# **RUTIN för personuppgiftsincidenter**

**Bakgrund och syfte**

Företaget/Organisationen ska se till att de följer dataskyddsförordningen (GDPR) och arbetar förebyggande med att undvika personuppgiftsincidenter. Denna rutin syftar till att förtydliga vilka åtgärder som ska tas i samband med en incident.

**Vad är en personuppgiftsincident?**

En personuppgiftsincident är en händelse som kan innebära risker för människors fri- och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter eller att rättigheterna inskränks. Till exempel:

* diskriminering, identitetsstöld, bedrägeri, skadlig ryktesspridning
* finansiell förlust
* brott mot sekretess eller tystnadsplikt

En personuppgiftsincident har till exempel inträffat om uppgifter om en eller flera registrerade personer har

* blivit förstörda
* gått förlorade på annat sätt
* kommit i orätta händer

Det spelar ingen roll om händelsen har skett oavsiktligt eller med avsikt. I båda fallen kan det vara personuppgiftsincidenter.

**Exempel på personuppgiftsincidenter**

* Någon obehörig part har fått tillgång till personuppgifter, till exempel om någon har skickat personuppgifter till mottagare som inte skulle ha uppgifterna.
* Datorer som innehåller personuppgifter har förlorats eller stulits.
* Någon har ändrat personuppgifter utan tillstånd.
* Personuppgifter är inte tillgängliga för den som behöver dem, och det leder till negativa effekter för de registrerade personerna.

**Anmäla personuppgiftsincident till Datainspektionen**Företaget/Organisationen har en skyldighet att anmäla en personuppgiftsincident till Datainspektionen inom 72 timmar från att incidenten upptäcktes. Anmälan sker via Datainspektionens e-tjänst. Anmälan syftar till att göra det möjligt för Datainspektionen att se och bevaka vilka åtgärder som vidtas för att motverka negativa effekter av det inträffade. Om det blir nödvändigt kan Datainspektionen också komma att utöva sina tillsynsbefogenheter för att få den som är ansvarig för behandlingen att vidta nödvändiga åtgärder.

**Undantag från anmälningsskyldighet**  
Anmälningsskyldigheten gäller inte om det är osannolikt att personuppgiftsincidenten medför en risk för fysiska personers rättigheter och friheter. Det är Företaget/Organisationen, enligt ansvarsprincipen, som måste påvisa att det är osannolikt att personuppgiftsincidenten kommer att medföra en risk för fysiska personers rättigheter och friheter.

**Konsekvenser**  
En personuppgiftsincident som inte snabbt åtgärdas på lämpligt sätt kan för fysiska personer leda till fysisk, materiell eller immateriell skada, såsom förlust av kontrollen över de egna personuppgifterna eller till begränsning av deras rättigheter, diskriminering, identitetsstöld eller bedrägeri, ekonomisk förlust, obehörigt hävande av pseudonymisering, skadat anseende, förlust av konfidentialitet när det gäller personuppgifter som omfattas av tystnadsplikt, eller till annan ekonomisk eller social nackdel för den berörda fysiska personen.

**Vem ska göra anmälan**?  
Företaget/Organisationen är i egenskap av personuppgiftsansvarig ansvarig för att upprätta anmälan. Vi ska varje verksamhetsår utse en person som är ansvarig för att upprätta en anmälan vid en eventuell personuppgiftsincident.

**Undvik sanktionsavgifter**

Om vi inte rapporterar en personuppgiftsincident kan det innebära en överträdelse av dataskyddsförordningen, vilket kan leda till att föreningen måste betala sanktionsavgifter.

**Informera de registrerade**

Om personuppgiftsincidenten är allvarlig ska vi skyndsamt även informera de registrerade om personuppgiftsincidenten. Detta gäller alltså om det är sannolikt att personuppgiftsincidenten leder till en hög risk för att fysiska personers rättigheter och friheter inskränks.

Företaget/Organisationen ska bedöma både allvarligheten av den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha och sannolikheten för att detta inträffar.

* + - Hur allvarliga kan konsekvenserna bli?
    - Hur sannolikt är det att enskilda personer drabbas?

Om personuppgiftsincidenten är allvarlig är risken högre. Om sannolikheten för konsekvenser är stor är risken också högre. När risken är hög ska vi genast informera de personer som har drabbats, särskilt om det finns ett behov av att mildra en omedelbar risk för skador. En av huvudorsakerna är att vi ska kunna hjälpa individerna att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

**Information till de registrerade**

Företaget/Organisationens information till de registrerade ska uppfylla Datainspektionens minimikrav:

* Tydlig och klar beskrivning av orsaken till personuppgiftsincidenten.
* Namn och kontaktuppgifter till vår kontaktperson i ärendet eller till en annan kontakt som är insatt i frågan och kan svara på frågor.
* Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
* Beskrivning vad vi har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
* I förekommande fall: Beskriv vad vi har gjort för att mildra eventuella negativa effekter.

**Dokumentation**

Företaget/Organisationen ska dokumentera alla personuppgiftsincidenter, omständigheterna, dess effekter och de åtgärder som tagits till. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av vår anmälningsskyldighet och ytterligare skyldigheter som följer av anmälan om personuppgiftsincident.

**Undvika personuppgiftsincidenter**

Företaget/Organisationen ska arbeta medvetet och förebyggande för att undvika personuppgiftsincidenter. Detta innebär bland annat att vi ska:

* Skapa tydliga rutiner för att enkelt kunna upptäcka personuppgiftsincidenter.
* Upprätta en handlingsplan för de fall en personuppgiftsincident inträffar.
* Dokumentera alla personuppgiftsincidenter, även dem som inte måste anmälas till Datainspektionen.