

Rutin för hantering av personuppgiftsincidenter

Alingsås kommun

Typ av styrdokument: Rutin

Beslutande instans: Kommundirektör

Datum för beslut: 2020-10-27

Diarienummer: --

Gäller för: Kommunövergripande

Giltighetstid: Tills vidare

Revideras senast: --

Dokumentansvarig: Kommunjurist



ALINGSÅS
KOMMUN

Rutinen gäller för samtliga nämnder/styrelser i Alingsås kommun.

Rutinen ska årligen ses över och vid behov revideras av kommunledningskontoret.

Personuppgiftsincident

En personuppgiftsincident är en händelse som innebär en risk att någon förlorar kontrollen över sina personuppgifter eller att dennes fri- och rättigheter påverkas negativt. Exempel på konsekvenser är identitetsstöld, bedrägeri, finansiell förlust, brott mot sekretess eller tystnadsplikt.

En personuppgiftsincident har inträffat om en eller flera personers personuppgifter har blivit förstörda, gått förlorade på annat sätt eller kommit i orätta händer. En personuppgiftsincident har inträffat oavsett det har skett med avsikt eller av en olyckshändelse.

Kontaktpersoner

Varje nämnd/styrelse inom kommunen har en GDPR-samordnare som hanterar samordningen av personuppgiftsfrågor. Denna roll återfinns och definieras i *Policy för personuppgiftshantering i Alingsås kommun*. Personuppgiftsansvarig delegerar till GDPR-samordnare att bedöma om en personuppgiftsincident ska anmälas till Integritetsskyddsmyndigheten.

Dataskyddsbud finns tillgänglig för konsultation avseende denna rutins alla delar men beslut fattas alltid av personuppgiftsansvarig själv. Kontaktuppgifter till dataskyddsbud finns på alingsas.se.

Anmäla till Integritetsskyddsmyndigheten

Om en inträffad händelse bedöms att den ska anmälas till Integritetsskyddsmyndigheten, (IMY), så ska detta ske inom 72 timmar från den tidpunkt som den inträffade. Därför är det viktigt att den interna hanteringen och rapporteringen sker skyndsamt och i nära anslutning till att händelsen upptäcks.

Anmälan och rapportering vid en personuppgiftsincident

- Den anställda som själv upptäcker en potentiell incident eller får kännedom om en incident från ett personuppgiftsbiträde kontaktar omedelbart sin närmaste chef.
- Ansvarig chef och den anställda genomför en första kartläggning av incidenten. Därefter fylls den interna e-tjänsten för rapportering av personuppgiftsincidenter i. Rapporten skickas per automatik till de av nämnden/styrelsens valda e-postlådor för utredning och diarieföring.
- GDPR-samordnare bedömer om det är fråga om en personuppgiftsincident och om den ska anmälas till Integritetsskyddsmyndigheten. Samordnaren genomför eventuell anmälan inom 72 timmar från att incidenten blivit känd. Diarienumret från ärendet i diariesystemet (Platina) anges som referensnummer vid anmälan. Diarieföring av själva anmälningen ska också ske hos den personuppgiftsansvarige. Delegationsbeslut ska upprättas för information till ansvarig nämnd. Dataskyddsbud finns att konsultera om ett sådant behov finns.
- GDPR-samordnare gör bedömningen ifall de registrerade behöver informeras. Om de registrerade behöver informeras så tar ansvarig chef fram en

informationsplan och ser till att den verkställs.

- GDPR-samordnare initierar att ansvarig chef, vid behov i samråd med andra som kan bidra med bedömningen, gör en utredning om incidenten samt inkluderar en plan för att förhindra/minska risken för att liknande händelser sker igen. Utredningen med tillhörande plan diarieförs tillsammans det övriga dokument i ärendet. En kommungemensam utredningsmall finns att tillgå i den gemensamma dokumentlagringsytan Alfresco.
- Om flera personuppgiftsansvariga är en del av samma personuppgiftsincident så ska en anmälan per personuppgiftsansvarig upprättas.