Incidenthanteringsplan för Samordningsförbundet i Blekinge län

Revideringshistorik:

1. 2025-04-15 Första version

Innehållsförteckning

1. Inledning

I dataskyddsförordningen (GDPR) finns en skyldighet för organisationer att anmäla vissa typer av personuppgiftsincidenter till Integritetsskyddsmyndigheten (IMY). Detta dokument beskriver Samordningsförbundets i Blekinge läns (nedan kallat "förbundet") rutiner för att kunna upptäcka, rapportera, utreda och hantera personuppgiftsincidenter. Vidare är syftet att skapa en systematisk, bred och samlad rapportering av personuppgiftsincidenter inom förbundet för att minimera risker och skador.

2. Definitioner

2.1 Personuppgiftsincident

En personuppgiftsincident är en säkerhetsincident som kan innebära risker för människors friheter och rättigheter. Riskerna kan innebära att någon förlorar kontrollen över sina uppgifter, att någons rättigheter inskränks eller att tjänster inte är tillgängliga.

Exempel på personuppgiftsincidenter är:

- Obehörig åtkomst till ett system som innehåller personuppgifter (t.ex., dataintrång).
- Oavsiktlig eller olaglig förstöring, förlust, ändring eller obehörigt röjande av personuppgifter.
- Utskick av e-post med personuppgifter till fel mottagare.
- Förlust eller stöld av enhet (t.ex., laptop, mobiltelefon) som innehåller personuppgifter.
- Publicering av personuppgifter på en webbplats utan rättslig grund.
- Otillgänglighet av ett system som krävs för att behandla personuppgifter (t.ex., ett lönesystem).

2.2 Kategorisering av incidenter

För att underlätta hanteringen av incidenter, kategoriseras de enligt följande allvarlighetsgrader:

- **Kategori 1 (Låg):** Incidenter som sannolikt inte medför någon betydande risk för de registrerades rättigheter och friheter.
- **Kategori 2 (Medel):** Incidenter som *kan* medföra en risk för de registrerades rättigheter och friheter.
- **Kategori 3 (Hög):** Incidenter som *sannolikt* medför en hög risk för de registrerades rättigheter och friheter.

3. Roller och ansvar

3.1 Anmälare

En anmälare kan vara en medarbetare i förbundet, ett personuppgiftsbiträde eller en extern part som upptäcker en personuppgiftsincident.

- **Ansvar:**
    - Att omedelbart rapportera alla misstänkta eller faktiska personuppgiftsincidenter.
    - Att lämna så mycket information som möjligt om incidenten vid rapportering.

3.2 Incidentansvarig

Incidentansvarig är den person som har det operativa ansvaret för att samordna och hantera en personuppgiftsincident. För Samordningsförbundet i Blekinge län är förbundschefen, Magnus von Schenck, Incidentansvarig.

- **Ansvar:**
    - Att ta emot och registrera incidentrapporter.
    - Att göra en första bedömning av incidenten.
    - Att sammankalla och leda incidenthanteringsteamet (vid behov).
    - Att samordna utredningen av incidenten (eventuellt med stöd från extern expertis).
    - Att säkerställa att nödvändiga åtgärder vidtas för att begränsa skadan.
    - Att dokumentera alla steg i incidenthanteringsprocessen.
    - Att säkerställa att relevanta uppgifter delegeras vid behov.
    - Att säkerställa att det finns en tydlig rutin för hantering av incidenter vid Magnus von Schencks otillgänglighet.

3.3 Dataskyddsombud (DSO)

Dataskyddsombudet är en rådgivande funktion som gör bedömningar och är kontaktperson för såväl Integritetsskyddsmyndigheten (IMY) som de registrerade vid personuppgiftsincidenter. För Samordningsförbundet i Blekinge län är Vanja Stenius DSO.

- **Ansvar:**
    - Att ge råd om dataskyddsfrågor i samband med incidenthantering.
    - Att göra kvalificerade bedömningar gällande beslut om personuppgiftsincidenter ska rapporteras till IMY eller ej.
    - Att bistå vid riskbedömningen av incidenten.
    - Att granska och godkänna meddelanden till de registrerade.
    - Att dokumentera beslut om incidenter rapporteras eller ej, med motivering.

3.4 Personuppgiftsansvarig

Personuppgiftsansvarig är förbundsstyrelsen för Samordningsförbundet i Blekinge län, men förbundschefen har det operativa ansvaret.

- **Ansvar:**
    - Att tillhandahålla resurser och stöd för incidenthantering.
    - Att godkänna övergripande strategier och åtgärdsplaner.
    - Att säkerställa att incidenthanteringsplanen är aktuell och kommunicerad.
    - Att bevaka allvarliga incidenter och säkerställa adekvat hantering.
    - Att godkänna och distribuera meddelanden till de registrerade.

3.5 Personuppgiftsbiträde

Ett personuppgiftsbiträde är en organisation (eller ibland en fysisk person) som behandlar personuppgifter för den personuppgiftsansvariges räkning. Om det inträffar en personuppgiftsincident hos ett personuppgiftsbiträde, måste denne omedelbart rapportera detta till förbundet i enlighet med gällande personuppgiftsbiträdesavtal.

- **Ansvar:**
    - Att omedelbart upptäcka och rapportera alla misstänkta eller faktiska personuppgiftsincidenter till förbundet.
    - Att tillhandahålla all nödvändig information om incidenten.
    - Att samarbeta med förbundet för att utreda och hantera incidenten.
    - Att vidta åtgärder för att begränsa skadan och förhindra upprepning.

3.6 Samordningsförbundet

- **Ansvar:**
    - Att se till att alla medarbetare och personuppgiftsbiträden känner till vad en personuppgiftsincident är, hur de kan identifieras, kraven på att de ska rapporteras och var man ska rapportera dem.
    - Att utan dröjsmål vidta relevanta åtgärder för att hantera incidenter, åtgärder för att mildra eventuella negativa effekter av incidenter och även förebygga risker för liknande incidenter.
    - Att dokumentera inträffade personuppgiftsincidenter och under vilka omständigheter de inträffat, vilka effekter incidenten fått och vilka åtgärder som vidtagits.
    - Att analysera och använda den kunskap och lärdom som dras i samband med incidenter för att motverka och vidta förebyggande arbete för att minska riskens sannolikhet och konsekvens för att liknande incidenter inträffar igen.

4. Process för rapportering av personuppgiftsincidenter

4.1 Rapporteringskanaler

Alla personuppgiftsincidenter ska rapporteras till Incidentansvarig (Magnus von Schenck) via följande kanaler:

- E-post: magnus(at)finsam-blekinge.se
- Telefon: 0735-203 20
- Formulär: https://www.finsam-blekinge.se/intern9df9skL/

4.2 Information som ska rapporteras

Rapporten ska innehålla så mycket av följande information som möjligt:

- Datum och tidpunkt för upptäckt av incidenten.
- Datum och tidpunkt för när incidenten inträffade (om känt).
- Plats för incidenten.
- Beskrivning av incidentens art (t.ex., dataintrång, förlust av data).
- Berörda system och applikationer.
- Kategorier av personuppgifter som berörs (t.ex., namn, adress, personnummer).
- Antal registrerade som berörs (om känt).
- Potentiella konsekvenser av incidenten för de registrerade.
- Redan vidtagna åtgärder för att begränsa skadan.
- Namn och kontaktuppgifter till anmälaren.

4.3 Prioritering av incidenter

Incidenter prioriteras baserat på deras allvarlighetsgrad (se 2.2 Kategorisering av incidenter):

- **Högsta prioritet (P1):** Incidenter i kategori 3 (Hög).
- **Hög prioritet (P2):** Incidenter i kategori 2 (Medel).
- **Normal prioritet (P3):** Incidenter i kategori 1 (Låg).

4.4 Dokumentation av rapportering

Alla rapporterade incidenter ska dokumenteras av förbundet. Dokumentationen ska innehålla all relevant information om incidenten, åtgärder som vidtagits och beslut som fattats.

5. Process för bedömning av personuppgiftsincidenter

5.1 Inledande bedömning

Incidentansvarig ska genomföra en inledande bedömning av den rapporterade incidenten så snart som möjligt för att:

- Bekräfta att en personuppgiftsincident har inträffat.
- Samla in ytterligare information om incidenten.
- Avgöra om incidenten kräver omedelbara åtgärder för att begränsa skadan.
- Prioritera incidenten enligt 4.3.

5.2 Riskbedömning

I samråd med Dataskyddsombudet ska Incidentansvarig genomföra en riskbedömning för att utvärdera risken för de registrerades rättigheter och friheter. Vid riskbedömningen ska följande faktorer beaktas:

- **Typ av personuppgifter som berörs:** Känsliga personuppgifter (t.ex., hälsa, politisk åsikt) innebär högre risk.
- **Antal registrerade som berörs:** Ett stort antal berörda innebär högre risk.
- **Sannolikheten för att incidenten leder till skada:** Hur sannolikt är det att de registrerade kommer att drabbas av negativa konsekvenser?
- **Potentiella konsekvenser för de registrerade:** Vilka negativa konsekvenser kan de registrerade drabbas av (t.ex., identitetsstöld, ekonomisk förlust, psykisk ohälsa)?
- **Lättheten att identifiera de berörda:** Hur lätt är det att identifiera de individer vars personuppgifter har påverkats?

5.3 Beslutsmatris för anmälan till IMY

Följande matris används som vägledning för att avgöra om en incident ska anmälas till IMY:

Allvarlighetsgrad	**Risk för registrerade**	**Anmälningsskyldighet till IMY**
Kategori 1 (Låg)	Låg	Nej
Kategori 2 (Medel)	Låg - Medel	Överväg anmälan
Kategori 2 (Medel)	Hög	Ja
Kategori 3 (Hög)	Låg - Hög	Ja

5.4 Dokumentation av bedömning

Alla bedömningar av personuppgiftsincidenter ska dokumenteras. Dokumentationen ska innehålla:

- Beskrivning av incidenten.

- Resultat av riskbedömningen.
- Beslut om anmälan till IMY (med motivering).
- Namn på de personer som genomförde bedömningen.
- Datum och tidpunkt för bedömningen.

6. Anmälan till Integritetsskyddsmyndigheten (IMY)

6.1 Anmälningsskyldighet

Förbundet är skyldigt att anmäla en personuppgiftsincident till IMY inom 72 timmar efter att förbundet har blivit varse om incidenten, om det är sannolikt att incidenten leder till en hög risk för de registrerades rättigheter och friheter.

6.2 Anmälningsprocess

Anmälan till IMY ska göras via IMY:s webbplats:
https://www.imy.se/verksamhet/utfora-arenden/anmal-personuppgiftsincident/

6.3 Information som ska inkluderas i anmälan

Anmälan till IMY ska innehålla följande information:

- Beskrivning av personuppgiftsincidentens art, inbegripet om möjligt kategorierna av registrerade och ungefärligt antal registrerade som berörs samt kategorierna av och ungefärligt antal personuppgiftsposter som berörs.
- Namn på och kontaktuppgifter för dataskyddsombudet eller andra kontaktpunkter där mer information kan fås.
- Beskrivning av de sannolika konsekvenserna av personuppgiftsincidenten.
- Beskrivning av de åtgärder som förbundet har vidtagit eller föreslagit för att åtgärda personuppgiftsincidenten, inbegripet i förekommande fall åtgärder för att mildra dess negativa effekter.

6.4 Tidsfrister för anmälan

Anmälan till IMY ska göras inom 72 timmar efter att förbundet har blivit varse om incidenten. Om anmälan inte kan göras inom 72 timmar, ska en motivering till förseningen lämnas.

6.5 Ansvar för anmälan

Incidentansvarig ansvarar för att anmäla incidenten till IMY efter godkännande av Personuppgiftsansvarig och samråd med Dataskyddsombudet.

7. Information till registrerade

7.1 Beslutskriterier för information till registrerade

Förbundet ska informera de registrerade utan onödigt dröjsmål om personuppgiftsincidenten sannolikt leder till en hög risk för deras rättigheter och friheter. Vid bedömningen av om de registrerade ska informeras ska följande kriterier beaktas:

- Typ av personuppgifter som berörs (känsliga uppgifter innebär högre risk).
- Potentiella konsekvenser för de registrerade (t.ex., identitetsstöld, ekonomisk förlust, psykisk ohälsa).
- Möjligheten för de registrerade att skydda sig mot skadan.

7.2 Informationskanaler

Information till de registrerade kan lämnas via följande kanaler, beroende på situationen:

- E-post
- Brev
- Telefon
- Meddelande på förbundets webbplats

7.3 Innehåll i informationen

Informationen till de registrerade ska vara:

- Tydlig och klar.
- Innehålla en beskrivning av personuppgiftsincidentens art.
- Innehålla namn på och kontaktuppgifter för dataskyddsombudet eller andra kontaktpunkter där mer information kan fås.
- Beskriva de sannolika konsekvenserna av personuppgiftsincidenten.
- Beskriva de åtgärder som förbundet har vidtagit eller föreslagits för att åtgärda personuppgiftsincidenten, inbegripet i förekommande fall åtgärder för att mildra dess negativa effekter.

7.4 Uppföljning

Förbundet ska dokumentera all kommunikation med de registrerade och hantera eventuella frågor eller klagomål som uppstår.

8. Åtgärder för att begränsa skadan

Vid en personuppgiftsincident ska förbundet vidta alla rimliga åtgärder för att begränsa skadan för de registrerade. Dessa åtgärder kan inkludera:

- Stoppa den pågående incidenten.
- Säkra berörda system och data.
- Återställa system från säkerhetskopior.

- Ändra lösenord och åtkomstbehörigheter.
- Informera relevanta myndigheter eller organisationer.
- Erbjuda stöd till de registrerade.

9. Lärdomar och förbättringar

Efter varje personuppgiftsincident ska en utvärdering genomföras för att identifiera orsaken till incidenten, brister i befintliga säkerhetsåtgärder och möjligheter till förbättring. Resultaten av utvärderingen ska dokumenteras och användas för att uppdatera förbundets säkerhetsrutiner och incidenthanteringsplan.

10. Övningar och tester

Förbundet ska regelbundet genomföra övningar och tester av denna incidenthanteringsplan för att säkerställa att den är effektiv och att all berörd personal är bekant med sina roller och ansvar.

11. Kontaktlista för incidenthantering

Dataskyddsombud Vanja Stenius 0707 – 430 436, info(at)finsamgotland.se

Förbundschef Magnus von Schenck 0735 – 032 000, magnus(at)finsam-blekinge.se

12. Bilagor

- Länk till formulär för rapportering av personuppgiftsincident