Nacka kommun

Revisionsskrivelse 2023-05-24

Revisorerna

Till: kommunstyrelsen, nämnden för arbete och försörjning, socialnämnden och utbildningsnämnden
För kännedom: Kommunfullmäktige

**Granskning av kommunens hantering av skyddade personuppgifter**
Vi revisorer har låtit EY genomföra en granskning med syftet att bedöma hur kommunen säkerställer att skyddade personuppgifter inte röjs till obehöriga samt om kommunens rutiner är ändamålsenliga och tillämpade. Detta har avsett skyddade personuppgifter för både medborgare och anställda vid kommunen. Granskningen har omfattat kommunstyrelsen, socialnämnden, utbildningsnämnden samt nämnden för arbete och försörjning. Vår övergripande bedömning är att kommunstyrelsen och de granskade nämnderna inte har säkerställt att skyddade personuppgifter röjs till obehöriga.

De olika enheterna har vidtagit diverse åtgärder i sitt löpande arbete för att förhindra röjning av skyddade personuppgifter. Detta är delvis inom det ordinarie sekretessarbetet som omfattar alla medborgare i kommunen som kan vara berörda liksom anställda i kommunen, men även riktade åtgärder. Inom ramen för det riktade arbetet har enheterna på eget initiativ och i varierande grad upprättat rutinbeskrivningar och processer för hanteringen av skyddade personuppgifter. Överlag bedömer vi att dessa är ändamålsenliga och tillämpliga men har också identifierat brister och förbättringsområden [redacted]

Kommunen har ingen övergripande styrning inom området och de granskade nämnderna har inte heller beslutat om egna styrdokument. Vår bedömning är att även med hänsyn till Nacka kommuns styrmodell är en politiskt beslutad strategisk inriktning inom området nödvändig. Varken kommunstyrelsen eller de granskade nämnderna har gjort någon uppföljning inom området avseende exempelvis enheternas arbetsrutiner, kompetensutveckling eller avvikelsehantering. Det har heller inte genomförts risk- och konsekvensanalyser avseende röjning av skyddade personuppgifter inom ramen för internkontrollarbetet. Således bedömer vi att de inte har säkerställt att ett ändamålsenligt arbete bedrivs.

Det genomförs ingen systematisk och kommunövergripande fortlöpande kompetensutveckling inom området och det finns inget särskilt utrymme för rutinförankring. Enheterna genomför själva en viss rutinförankring och kompetensutveckling genom att löpande behandla frågan internt på möten. Vår bedömning är dock att det finns ett behov av att utbilda samtliga medarbetare i hanteringen av skyddade personuppgifter specifikt och att det bör ske regelbundet i syfte att hålla kunskapen vid liv över tid. Det skulle stärka grundkunskaperna bland de medarbetare som sällan kommer i kontakt med skyddade personuppgifter och minska risken för fel som orsakas av den mänskliga faktorn. Den ser vi som den största risken, då man hanterar skyddade personuppgifter.

Avvikelser avseende skyddade personuppgifter behandlas i samma process som andra personuppgiftsincidenter. Detta inkluderar anmälning till Integritetsskyddsmyndigheten enligt lagstadgad tidsram. Då incidenterna som rör skyddade personuppgifter inte särskiljs finns risk att det blir sämre uppföljning, särskilt från nämnderna.

Vi rekommenderar kommunstyrelsen att:

- Upprätta och anta ett kommunövergripande styrdokument för hanteringen av skyddade personuppgifter. Ett sådant styrdokument bör på strategisk nivå omfatta både kommunmedborgarna och kommunens anställda.

Kommunstyrelsen och nämnderna rekommenderas att:

- Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna.
- Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet. Dessa bör vara av övergripande karaktär.
- Genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt hanteringen av skyddade personuppgifter regelbundet. Säkerställ samtidigt att enheternas arbetsrutiner för hantering av skyddade personuppgifter är förankrade hos medarbetarna, exempelvis som en del av årshjul.
- Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning.
- Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter.
- Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade personuppgifter.

Nämnden för arbete och försörjning och utbildningsnämnden rekommenderas att:

- Utvärdera riskerna att arbetet med skyddade personuppgifter påverkas negativt av att arbets- och etableringsenheten och utbildningsenheten delar kontorslokal.

Vi önskar svar på rekommendationerna från kommunstyrelsen, nämnden för arbete och försörjning, socialnämnden och utbildningsnämnden senast 2023-11-15

För revisorerna i Nacka kommun

Yvonne Wessman
Ordförande

Lars Berglund
Vice ordförande

Bilaga: Revisionsrapport 4/2023 Granskning av kommunens hantering av skyddade personuppgifter