Samordningsförbundet i Kalmar län

Rutin för personuppgiftsincidentsrapportering

Syfte

Att möjliggöra en enkel och effektiv personuppgiftsincidentsrapportering (nedan rapport) som kan vara tillsynsmyndigheten tillhanda inom 72 timmar.

Ansvar

Rutinen omfattar samtliga anställda samt alla övriga inom verksamheten som upptäcker en personuppgiftsincident.

Chefer som får en rapport till sig ansvarar för att rapporten omgående vidarebefordras till dataskyddsombudet så att rapporten kan vara tillsynsmyndigheten tillhanda inom 72 timmar.

Definitioner

Personuppgifter: varje upplysning som avser en identifierad eller identifierbar fysisk person (nedan kallad en registrerad), varvid en identifierbarfysisk person är en person som direkt eller indirekt kan identifieras särskilt med hänvisning till en identifierare som ett namn, ett identifikationsnummer, en lokaliseringsuppgift eller online-identifikatorer eller en eller flera faktorer som är specifika för den fysiska personens fysiska, fysiologiska, genetiska, psykiska, ekonomiska, kulturella eller sociala identitet.

Personuppgiftsincident: 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.

Rutin

När en personuppgiftsincident upptäcks ska en anmälan till dataskyddsombudet göras av den som upptäckte incidenten eller av annan lämplig person. Nedanstående frågor besvaras efter bästa förmåga och lämnas över till dataskyddsombudet för vidare handläggning.

Personuppgiftsincidenten
När inträffade personuppgiftsincidenten?
När upptäckte ni personuppgiftsincidenten?
Hur upptäckte ni personuppgiftsincidenten?
Vad har hänt vid personuppgiftsincidenten?
Varför inträffade personuppgiftsincidenten enligt er uppfattning?
Inom vilket verksamhetsområde inträffade personuppgiftsincidenten?

Personuppgifterna och de registrerade
Hur många registrerade har påverkats?
Hur många personuppgiftsposter har personuppgiftsincidenten påverkat?
Vilka grupper tillhör de registrerade?
Vilken sorts personuppgifter berörs av personuppgiftsincidenten?
Var personuppgifterna krypterade?

Konsekvenser
Vad kan bli konsekvenserna av personuppgiftsincidenten?
Hur allvarlig bedömer ni att personuppgiftsincidenten är?

Information till de registrerade
Har ni informerat de registrerade om personuppgiftsincidenten? När?
Kommer ni att informera de registrerade? När? Om inte, varför kommer ni inte att informera de registrerade?

Samordningsförbundet i Kalmar län

Chefer som får en rapport till sig ansvarar för att rapporten omgående vidarebefordras till dataskyddsombudet så att rapporten kan vara tillsynsmyndigheten tillhanda inom 72 timmar.

1. Dataskyddsombudet ser över anmälan av personuppgiftsincidenten och kontaktar anmälaren vid behov av komplettering.

2. Dataskyddsombudet gör en bedömning av huruvida personuppgiftsincidenten utgör en risk för den registrerades fri- och rättigheter.

2.1 Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för den registrerades rättigheter och friheter ska dataskyddsombudet anmäla incidenten till tillsynsmyndigheten via dess tillhandahållna e-tjänst.

2.1.1 Om risken bedöms som stor för att rättigheter och friheter kan påverkas negativt för de registrerade som drabbats av personuppgiftsincidenten ska de informeras om incidenten. Om de registrerade ska informeras kan tillsynsmyndigheten, i anslutning till att myndigheten erhållit anmälan, komma att ge vägledning eller råd om hur detta ska ske.

2.2 Är det osannolikt att en personuppgiftsincident medför risk för den registrerades fri- och rättigheter behöver incidenten inte anmälas till tillsynsmyndigheten.

3. Alla personuppgiftsincidenter ska dokumenteras. Om beslut fattas att inte anmäla en inrapporterad incident till tillsynsmyndigheten ska detta beslut motiveras och dokumenteras.

4. Återkoppling görs till anmälaren för vidare utredning om förbättringar bör genomföras för att undvika liknande incidenter i framtiden.

Tänk på sekretessen

Personuppgiftsincidentrapporter är allmänna handlingar som kan begäras ut, skriv inte mer än nödvändigt i personuppgiftsincidentrapporten.

Ändringshistorik

Datum	Ändring	Utförd av