Sundbybergs stads revisorer
Granskningsrapport 12/2022-2

Svar på revisorernas granskning av stadens hantering av skyddade personuppgifter

Nämndens kommentarer

Social- och arbetsmarknadsnämnden lämnar följande kommentarer som svar på revisionens rekommendationer:

1. **Upprätta risk- och konsekvensanalyser avseende hanteringen av skyddade personuppgifter och vid behov låt inkludera i internkontrollplanerna.**

   Nämndens kommentar: Nämndens risk– och väsentlighetsanalys för 2022 innefattar en risk kopplat till hanteringen av integritetskänslig information, dock saknas en specifik analys avseende hanteringen av skyddade personuppgifter. Nämnden kommer, i enlighet med revisionens rekommendation, att analysera hanteringen av skyddade personuppgifter inom ramen för nämndens risk- och väsentlighetsanalys med start 2023. En bedömning kommer även att göras om behovet finns att lyfta in risken i nämndens internkontrollplan.

2. **Upprätta och anta styrande dokument för hanteringen av skyddade personuppgifter.**

   Nämndens kommentar: Nämnden bedömer att området är väl reglerat och att det därmed inte behövs några riktlinjer/styrande dokument för social- och arbetsmarknadsnämndens arbete med skyddade personuppgifter. Däremot finns behov av att upprätta tillämpningsanvisningar och rutiner som stöd i det dagliga arbetet. Ett arbete pågår inom sektorn med att ta fram en skriftlig rutin för hanteringen av skyddade personuppgifter. Arbetet är i slutfasen. En plan för implementering kommer att utformas där utbildning till medarbetare ingår.

3. **Överväga att genomföra obligatoriska utbildningar för samtlig personal i tillämpning av styrande dokument samt praktisk hantering av vardagssituationer där skyddade personuppgifter förekommer.**

   Nämndens kommentar: Nämnden ser, i enlighet med revisionens förslag, att det finns ett behov av att utbilda nämndens medarbetare avseende hanteringen av skyddade personuppgifter. Samtliga enheter kommer att utbildas när rutinen för hantering av skyddade personuppgifter är på plats.

   När det gäller återkommande utbildning skulle denna del exempelvis kunna läggas till i den befintliga introduktionsutbildningen i handläggning och dokumentation som hålls för nya handläggare. Alternativt att en utbildning om skyddade personuppgifter läggs till som en återkommande utbildning bland sektorns internutbildningar. Frågan kommer att tas upp för övervägande/beslut i sektorns ledningsgrupp.

4. **Genomföra penetrationstester och systematiska loggkontroller av IT-system och rutiner för att identifiera sårbarheter och skadekonsekvenser vid intrång samt att obehöriga inte kan få tillgång till skyddade personuppgifter.**

   Nämndens kommentar: Loggkontroller genomförs kvartalsvis enligt framtagen rutin med syfte att kontrollera att personal inte tagit del av uppgifter i systemet som de inte är behöriga till. Kontrollerna görs i form av stickprov av loggarna i sektorns verksamhetssystem. I dagsläget görs inga särskilda kontroller av ärenden med skyddade personuppgifter. Systemförvaltare, kommer utifrån revisonens rekommendationer, att se över möjligheten att lägga till regelbundna kontroller av loggar för ärenden med skyddade personuppgifter. Även behörigheterna i systemet kommer att ses över. De penetrationstester som föreslås genomförs redan av verksamhetssystemets leverantör.

5. **Stärka avvikelsehanteringen och uppföljningen avseende skyddade personuppgifter.**

   Nämndens kommentar:
   Nämnden har kartlagda processer för avvikelsehantering i kvalitetsledningssystemet i Stratsys. För att ytterligare uppmärksamma ställningstaganden kring personuppgiftsincidenter kommer en sådan fråga att läggas in i den befintliga avvikelseprocessen med hänvisning till stadens rutin för rapportering av personuppgiftsincidenter.

   När det gäller analys av personuppgiftsincidenter, och brister i hanteringen av skyddade personuppgifter, genomförs i dagsläget ingen sammanställning/analys på aggregerad nivå. Nämnden planerar att se över möjligheten att kategorisera rapporterade avvikelser på ett bättre sätt för att möjliggöra en analys av inkomna brister kopplade till hanteringen av skyddade personuppgifter.

   Avvikelser/brister som medför konsekvenser för brukare som är aktuella inom socialtjänsten ska rapporteras och utredas enligt lex Sarah. Det inkluderar även avvikelser i hanteringen av skyddade personuppgifter. Arbetet med lex Sarah syftar till att analysera bakomliggande orsaker och utifrån det vidta relevanta åtgärder för att komma till rätta med bristerna. En årlig sammanställning/analys görs inom sektorn utifrån de avvikelser som har rapporterats enligt lex Sarah.

Sammanfattande kommentar
Revisionens rekommendationer bedöms relevanta för social- och arbetsmarknadsnämnden. Åtgärder och överväganden kommer utifrån rekommendationerna att genomföras för att ytterligare stärka arbetet med skyddade personuppgifter.

Å social- och arbetsmarknadsnämndens vägnar

Marie Lundman Völker (S)
Social- och arbetsmarknadsnämndens ordförande