

Granskning av enheten för personligt stöds arbete med informationssäkerhet och efterlevnad av dataskyddsförordningen

Förvaltningens informationssäkerhetssamordnare och arkivansvarig samt nämndens dataskyddsombud har den 30 september 2019 gjort en översiktlig granskning av arbetet med informationssäkerhet och efterlevnad av dataskyddsförordningen inom enheten för personligt stöd. Granskningen var föraviserad. Den övergripande revisionsfrågan har varit: Har verksamheten ett ändamålsenligt arbete med informationssäkerhet och behandlingen av personuppgifter?

Efter genomförd granskning bedömer vi att verksamheten delvis uppfyller kontrollmålen. Förbättringsområden finns för att nå ett fullt ut tillfredsställande och ändamålsenligt arbete. Därtill bör verksamheten följa de rekommendationer som läggs fram i rapporten för att säkerställa ett fortsatt effektivt arbete inom området.

Introduktion och utbildning

Enhetschefen har en dokumenterad rutin för hur introduktion/utbildning sker av nyanställda. All personal är timanställd och det är låg personalomsättning. Frågor kopplade till informationssäkerhet och GDPR lyfts som regel inte på personalmöten. Enhetschefen känner inte till att medarbetarna ska ha genomgått stadens e-utbildning om GDPR.

Föreslagna aktiviteter

- Utifrån informationen på intranätet om GDPR och informationssäkerhet bör enheten implementera rutiner inom sin egen verksamhet.
- Sprida stadens riktlinjer för informationssäkerhet bland medarbetare.
- Uppmana alla medarbetare att genomföra stadens e-utbildning i GDPR samt verifiera att så har skett.

Användaradministration och behörigheter

Enhetschefen och den biträdande enhetschefen ansvarar för användaradministration i systemet AiAi och i Paraplyet. Det finns ingen dokumenterad rutin för hur behörigheter hålls korrekta och uppdaterade.

Föreslagna aktiviteter

- Säkerställa att alla behörighetsgrupper är korrekta och att alla medarbetare har korrekta behörigheter.
- Ta fram en rutin för att lägga till, ändra och ta bort behörigheter vid förändring av anställningsförhållanden.

Lösenord och pinkoder

Hos varje brukare finns en arbetstelefon för medarbetarna. Varje telefon har en egen pinkod som är känd bland behöriga medarbetare. Av verksamhetens art framgår att det är nödvändigt för de anställda att PIN-koder och lösenord till de telefoner som finns hos brukarna är kända bland de medarbetare som arbetar hos brukaren.

Identifiering av risker

Det är oklart om det finns en rutin för att hantera identifierade risker. Ingen riskanalys eller informationsklassning gjordes innan systemet AiAi sattes i bruk. Enhetschefen har tidigare fått information om förvaltningens rutin om hur personuppgiftsincidenter ska hanteras men rutinen är inte vidareförmedlad till medarbetarna. Enhetschefen känner inte till att någon personuppgiftsincident ska ha inträffat.

Föreslagna aktiviteter

- Genomföra riskanalyser vid förändrade arbetsätt.
- Tillse att medarbetare har kännedom om förvaltningens rutiner för informationssäkerhetsincidenter och personuppgiftsincidenter.

Avtal

Enheten ingår som regel inga egna avtal. För två år sedan tecknade enheten avtal med Kaustik AB för systemet AiAi. Verksamhetsutvecklaren inom avdelningen för egen regi håller på att teckna ett personuppgiftsbiträdesavtal med leverantören.

Enheten har lämnat in en avtalsinventering till upphandlingssamordnaren och dataskyddsombudet.

Vid uppföljningen tas vikten upp av att alla avtal lämnas till registratören för diarieföring.

Hantering, arkivering och gallring

Enhetens dokumenthantering bedöms, utifrån vad som framkommit vid granskningen, vara god.

Rekommendation

Enheten rekommenderas att vid inventeringen av personuppgiftsbehandlingar säkerställa att personuppgifter gallras på ett korrekt sätt utifrån stadens hanteringsanvisningar och i enlighet med dataskyddsförordningens bestämmelser.

Övrigt

Enheten har inte färdigställt sin inventering och registrering av personuppgiftsbehandlingar. Enheten behöver också genomföra riskanalyser och i vissa fall konsekvensbedömningar utifrån personuppgiftsbehandlingarna. Enheten rekommenderas att under arbetet säkerställa att personuppgifter gallras på ett korrekt sätt utifrån stadens hanteringsanvisningar och i enlighet med dataskyddsförordningens bestämmelser.

Enheten rekommenderas också säkerställa att det finns gallringsrutiner för dokument som sparas utanför verksamhetssystem.

Erica Wangenheim
Dataskyddsombud

Mats Österlund
Informationssäkerhetssamordnare

Jenny Valentin
Arkivansvarig