

## **Policy för hantering av personuppgiftsincident**

Vad är en personuppgiftsincident?

En personuppgiftsincident definieras enligt förordningen som: En säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring eller till obehörigt röjande av eller obehörig åtkomst till de personuppgifter som överförts, lagrats eller på annat sätt behandlats.

### **Handlingsplan vid personuppgiftsincident**

#### **Misstanke**

om styrelsemedlem eller anställd hos FRG misstänker att personuppgiftsincident har inträffat så ska denna informera kanslichef och sedan själv eller tillsammans med chefen utreda huruvida personuppgiftsincident har inträffat.

#### **Bekräftad incident**

Om styrelsemedlem eller anställd hos FRG får kännedom om att personuppgiftsincident har inträffat ska denna informera kanslichefen och sedan själv eller tillsammans med chefen utreda huruvida personuppgiftsincidenten utgör risk för fysiska personers rättigheter och friheter.

#### **Risk för fysiska personers rättigheter och friheter**

Vid personuppgiftsincident som utgör risk för fysiska personers rättigheter och friheter ska den identifierande utan onödigt dröjsmål, dock inte senare än 72 timmar anmäla incidenten till tillsynsmyndigheten. Den identifierande ska informera den registrerade.

#### **Ingen risk för fysiska personers rättigheter och friheter**

Vid personuppgiftsincident som inte utgör risk för fysiska personers rättigheter och friheter ska den identifierande fylla i en incidentrapport.

#### **Dokumentation av personuppgiftsincidenter**

Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och vidtagna åtgärder. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av denna artikel.

#### **Personuppgiftsbiträde**

I de fall som FRG är personuppgiftsbiträde så ska FRG underrätta den personuppgiftsansvarige utan onödigt dröjsmål om att personuppgiftsincident har inträffat och om så inte är möjligt ska FRG anmäla incidenten till tillsynsmyndigheten.

## **Anmälan till tillsynsmyndighet**

En anmälan om personuppgiftsincident ska innehålla:

- 1 Beskrivning av personuppgiftsincidentens art, vilken typ av uppgifter, antalet uppgifter och antalet registrerade som berörs.
- 2 Namn och kontaktuppgifter till dataskyddsombudet.(Om sådan finns)
- 3 Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
- 4 Beskrivning av de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten.

## Incidentrapport

Datum och tid då incidenten upptäcktes	
Beskrivning av incidenten	
Beskrivning av vidtagna, eller föreslagna åtgärder, för att åtgärda, eller mildra effekterna av incidenten	
Datum och tid då incidenten kom till personuppgiftsansvariges kännedom	
Beskrivning av vilka som är berörda	
Antal registrerade som berörs	
Kategori av personuppgifter som berörs	
Antal berörda personuppgiftsposter	
Beskrivning av sannolika konsekvenserna av personuppgiftsincidenten	
Utgör personuppgiftsincidenten risk för fysiska personers rättigheter och friheter? (Ja/Nej)	
Datum och tid då registrerad informerades om incidenten	
Datum och tid då Datainspektionen informerades om incidenten	
Namn och kontaktuppgifter för personuppgiftsombud	