Uppföljning av personuppgiftsincidenter

Nämndens dataskyddsombud har följt upp hur personuppgifts-incidenter har hanterats inom förvaltningen för att minimera risken för att liknande incidenter inträffar på nytt.

Uppföljningen visar att förvaltningen har påbörjat ett systematiskt arbete för att hantera inträffade personuppgiftsincidenter. Uppföljningen visar ett fortsatt behov av att förankra rutinen för hantering av personuppgiftsincidenter inom verksamheterna samt behov av att tydliggöra dess tillämpning i förhållande till andra rutiner.

Rapporterade personuppgiftsincidenter

År 2018 togs en förvaltningsövergripande rutin fram för hur inträffade personuppgiftsincidenter ska hanteras. Syftet med rutinen var att skapa enhetlighet i förvaltningens hantering av personuppgiftsincidenter och se till att Datainspektionen i tid informeras om vissa incidenter.

Denna uppföljning gäller incidenter som har rapporterats under 2018 fram till den 18 november 2019 (totalt 10 stycken). De handlar framförallt om röjda personuppgifter i samband med mejlutskick till fel mottagare eller röjda personuppgifter vid utskrift av dokument som inte har hämtats från skrivaren.

I två fall (som totalt genererat tre rapporteringar) har incidenterna varit av stadsövergripande karaktär, det vill säga där ett flertal nämnder/förvaltningar har drabbats, och som har berott på tekniska fel hos leverantörerna. Händelserna har också varit av sådan allvarlig karaktär att Datainspektionen har blivit informerad. Den ena incidenten (Tieto-incidenten) föranledde också att en särskild utredning inleddes då förvaltningen, som en följd av incidenten, också identifierade vissa interna administrativa brister. Utredningen utmynnade också i en lex Sarah.

Uppföljningen

En uppföljning av personuppgiftsincidenter har gjorts per mejl till de enheter som har avlämnat rapporter i IA. Totalt gäller det fem enheter (enheten för barn och familj, enheten för äldre, enheten för ekonomiskt bistånd och arbetsmarknad, Älvsjö hemtjänst och

Älvsjö stadsdelsnämnd

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

förskoleenhet 3). Rapportering har också gjorts av dataskyddsombudet (stadsdelsdirektörens stab). Tre enheter har lämnat svar. Två enheter har fått påminnelse om att besvara ställda frågor men har inte återkopplat.

Resultat av uppföljningen

Uppföljningen visar att förvaltningen har påbörjat ett systematiskt arbete för att hantera inträffade personuppgiftsincidenter. I och med förvaltningens byte av IT-miljö används numera funktionen Pullprint som innebär att utskrifter endast kan göras med tjänstekort vid skrivaren. Medarbetare behöver därmed inte göra ett aktivt val att skriva ut med Säker utskrift. Därmed har risken för att dokument blir liggande i skrivare minskat.

I de fall incidenter beror på mänskliga faktorn (handhavandefel) i samband med mejlutskick visar uppföljningen att förvaltningen regelbundet understryker vikten av att vidta försiktighet i samband med att mejl skickas som innehåller skyddsvärd information. Inom förvaltningen finns också en rutin att i möjligaste mån använda pseudonymiserade (kodade) personuppgifter i mejl. Uppföljningen visar inte på några brister i den rutinefterlevnaden.

Uppföljningen visar att det finns en osäkerhet kring rapporteringen av personuppgiftsincidenter i IA. I vissa fall kan en incident röra flera andra typer av incidenter än bara personuppgiftsincidenter. Det behöver därför förtydligas hur rapporteringen ska förhålla sig till andra enhetsspecifika rutiner, exempelvis avvikelsehantering och lex Sarah-rapportering. Dokumentationen i IA är också bristfällig då de frågor som framgår i rutinens bilagda checklista inte besvaras utförligt.

Jag bedömer att det finns personuppgiftsincidenter som har inträffat men som inte har rapporterats. Förvaltningen behöver fortsätta arbeta för en ”rapporterande kultur” – där man vågar rapportera incidenter i syfte att utveckla sin förmåga att förebygga, upptäcka och hantera risker. Jag rekommenderar också att förvaltningen löpande dokumenterar vidtagna åtgärder som styrker egenkontroller och lärdomar av tidigare incidenter. Det är en viktig aspekt för att uppnå en god säkerhetskultur.

Dataskyddsombudet kommer att se över förvaltningens rutin för hantering av personuppgiftsincidenter. Vidare kommer dataskydds-ombudet föra dialog med IA-ansvarig om möjligheten att införa kontrollfrågor i IA-systemet i syfte att rationalisera rapporterings-förfarandet. Med anledning av brottsdatalagens bestämmelser om incidentrapportering kommer dataskyddsombudet även föreslå vissa anpassningar i systemet.

Erica Wangenheim
Dataskyddsombud