
Rutin för rapportering av personuppgiftsincident

Incidentrapporter

Enligt GDPR ska i princip alla personuppgiftsincidenter rapporteras till Datainspektionen inom lagstadgad tid om 72 timmar .

Anmälan av en personuppgiftsincident till tillsynsmyndigheten

1. Vid en personuppgiftsincident ska den personuppgiftsansvarige utan onödigt dröjsmål och, inte senare än 72 timmar efter att ha fått vetskap om det. Anmäl personuppgiftsincidenten till Datainspektionen. Om anmälan till tillsynsmyndigheten inte görs inom 72 timmar ska den åtföljas av en motivering till förseningen.
2. Den personuppgiftsansvarige ska utan onödigt dröjsmål få vetskap om en personuppgiftsincident.
3. En anmälan ska:
 - a. beskriva personuppgiftsincidentens art, inbegripet, om så är möjligt, de kategorier av och det ungefärliga antalet registrerade som berörs samt de kategorier av och det ungefärliga antalet personuppgiftsposter som berörs,
 - b. förmedla namnet på kontakt och kontaktuppgifterna där mer information kan erhållas,
 - c. beskriva de sannolika konsekvenserna av personuppgiftsincidenten, och
 - d. beskriva de åtgärder som den personuppgiftsansvarige har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet, när så är lämpligt, åtgärder för att mildra dess potentiella negativa effekter.
4. Om, och i den utsträckning det inte är möjligt att tillhandahålla informationen samtidigt, får informationen tillhandahållas i omgångar utan onödigt ytterligare dröjsmål.
5. Den personuppgiftsansvarige ska dokumentera alla personuppgiftsincidenter, inbegripet omständigheterna kring personuppgiftsincidenten, dess effekter och de korrigerande åtgärder som vidtagits.