Granskning av enheten för barn och familjs arbete med informationssäkerhet och efterlevnad av dataskyddsförordningen

Nämndens dataskyddsombud och förvaltningens informationssäkerhetssamordnare har den 22 maj 2019 granskat enheten för barn och familjs arbete med informationssäkerhet och efterlevnad av dataskyddsförordningen. Granskningen var föraviserad. Den övergripande revisionsfrågan har varit: Har enheten ett ändamålsenligt arbete med informationssäkerhet och behandlingen av personuppgifter?

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

Introduktion och utbildning

Tidigare enhetschef har använt en checklista för introduktion av nyanställda som enheten själv har tagit fram. Det finns behov av en generell checklista för introduktion till arbete i förvaltningshuset. Vi skickar den frågan vidare till HR och extern service.

Kännedomen om informationssäkerhet och GDPR är god men kunskapen är generellt sett låg. Frågorna diskuteras som regel inte vid arbetsplatsträffar. Enhetschefen har tidigare påtalat vikten att alla medarbetare ska gå stadens e-utbildning om GDPR, men man har inte kontrollerat utfallet.

Föreslagna aktiviteter

- Utifrån informationen på intranätet om GDPR och informationssäkerhet bör enheten ta fram anvisningar för sin egen verksamhet.
- Sprida stadens riktlinjer för informationssäkerhet bland medarbetare.
- Verifiera att alla medarbetare har genomgått stadens e-utbildning i GDPR.

Älvsjö stadsdelsnämnd

Älvsjö stationsgata 21
12521 Älvsjö
Telefon 08-50821008
alvsjo@stockholm.se
-

Användaradministration och behörigheter

Det finns en gemensam behörighetsgrupp för alla olika funktioner inom enheten dit samtlig personal ska ha behörighet. I stort är det tänkt att där endast ska lagras policydokument och process- och rutinbeskrivningar. Enheten för även en lista över inkommen information om barn/unga (förhandsbedömningsfil) som lagras i den mappen. Gallringsrutiner saknas för listan. Vi föreslår att listan flyttas till en egen gruppdisk dit endast enhetschef och biträdande enhetschef har behörighet.

Föreslagna aktiviteter

- Säkerställa att enheten har en egen paraplyadministratör.
- Säkerställa att alla behörighetsgrupper är korrekta och att alla medarbetare har korrekta behörigheter.
- Se över gallringsrutiner över dokument som sparas utanför verksamhetssystem.
- Ta fram en rutin för att lägga till, ändra och ta bort behörigheter vid förändring av anställningsförhållanden.
- Genomföra och dokumentera loggkontroller i Paraplysystemet.

Rekommendation

I övrigt rekommenderar vi att enheten tar fram mallar för hur tjänsteutlåtanden och utredningar ska göras eftersom det vid mötet framkom att medarbetare använder varandras handlingar med personuppgifter som mallar.

Lösenord och pinkoder

Enheten redogör för att lösenord och pinkoder hanteras olika bland medarbetarna. I de förvaltningsövergripande rutinerna framgår bland annat vad som gäller i fråga om pinkod för tjänstekort, smartphone och användarkonto.

Föreslagna aktiviteter

- Tillse att medarbetare har kännedom om förvaltningens rutiner vad gäller lösenord och pinkoder.
- Ta fram rutin för att fabriksåterställa smartphones/iPads vid avslutad anställning.

Identifiering av risker

Riskanalyser genomförs av enhetschefen. Det är oklart om det finns en rutin för att hantera identifierade risker. Enheten har en dokumenterad personuppgiftsincident i systemet IA. Det är oklart om planerade åtgärder som framkommer i incidentrapporteringen har följts upp.

Föreslagna aktiviteter

- Tillse att medarbetare har kännedom om förvaltningens rutiner för informationssäkerhetsincidenter och personuppgiftsincidenter.
- Följa upp att åtgärder vidtagits efter inträffade incidenter.

Avtal

I de fall enheten tecknar avtal med ett personuppgiftsbiträde så tecknas även personuppgiftsbiträdesavtal (stadens mall). Enheten tecknar inte personuppgiftsbiträdesavtal vid ramavtalsavrop. Det råder en osäkerhet när personuppgiftsbiträdesavtal ska tecknas på nämndnivå när avtalet är centralt. Stadens dataskyddsombud samverkar i frågan.

Föreslagna aktiviteter

- Teckna personuppgiftsbiträdesavtal med samtliga motparter som behandlar personuppgifter tills frågan är utredd inom staden.

Registerutdrag

Som regel vänder sig enskilda direkt till sin socialsekreterare när de begär ut information. Enheten känner inte till att någon begäran om registerutdrag i enlighet med GDPR har kommit in.

Hantering, arkivering och gallring

Enheten har rutiner för hur avslutade ärenden ska hanteras.

Övrigt

Vid kontrollen har vi genomfört stickprovskontroller i kontorsutrymmen. Utifrån den bedömer vi att informationshanteringen är god men med anmärkningen att enheten behöver tillse att alla sekretesskåp är låsta i obemannade rum.

Vid kontrollen noterade vi också att plan 1 saknar en sekretesstunna och en allmän skräptunna i postrummet. Bristen har lyfts med vaktmästaren som ska åtgärda detta.

Erica Wangenheim	Mats Österlund
Dataskyddsombud	Informationssäkerhetssamordnare