KOMMUNSTYRELSENS FÖRVALTNING
DATASKYDDSOMBUD

Rutin för hantering av personuppgiftsincident

OMFATTNING

Riktlinjerna gäller för samtliga styrelser/nämnder i Sala kommun.

Syfte

Dessa riktlinjer syftar till att skapa en systematisk och samlad rapportering av personuppgiftsincidenter enligt krav i gällande dataskyddsförordning.

VAD ÄR EN PERSONUPPGIFTSINCIDENT?

Enligt en särskild definition i dataskyddsförordningen definieras begreppet personuppgiftsincident som en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som behandlas. Det kan också vara fråga om en personuppgiftsincident om en säkerhetsincident leder till obehörigt röjande av eller obehörig åtkomst till de behandlade personuppgifterna.

Exempel på incidenter kan vara

- Någon har kommit över ett lösenord som gör att den skulle kunna logga in i system som behandlar personuppgifter.
- Ett mail med känsligt eller extra skyddsvärda personuppgifter skickas till fel mottagare.
- Ett glömt papper i skrivare som innehåller uppgifter om namn och sjukdomstillstånd.
- En dator har fått skadlig kod som gör att obehörig skulle kunna komma åt personuppgifter.

ANMÄLAN OCH RAPPORTERING

När det har inträffat en personuppgiftsincident ska först och främst sannolikheten och allvaret, och den därmed följande risken för människors rättigheter och friheter fastställas. Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade måste incidenten anmälas till Datainspektionen. Men om det är osannolikt att en personuppgiftsincident medför risker behöver någon anmälan inte göras. De risker man tänker på är till exempel att enskilda förlorar kontrollen över sina uppgifter eller att deras rättigheter inskränks, att man utsätts för diskriminering, identitetsstöld eller bedrägeri, finansiell förlust, skadlig ryktesspridning samt brott mot sekretess eller tystnadsplikt.

Riskbedömningen och beslutet att anmäla eller icke anmäla ska motiveras och dokumenteras.

Kommunstyrelsens förvaltning
Dataskyddsombud

Anmälan till Datainspektionen **ska** göras inom 72 timmar från det att man upptäckt vad som hänt. Därför är det viktigt att incidenter rapporteras så snart som möjligt efter upptäckt. Alla personuppgiftsincidenter ska rapporteras. Det är viktigt att rapportera om en incident så att en riskbedömning kan göras och beslut kan fattas om incidenten ska anmälas till Datainspektionen eller ej. Rapportering av incidenter görs via självservicetjänsten Personuppgiftsincident på Sala kommuns hemsida.

Om det inte är möjligt att vid anmälan lämna all information inom 72 timmar kan man dela upp det och lämna uppgifter vid olika tillfällen allt eftersom det blir möjligt. Hinner man inte göra anmälan alls inom 72 timmar ska Datainspektionen ändå informeras och skälen ska anges för förseningen.

ANSVAR OCH ROLLER

Den personuppgiftsansvarige ansvarar för att anmälan görs, det vill säga den nämnd, myndighet eller annan organisation som bestämmer ändamål och medel för behandlingen. Riskbedömning och anmälan till Datainspektionen görs av kommunens dataskyddsombud.

Varje medarbetare ansvarar för att rapportera risk för, misstanke om eller inträffande av en personuppgiftsincident. Rutiner ska finnas i varje verksamhet för hur rapportering görs.

I de fall ett personuppgiftsbiträde har anlitats finns också en skyldighet för biträdet att uppmärksamma den personuppgiftsansvarige på en säkerhetsincident så fort den upptäckts. Detta ska framgå i de personuppgiftsbiträdesavtal som upprättas.

Under vissa omständigheter är den personuppgiftsansvarige skyldig att informera de personer vars uppgifter berörs av incidenten. Den informationen ska minst omfatta:

- Klar och tydlig beskrivning av orsaken till personuppgiftsincidenten,
- Namn och kontaktuppgifter till dataskyddsombudet,
- Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten,
- Beskrivning av vad vi har gjort, eller tänker göra, för att hantera personuppgiftsincidenten,
- I förkommande fall: Beskrivning av vad vi har gjort för att mildra eventuella negativa effekter

När Datainspektionen blir informerad om en incident kan myndigheten fatta beslut om att den personuppgiftsansvarige måste informera de registrerade eller att det inte är nödvändigt. Om de registrerade ska informeras kan Datainspektionen komma att ge råd om hur detta ska ske.