Personuppgiftsincident

Rutin för identifiering och hantering av personuppgiftsincidenter

Dokumenttyp: Rutin

Antaget av: Kommundirektör

Antagen: 2 juli 2018

Giltighetstid: Tillsvidare

Ronneby kommun

Ronneby.se

Diarienummer: dnr KS 2018-000415, dnr KS 2023/225

Ansvarig för dokumentet: Dataskyddsombudet

Tidpunkt för senaste aktualitetsprövning: 31 mars 2023

Tidpunkt för senaste revidering: 31 mars 2023

Relaterade styrdokument: Informationssäkerhetspolicy, Dataskyddspolicy

Sökord: GDPR, incident, förlorad information

1. Inledande bestämmelse

Denna rutin beskriver vad en personuppgiftsincident är samt hur Ronneby kommun ska hantera en sådan incident.

2. Definition av en personuppgiftsincident

En personuppgiftsincident uppstår när de personuppgifter vi behandlar;

- Medvetet, omedvetet eller olagligt förstörs, förvanskas, försvinner eller ändras.
- När någon som inte har behörig tillgång till personuppgifterna får tillgång eller åtkomst till dessa (obehörig åtkomst).
- När personuppgifter på ett felaktigt sätt sprids eller publiceras internt eller externt (obehörigt röjande).

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har blivit förstörda, gått förlorade eller kommit i orätta händer. Det spelar ingen roll om det har skett oavsiktligt eller med avsikt. I båda fallen är det personuppgiftsincidenter.

3. Exempel på personuppgiftsincident

Att en personuppgiftsincident har inträffat är inte alltid tydligt. En personuppgiftsincident kan ha inträffat om någon kan ha kommit åt eller tagit del av uppgifter denne inte har behörighet till. Några exempel.

- Någon har kommit över ett lösenord som gör att vederbörande 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.
- Ett USB-minne med personuppgifter kommer på avvägar.
- En mobiltelefon med eller utan mailkonto hamnar i orätta händer.

4. Vem ansvarar för att rapportera en personuppgiftsincident

Samtliga anställda och förtroendevalda inom kommunen har ett snavsr att rapportera till ansvarig chef eller gruppledare under följande förutsättningar

- anställd/förtroendevald vet att det inträffat en incident
- anställd/förtroendevald misstämker att det har inträffat en incident
- anställd förtroendevald ser en risk för att det ska inträffa en incident

Alla personuppgiftsincidenter ska rapporteras till närmaste chef eller gruppledare så snart som möjligt efter upptäckt. Det gäller även om incidenten hunnit bli åtgärdad. Vid osäkerhet så är det alltid bättre att rapportera till närmaste chef.

5. Anmälan till Integritetsskyddsmyndigheten (IMY)?

Ansvarig chef inom den verkasmhet som incidenten inträffade ansvarar för att personuppgiftsincidenter rapporteras till IMY. Inte alla incidenter behöver anmälas, ansvarig chef bör därför rådgöra med dataskyddsombudet snarast möjligt.

Om det är en sådan incident som ska rapporteras till datainspektionen ska detta ske inom 72 timmar från upptäckt. *Om du ansvarar för att rapportera en incident* är det därför viktigt att du gör det omedelbart då du upptäcker den.

Ansvarig chef avgör huruvida personuppgiftsincidenten ska anmälas till IMY. Dataskyddsombudet ska involveras vid bedömningen. Vid behov ska Kommundirektör och Kommunjurist också involveras för att avgöra om incidenten ska rapporteras till IMY eller om det räcker med att incidenten dokumenteras och arkiveras.

5.1. Blankett för anmälan

Integritetsskyddsmyndigheten har tagit fram en blankett för anmälan av personuppgiftsincidenter. Den hålles tillgänglig på deras hemsida, sök efter *personuppgiftsincident* på deras hemsida så hittar du blanketten.

6. Vem ansvarar för att informera de registrerade

I vissa fall måste kommunen informera de registrerade att det inträffat en personuppgiftsincident. Detta gäller om personuppgiftsincidenten kan leda till en hög risk för de registrerades rättigheter och friheter. Huruvida de registrerade måste informeras avgörs från fall till fall.
Ansvarig chef är den som, efter samråd med dataskyddsombudet, är den som ska informera de registrerade.

7. Revidering

Rutinen är beslutad av kommundirektör. Rutinen ska revideras vid behov, men minst en gång per mandatperiod. Vid antagande av ny rutin upphör denna rutin att gälla. Dataskyddsombudet ansvarar för att rutinen revideras.