**Kommunrevisionen**
**Täby kommun**

Kommunstyrelsen

*För kännedom:*
Kommunfullmäktige

**Granskning av kommunens styrdokument inom ramen för dataskyddsförordningen**

KPMG har av Täby kommuns revisorer fått i uppdrag att granska kommunens styrdokument inom ramen för dataskyddsförordningen. Dataskyddsförordningen trädde ikraft den 25 maj 2018 och är gällande ramverk för behandling av personuppgifter. Den nya lagstiftningen syftar bl.a. till ett starkare skydd för individers integritet och större makt till att kunna bestämma över sina personuppgifter.

Bristande hantering samt överträdelser kan innebära betydande sanktionsavgifter samt leda till förtroendeskador för kommunen. Sammanfattningsvis kan konstateras att kommunstyrelsen i huvudsak har tillfredställande styrdokument och rutiner vad avser tillämpningen av dataskyddsförordningen. Det finns utvecklingsområden vad avser arbetet med och efterlevnaden av dataskyddsförordningen.

Mot bakgrund av vår granskning och våra iakttagelser rekommenderar vi följande:

- Mot bakgrund av den centraliserade dataskyddsorganisationen vill vi betona att det är av stor vikt att nämnder och styrelser är införstådda med ansvarsförhållandet, där respektive nämnd och styrelse är juridiskt sett ytterst ansvarig för att uppnå en tillfredställande nivå vad avser efterlevnaden av dataskyddsförordningen samt ansvarar för att säkerställa att hantering av personuppgifter följer gällande föreskrifter. Kommunstyrelsen kan inte inta rollen som personuppgiftsansvarig för någon annan nämnd eller styrelse. Detta även att dataskyddsorganisationen lyder under kommunstyrelsen. Det är med andra ord inte dataskyddsombudet eller kommunstyrelsen som hålls ansvarig vid en eventuell bristande efterlevnad av dataskyddsförordningen inom övriga nämnder och styrelser.
- Kommunstyrelsen bör säkerställa att medarbetarna har en insikt för utredningsunderlagets funktion och syfte avseende personuppgiftsincidenter. Underlaget är avgörande för bedömning av incidenterna, där bl.a. risk- och konsekvensbedömning av inträffade incidenter är en central del som behöver genomföras och färdigställas.
- Den kommunövergripande utredningsmallen avseende personuppgiftsincidenter bör kompletteras med svars-/bedömningsrutor avseende information om huruvida incidenten kommer att anmälas till tillsynsmyndigheten samt huruvida de registrerade ska informeras om incidenten. Det är av vikt att denna information dokumenteras samt framgår på ett tydligt sätt i underlaget.
- Rutinbeskrivningen avseende hantering av personuppgiftsincidenter bör revideras vad avser formuleringen om ”information till den registrerade” i Täby kommun Granskning av kommunens styrdokument inom ramen för dataskyddsförordningen 2021-03-10 samband med en incident, där dagens formulering riskerar leda till misstolkningar.

- Beskrivning av rutiner för utvärdering och avgörande av anmälningspliktiga incidenter i styrdokumentet samt den information som återges på intranätet bör vara densamma. - Styrdokumentet avseende hantering av personuppgiftsincidenter kan med fördel förtydligas med att dokumentation av personuppgiftsincidenter ska ske oaktat allvarlighetsgrad samt oaktat om incidenten anmäls till tillsynsmyndigheten eller ej.
- Det finns ett behov av kunskapsökning bland personalen i verksamheterna, där utbildning i form av återgivning av konkreta exempel är av betydelse för en ökad förståelse samt upptäckt av eventuella personuppgiftsincidenter. - Det finns ett behov av riktade utbildningsinsatser till verksamheterna vad avser registerförteckningar. Registerförteckningarna är en central del i hanteringen av personuppgifter, där kommunstyrelsen i egenskap av personuppgiftsansvarig bör se över styrelsens förteckningar och genomföra erforderliga kompletteringar och korrigeringar.

Revisionen önskar att kommunstyrelsen ger ett yttrande över granskningens slutsatser senast den 30 juni 2021.

Täby 30 mars 2021

På uppdrag från Täby kommuns revisorer

Lars Nordin
*Ordförande*

Malin Forsberg Helgesson
*Vice ordförande*

Bilaga: Rapport KPMG granskning av kommunens styrdokument inom ramen för GDPR