# ÅTGÄRDSPLAN FÖR PERSONUPPGIFTSINCIDENTER

## Bakgrund och syfte

Föreningen följer dataskyddsförordningens regler och arbeta aktivt för att undvika personuppgiftsincidenter. Denna åtgärdsplan beskriver föreningens hantering om en personuppgiftsincidenter ändå skulle inträffa och hur föreningen skapar medvetenhet kring de risker som följer av personuppgiftsincidenter.

## Vad är en personuppgiftsincident?

En personuppgiftsincident är när en brist i dataskyddet medför risk för en enskild i exempelvis följande hänseenden.

- 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 eller kommit i orätta händer. Det spelar ingen roll om händelsen har skett avsiktligt eller inte.

Personuppgiftsincidenter kan exempelvis uppkomma om

- någon obehörig har fått tillgång till personuppgifter, till exempel om personuppgifter har skickats till mottagare som inte skulle ha uppgifterna,
- datorer som innehåller personuppgifter har förlorats eller stulits,
- någon har ändrat personuppgifter utan tillstånd eller
- personuppgifter inte är tillgängliga för den som behöver dem, och det leder till negativa effekter för den registrerade personen.

## Anmäla personuppgiftsincident till Datainspektionen

Föreningen har en skyldighet att utan onödigt dröjsmål och, om så är möjligt, inte senare än **72 timmar** efter att ha fått vetskap om en personuppgiftsincident, anmäla denna till Datainspektionen. Anmälan sker via Datainspektionens e-tjänst för att rapportera personuppgiftsincidenter.

Anmälan syftar till att göra det möjligt för Datainspektionen att bevaka vilka åtgärder som vidtas för att motverka negativa effekter av det inträffade. Om det blir nödvändigt kan Datainspektionen även 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 föreningen som, enligt ansvarsprincipen, 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 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.

## Innehåll i anmälan av personuppgiftsincident

All information som ska finnas i en anmälan avseende personuppgiftsincidenter återfinns i Datainspektionen e-tjänst för att rapportera personuppgiftsincidenter.

## Vem ska göra anmälan

Föreningen är i egenskap av personuppgiftsansvarig ansvarig för att upprätta anmälan. Inom föreningen är det styrelsen som ansvarar för att föreningen efterlever kraven under dataskydds-förordningen. Föreningen ska varje verksamhetsår utse en person som är ansvarig för att upprätta en anmälan vid en eventuell personuppgiftsincident.

## Undvik sanktionsavgifter

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

## Informera de registrerade

Om personuppgiftsincidenten är allvarlig ska föreningen utan onödigt dröjsmål informera de registrerade om personuppgiftsincidenten. Detta gäller om det är sannolikt att personuppgiftsincidenten leder till en hög risk för fysiska personers rättigheter och friheter. Föreningen ska bedöma både allvarligheten av den potentiella eller faktiska påverkan på personer som ett resultat av en personuppgiftsincident kan ha (”Hur allvarliga kan konsekvenserna bli?”) och sannolikheten för att detta inträffar (”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 föreningen 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 föreningen ska kunna hjälpa individerna att vidta åtgärder för att skydda sig mot effekterna av en personuppgiftsincident.

## Information till de registrerade

Föreningens information till de registrerade ska uppfylla följande krav som uppställts av Datainspektionen.

- Tydlig och klar beskrivning av orsaken till personuppgiftsincidenten.
- Namn och kontaktuppgifter till föreningens kontaktperson i ärendet eller till annan person som är insatt i frågan.
- Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
- Beskrivning av vad föreningen har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
- Beskrivning av vad föreningen, i förkommande fall, har gjort för att mildra eventuella negativa effekter.

## Dokumentation

Föreningen ska dokumentera alla personuppgiftsincidenter, inklusive omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits. Dokumentationen ska göra det möjligt för tillsynsmyndigheten att kontrollera efterlevnaden av föreningens anmälningsskyldighet samt ytterligare skyldigheter som följer av anmälan om personuppgiftsincident.

## Undvika personuppgiftsincidenter

Föreningen ska arbeta medvetet och proaktivt för att undvika personuppgiftsincidenter. Detta innebär bland annat att föreningen ska skapa tydliga rutiner för att enkelt kunna upptäcka personuppgiftsincidenter, upprätta en handlingsplan för de fall en personuppgiftsincident inträffar och dokumentera alla personuppgiftsincidenter, även sådana som inte måste anmälas till Datainspektionen.