser det vara allvarligt att ett beslutat och kommunicerat ledningssystem för informationssäkerhet fortsatt saknas. Det är inte ett lagstadgat krav att implementera ett ledningssystem för informationssäkerhet, men det kan enligt vår bedömning dels betraktas som vedertagen praxis, dels ha en betydande inverkan på resterande delar i stadens informationssäkerhetsarbete. Resultatet är att Sundbybergs stad fortsatt saknar flertalet grundläggande komponenter för att säkerställa ändamålsenlig informationssäkerhetsstyrning, däribland en informationssäkerhetsspecifik organisationsstruktur, adekvata uppföljningar samt en formulerad stadsövergripande process för åtkomsthantering.

Vi bedömer att det därför kvarstår ett omfattande arbete för att åtgärda de rekommendationer som delvis, alternativt inte alls, har beaktats.

För Sundbybergs stads revisorer

Torbjörn Nylén
Ordförande

HansErik Salomonsson
Vice ordförande

Revisionsskrivelsen har godkänts via e-post i enlighet med SKR:s instruktioner.