Socialnämnden

2023-10-09
TJÄNSTESKRIVELSE
Dnr: SOCN-2023-00208

Revisionsskrivelse och revisionsrapport 4, 2023 – Granskning av kommunens hantering av skyddade personuppgifter

Yttrande till kommunfullmäktiges revisorer

Förslag till beslut

Socialnämnden antar föreslaget yttrande över revisorernas granskning av hantering av skyddade personuppgifter i Nacka kommun.

Sammanfattning

Ernst and Young, EY har på uppdrag av Nacka kommuns revisorer granskat kommunens hantering av skyddade personuppgifter. Syftet med granskningen har varit 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.

Ärendet

Innehållet i revisionsgranskningen i korthet samt revisorernas rekommendationer

Ernst and Young, EY, har på uppdrag av Nacka kommuns revisorer granskat kommunens hantering av skyddade personuppgifter. Syftet med granskningen har varit 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.

Det finns inte några särskilda uppgifter om hur många personer som har skyddade personuppgifter inom kommunens olika verksamheter. Personer som har skyddade personuppgifter kan utgöras av såväl anställda, kunder, allmänhet med mera. Även om antalet personer med skyddade personuppgifter, som är i kontakt med kommunen, inte

beräknas vara så många är det av stor vikt att varje enskilt fall hanteras säkert och korrekt för att säkerställa skyddet för den enskilde och dess anhöriga. Utifrån statistik från de två senaste åren har det skett en (1) incident per år relaterat till röjande av skyddade identiteter. Revisorernas övergripande bedömning är att kommunstyrelsen och de granskade nämnderna inte har säkerställt att skyddade personuppgifter inte röjs till obehöriga.

Socialnämnden 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.

Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter. Vid behov inkludera området i internkontrollplanerna

Möjligheten att inkludera hanteringen av skyddade personuppgifter i respektive nämnds internkontrollplan finns redan idag. Vad som ingår i respektive nämnds interkontrollplan bygger på en genomförd väsentlighets- och riskanalys inom nämndens ansvarsområde. Om socialnämnden identifierar att hanteringen av skyddade personuppgifter har ett högt riskvärde inom nämnden blir risken ett område som förs in i nämndens internkontrollplan. Socialnämnden kommer att ta detta i beaktande framöver.

Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter inom det egna ansvarsområdet

Det viktigaste är att socialnämndens verksamhetsområde utarbetar interna rutiner som är anpassade utifrån verksamhetens olika målgrupper så att skyddade personuppgifter hanteras korrekt. Kommunstyrelsen ges i och med detta förutsättningar att regelbundet följa upp att enheter och verksamheter genomför detta arbete. 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.

Redan idag pågår det i kommunen en inventering över lämpliga utbildningsinsatser som medarbetare bör genomgå dels vid nyanställning, dels som återkommande utbildningsinsatser. I detta arbete är det naturligt att bygga in hur kommunen hanterar skyddade personuppgifter. Detta är något som socialnämndens medarbetare kommer att få ta del av.

Begränsa åtkomsten till personuppgifterna genom strikt behörighetstilldelning
Styrdokumentet ”Så här gör vi i Nacka – IT-säkerhet” anger ett flertal krav på hur åtkomst och behörigheter ska hanteras. Informationsinsatser för att höja medvetandet om de krav som ställs i detta dokument planeras till hösten 2023. Behörighetsstyrningen i verksamhetssystemet Combine har under hösten 2023 setts över och omstrukturerats. Detta har inneburit att behörighetsstrukturen har en tydligare organisationstillhörighet för att säkerställa att medarbetare ges behörighet till rätt information i systemet. Ett förtydligande gällande krav på att genom risk- och konsekvensanalys finna en lämplig nivå på en strikt behörighetsstyrning för varje behandling av skyddade personuppgifter inom berörda verksamheter bör förtydligas i det kommungemensamma styrdokument som är planerat till hösten 2023.

Genomföra kontroller av användarloggar som en organisatorisk säkerhetsåtgärd för att minska riskerna för röjning av skyddade personuppgifter
Detta genomförs inom socialnämndens verksamheter i samband med varje tertialrapport och det bedöms vara tillräckligt för att säkerställa att eventuella åtgärder utifrån riskerna för röjning av personuppgifter hanteras adekvat. Detta följs även upp som ett område i socialnämndens internkontrollplan för 2023.

Säkerställa möjligheten att systematiskt följa upp avvikelser avseende skyddade Personuppgifter
Detta genomförs inom socialnämndens verksamheter i och med att personuppgiftsincidenter utreds på enheterna och åtgärdsplaner tas fram. De rapporteras vidare till socialnämnden löpande i samband med tertialrapporter. Lärande utifrån detta sker på enheterna då vi lyfter avvikelserna i aktuell grupp och vid behov lyfter det även på enhetsnivå.

Ekonomiska konsekvenser
Förslaget till beslut om yttrande medför inga ekonomiska konsekvenser.

Konsekvenser för barn
Förslaget till beslut om yttrande medför inga direkta konsekvenser för barn. En god hantering av skyddade personuppgifter är av vikt för alla enskilda som är i behov av skyddade personuppgifter, däribland barn och unga.

Bilagor

Bilaga 1. Revisionsskrivelse 2023-05-24 Granskning av kommunens hantering av skyddade personuppgifter

Bilaga 2. Rapport 4, 2023 Granskning av kommunens hantering av skyddade personuppgifter

Bilaga 3. Förslag till yttrande

Karin Kollberg
Social- och äldredirektör
Stadsledningskontoret

Pernilla Majlöv
Kvalitetsutvecklare, Kvalitet IFO
Barn- och familjeenheten