Nacka kommun

Revisionsskrivelse A 2020-09-16

Revisorerna

Till: Kommunstyrelsen

För kännedom: Kommunfullmäktige

Granskning. Efterlevnad av Dataskyddsförordningen GDPR

EY har på vårt uppdrag genomfört en granskning av kommunens hantering av personuppgifter och efterlevnad av dataskyddsförordningen (The General Data Protection Regulation, GDPR). Granskningens syfte har varit att övergripande pröva om kommunen som helhet bedriver ett ändamålsenligt arbete med dataskyddsförordningen och hur väl man uppfyller de åtgärder som förordningen stipulerar.

En översiktlig granskning av 12 olika områden med utgång i EY:s ramverk för personuppgiftshantering gentemot dataskyddsförordningen för kommunala verksamheter har genomförts under maj till juni i år. Enligt metoden bedöms verksamhetens mognadsgrad enligt 116 punkter på en ordinarie skala från 1 (begynnande) till 5 (optimerad) inom de respektive 12 områdena. Den genomsnittliga mognadsgraden är baserad på snittet av mognadsgraden för de respektive 12 områdena.

Baserat på den analys och granskning som genomförts bedöms Nacka kommun ha den genomsnittliga mognadsgraden 3,4 av 5,0. Det är en högre mognadsgrad än vad EY har observerat att genomsnittet är för en kommun. Nacka har arbetat ambitiöst med personuppgiftsfrågor och nyckelpersonerna i den centrala dataskyddsorganisationen har kommit långt i sitt arbete.

Överlag bedöms mognadsgraden vara högst inom organisation och ansvar, riskhantering samt utbildning. Nacka har ett dataskyddsombud (DSO) på heltid, en väl utvecklad organisation kring dataskyddsfrågor och har ägnat mycket resurser åt utformning av rutiner samt implementation och medvetenhet bland anställda. Mognadsgraderna i styrning och kontroll bedöms däremot vara något lägre då dessa områden i viss mån har prioriterats lägre, när man har fokuserat på implementation av praktisk hantering av dataskyddsfrågor. En ej optimerad kontroll påverkar även flera andra områden negativt i bedömningen då en högre mognadsgrad generellt sett är beroende av systematisk uppföljning inom varje område.

Den viktigaste förbättringspunkten enligt EY är att upprätta mer formaliserade rutiner för granskning av efterlevnad. Syftet är att minska risker för otillbörlig behandling av personuppgifter på grund av att man missat efterlevnad av rutiner. Vi rekommenderar därför kommunen att förbättra sin internkontroll genom att skapa ett rapporteringskrav med fastställd frekvens och innehåll som de kommunala verksamheterna kan utgå från för att säkerställa att uppföljning och förbättringsarbete sker effektivt i samtliga enheter.

Med utgångspunkt från granskningen rekommenderar vi kommunstyrelsen att säkerställa:

- Utökad kontroll av efterlevnad (se revisionsrapporten)
- Att alla styrande dokument där så är lämpligt är uppdaterade enligt kraven i dataskyddsförordningen.
- Att kommunen utvärderar sina processer inom personuppgiftshantering utifrån grad av centralisering och decentralisering för att bedöma om varje process är optimal ur ett resursperspektiv.
- Att Nacka kommun prioriterar att kontrollera kvaliteten av registerutdragen.

Vi önskar svar på rekommendationerna från kommunstyrelse senast 2020-12-30.

För revisorerna i Nacka kommun

Yvonne Wessman
Ordförande

Lars Berglund
Vice ordförande

Bilaga: Revisionsrapport 2/2020 Granskning. Efterlevnad av Dataskyddsförordningen GDPR