Sundbybergs stad

Revisonsskrivelse 2020-03-26

Till: kommunstyrelsen, stadsmiljö- och tekniska nämnden
För kännedom: Fullmäktiges presidium

Granskning av efterlevnad av GDPR

De förtroende revisorerna har låtit EY genomföra en granskning av stadens efterlevnad av GDPR. Syftet med granskningen var att ge en *övergripande* förståelse och bedöma huruvida Sundbybergs stad och dess helägda bolag bedriver ett ändamålsenligt arbete med dataskyddsförordningen.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under november 2019 till februari 2020. Enligt metoden bedöms stadens mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (*begynnande*) till 5 (*optimerad*) inom de respektive 12 områdena. Analysen har baserats på intervjuer med identifierade nyckelpersoner i stadens och dess helägda bolags personuppgiftssäkerhetsarbete samt genomgång av insamlad styrdokumentation i staden och bolagen.

Baserat på den analys och granskning som genomförts bedöms Sundbybergs stad ha en förhållandevis låg mognadsgrad på 1,9 av maximalt 5,0. Mognadsgraden bedöms vara som högst inom incidenthantering samt begäran från och information till registrerade. Lägst är mognadsgraden inom styrning och riskhantering. De helägda bolagen har sammantaget medel till god mognadsgrad i förhållande till jämförbara organisationer, med undantag för vissa specifika områden inom respektive bolag.

Stadens mest väsentliga utvecklingsområde består i att ta fram och anta fullständiga styrdokument på personuppgiftsområdet. Staden måste även tydligt dokumentera organisationsstrukturen, främst avseende IT- och informationssäkerhetsbefattningar, med tydlig ansvarsfördelning, samt eventuellt revidera organisationsstrukturen. Dagens organisationsstruktur och brister i tilldelade resurser ligger till grund för de problem som rapporten identifierar för Sundbybergs stad. Övriga väsentliga förbättringsområden gäller införande av regelbundna utbildningar, strukturerade granskningar med föreslagna åtgärder och en översyn av leverantörsrelationerna. Av de 12 områden EY granskat har staden komplett dokumentation endast för incidenthantering.

Utifrån granskningens resultat riktas fem rekommendationer till staden. Rekommendationerna finns att ta del av i granskningsrapporten.

Rapporten överlämnas härmed till berörda nämnder. Nämndbehandlade svar till revisionen önskas senast den 30 juni 2020.

För Sundbybergs stads revisorer

Torbjörn Nylén
Ordförande

HansErik Salomonsson
Vice ordförande

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