



Rutin vid personuppgiftsincident

En personuppgiftsincident är en incident som innebär en risk för fysiska personers rättigheter och friheter.

Det kan till exempel vara att det finns en risk till obehörig åtkomst av personuppgifter eller att någon obehörig har fått tillgång till personuppgifter.

Föreningen har en skyldighet att anmäla till Datainspektionen inom 72 timmar från det att Föreningen har fått vetskap om incidenten.

Handlingsplan för personuppgiftsincident

1. Om en medlem, ledare, anställd eller annan person misstänker att en personuppgiftsincident kan ha skett ska denne omedelbart informera Klubbchef.
2. Klubbchef ska göra en initial bedömning och oavsett incidentens karaktär informera styrelsen
3. Klubbchef och styrelsen gör en bedömning om där finns en sannolikhet att incidenten kan medföra en risk för fysiska personers rättigheter och friheter.
 - a. Om punkt 3 innebär en risk för fysiska personers rättigheter och friheter görs en anmälan via Datainspektionens e-tjänst för att [rapportera personuppgiftsincidenter](#).
 - b. Om bedömning görs att punkt 3 ej innebär en risk för fysiska personers rättigheter och friheter dokumenteras incidenten och sparas.
4. Oavsett utfall i punkt 3 görs en bedömning avseende information till de registrerade. Bedömningen baseras på hur allvarliga konsekvenserna kan bli och hur sannolikt det är att enskilda personer har drabbats.
 - a. Om incidenten är allvarlig ska berörda personer informeras med följande:
 - i. Tydlig och klar beskrivning av orsaken till personuppgiftsincidenten
 - ii. Namn och kontaktuppgifter till föreningens kontaktperson i ärendet eller till en annan kontakt som är insatt i frågan och kan svara på frågor.
 - iii. Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
 - iv. Beskrivning vad föreningen har gjort, eller tänker göra, för att hantera personuppgiftsincidenten.
 - v. I förkommande fall: Beskriva vad föreningen har gjort för att mildra eventuella negativa effekter.