# Rutin för hantering av personuppgiftsincidenter 2019

Svenska kyrkan
TÄBY FÖRSAMLING

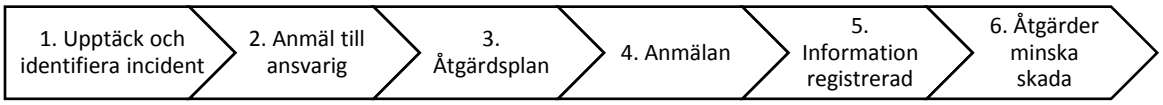
Svenska kyrkan
TÄBY FÖRSAMLING

| DOKUMENT | | | SIDA |
|---|---|---|---|
| Rutin för hantering av personuppgiftsincidenter | | | 1 (5) |
| UPPRÄTTAT AV | DATUM | DOKUMENTBETECKNING | VERSION |
| Olle Molin | 2019-05-28 | Ange beteckning | 1.1 |

# Rutin för hantering av personuppgiftsincidenter

Personuppgiftsincidenter måste hanteras på rätt sätt vilket bland annat innebär anmälan till Datainspektionen inom 72 timmar. Du kan behöva anmäla incidenter både när du konstaterat att en sådan föreligger och när du misstänker att så kan vara fallet. Nedan beskrivs processen och vad du ska göra om en incident inträffar både under incidenten och efter.
**Varje anställd har ansvar att hantera incidenter som upptäcks i arbetsuppgifter som den utför.**
I detta dokument beskrivs processerna för hur dessa två punkter ska hanteras.

## Åtgärder vid incident




**1. Upptäck och identifiera incident.** En personuppgiftsincident är enligt dataskydds-förordningens definition 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*.
En personuppgiftsincident kan bestå av följande händelser:

- **Sekretessbrytande incidenter:** någon får obehörigen (genom uppsåt) eller på grund av organisationens misstag tillgång till personuppgifter de inte borde ha fått se (till exempel att man råkat mejla eller på annat sätt dela information innehållande personuppgifter med obehörig eller att någon utomstående hackat systemet). Att en dator eller mobiltelefon som innehåller personuppgifter har förlorats – kanske stulits eller tappats bort – kan också innebära en sekretessbrytande incident om den inte hanteras.
- **Tillgänglighetsincidenter:** Om personuppgifter inte är tillgängliga för en person i organisationen som behöver dem och det leder till negativa effekter har vi en tillgänglighetsincident. Detta kan vara fallet om vi permanent eller tillfälligt inte får tillgång till information innehållande personuppgifter till exempel genom olycka (om personuppgifter av misstag raderas eller att vi förlorar en krypteringsnyckel) eller om viktiga IT-system slutar fungera helt eller periodvis. Kan personuppgifterna inte återställas genom till exempel en säkerhetskopia är incidenten permanent. Begreppet omfattar också annan icke auktoriserad tillgång eller förstörelse av personuppgifter (till exempel att en hackare förstör personuppgifter vi ansvarar för eller kidnappar våra system och därmed också våra personuppgifter). En tillgänglighetsincident kan också föreligga om en dator stjäls eller förstörs om uppgifter sparats lokalt på datorn.

Täby församling
POSTADRESS: BOX 208, 18323 TÄBY
BESÖKSADRESS: Attundavägen 3
TELEFON: +46(8)58003500

- **Integritetsincidenter:** I detta omfattas olyckor (till exempel att vi av misstag ändrar personuppgifter så att de inte längre är korrekta) och annan icke auktoriserad ändring av personuppgifter (till exempel att en hackare går in och ändrar personuppgifter eller att en anställd som slutar anställningen tar med sig dokumentation som innehåller personuppgifter vi ansvarar för).

**2. Anmäl incident till GDPR-ansvarig.** En personuppgiftsincident ska genast anmälas till en av följande GDPR-ansvariga personer.

| Namn/titel | E-post | Mobilnummer |
|---|---|---|
| Carl-Anders Fogelin | carl-anders.fogelin@svenskakyrkan.se | +46765273677 |
| Jacob Wedin | jacob.wedin@svenskakyrkan.se | +46765273676 |
| Olle Molin | olle.molin@svenskakyrkan.se | +46765273670 |

| Namn på vårt dataskyddsombud | E-post | Mobilnummer |
|---|---|---|
| Olof Mellqvist | olof.mellqvist@svenskakyrkan.se | +46708905135 |

Anmälan görs både via telefon/sms och e-post till någon som finns i första tabellen ovan (kontakta personerna i listan i den ordning de står tills du får tag på någon). Det är viktigt att du säkerställer att den du kontaktar kvitterat att denne fått din anmälan (innan du fått bekräftelse från ansvarig kan du inte anse att anmälan är gjord). Får du inte tag i någon på listan, kontakta i första hand någon annan i ledningsgruppen, i andra hand dataskyddsombudet (se kontaktuppgifter ovan).
Den GDPR-ansvariga person som får anmälan tar över ansvaret (anmälaren kan dock fortfarande behöva vara tillgänglig för att bistå med kompletterande uppgifter). Om GDPR-ansvarig bedömer att incidenten är allvarlig, ska ledningsgruppen ta ansvar för arbetet.
Dataskyddsombudet ska underrättas snarast (görs av GDPR-ansvarig) för att kunna ge stöd under processen, men dataskyddsombudet är inte ansvarig för att besluta om anmälan ska ske eller att anmäla incidenten.
**3. Åtgärdsplan.** Den GDPR-ansvarige ser till att incidenten dokumenteras och att en åtgärdsplan tas fram. Första steget är att avgöra vem som har personuppgiftsansvar för incidenten (notera att vi ibland kan samarbeta med andra organisationer eller ha personuppgiftsbiträden).
För att dokumentera incidenten används blanketten för dokumentation av personuppgiftsincidenter. Blanketten uppdateras löpande under hela incidentförloppet och versionshanteras. Blanketten diarieförs också efter avslutad incidenthantering, dock senast när anmälan görs till Datainspektionen. Övrig dokumentation (till exempel anmälan till och övrig korrespondens med Datainspektionen i ärendet) diarieförs också med samma ärendenummer, så att det är enkelt att följa hela processen. Ibland kan senare versioner av ifylld blankett också behöva diarieföras (till exempel om åtgärder vidtas efter att Datainspektionen kontaktats).
Om incident bedöms medföra risk för de registrerade eller om det är svårt att avgöra risknivån i inledningsskedet, ska anmälan till Datainspektionen ske inom 72 timmar efter vi som

personuppgiftsansvarig organisation först upptäckt incidenten. Dataskyddsombudet ska tillfrågas om sin bedömning och den ska dokumenteras i blanketten för incidenthantering. Vill vi avvika från dataskyddsombudets rekommendation ska skälen för detta dokumenteras.

**4 Anmälan till Datainspektionen inom 72 timmar.** Om det är troligt att personuppgiftsincidenten kommer att medföra en risk för de registrerade så måste vi meddela Datainspektionen. Vid bedömningen är det viktigt att fokusera på de potentiella negativa konsekvenserna för de registrerade. Om det är osannolikt att en personuppgiftsincident medför risker för de registrerade så behöver vi inte meddela Datainspektionen (är det få drabbade registrerade kan det vara en bra åtgärd att underrätta dem och efterhöra hur de bedömer saken). Samtliga incidenter ska dokumenteras, och vid beslut om att inte meddela Datainspektionen ska motiveringen bakom beslutet dokumenteras.

Blankett för anmälan finns på Datainspektionens webb. Det är den GDPR-ansvarige som hanterar incidenten som har ansvar för att anmäla den efter att beslut fattats att anmäla. Använd information från åtgärdsplanen när du fyller i blanketten. Tänk på följande när du anmäler:

- Vi ska på ett enkelt språk 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.
- Kontaktuppgifter ska anges.
- Vi ska beskriva de sannolika konsekvenserna av personuppgiftsincidenten, samt de åtgärder som har vidtagits eller föreslagits för att åtgärda personuppgiftsincidenten, till exempel åtgärder för att mildra incidentens potentiella negativa effekter.
- Om och i den utsträckning det inte är möjligt att tillhandahålla all information samtidigt, får informationen tillhandahållas i omgångar (utan onödigt ytterligare dröjsmål). Det är därför bra att så snart som möjligt och senast inom 72 timmar anmäla incidenten till Datainspektionen, även om utredningen av incidenten och nödvändiga åtgärder inte är klara.
- Om vi kommer att komplettera anmälan, ska vi beskriva varför.
- Om anmälan av någon anledning sker senare än 72 timmar efter att vi upptäckt personuppgiftsincidenten, ska vi beskriva varför.
- Om vi har skrivit något som vi anser bör omfattas av sekretess, beskriv vad och varför. Allt som rapporteras in till Datainspektionen blir så kallad allmän handling, som kan begäras ut av allmänheten och massmedier. Om någon begär ut uppgifterna gör Datainspektionen en sekretessprövning för att undersöka om uppgifterna kan anses vara offentliga och därmed kan lämnas ut, i sin helhet eller delvis. Integritetskänslig information eller information som kan innebära säkerhetsrisker om den kommer ut bör inte noteras i anmälan till Datainspektionen men ska finnas i vår egen dokumentation.

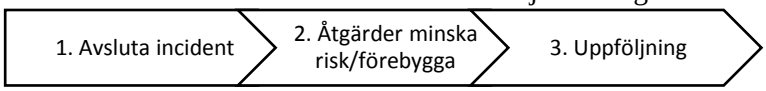
**5. Information till registrerad.** I vissa fall vi också vara skyldiga att informera registrerade om det inträffade. Det kan i oklara fall vara lämpligt att stämma av detta med Datainspektionen. Tänk på följande:

- Om en personuppgiftsincident bedöms sannolikt innebära en hög risk för fysiska personers rättigheter och friheter, ska vi utan onödigt dröjsmål informera de registrerade om personuppgiftsincidenten. Det mesta vi gör torde inte falla inom detta kriterium. Bedömningarna som görs i åtgärdsplanen utgör underlag för att fatta beslut om de registrerade behöver informeras eller inte.
- Om ett fåtal registrerade har drabbats kan det vara klokt att informera dem om incidenten för att få hjälp att bedöma hur allvarlig incidenten är utifrån deras utgångspunkt.
- Informationen till den registrerade ska innehålla en tydlig och klar beskrivning av personuppgiftsincidentens art och kontaktuppgifter till GDPR-ansvarig (eller andra kontaktpunkter) för mer information.
- I informationen ska de sannolika konsekvenserna av personuppgiftsincidenten beskrivas liksom de åtgärder som vi har vidtagit för att åtgärda personuppgiftsincidenten, till exempel åtgärder för att mildra negativa effekter (se steg 6).
- Vi ska också ge lämpliga råd till de registrerade.

**6. Åtgärder för att minska skada.** Åtgärdsplanen i steg 3 ska ha fokus på att minska skadan för de registrerade. Dokumentera fortlöpande vilka åtgärder som vidtas och vilken effekt de bedöms få/har fått i blanketten för incidenthantering.

## Åtgärder efter incident

Efterarbetet rörande en incident består av följande steg:




**1. Avsluta incident.** Inträffade incidenter ska rapporteras till ledningsgruppsmöte av den som ansvarat för att hantera incidenten. Ledningsgruppen beslutar när incidenthanteringen är genomförd, vilket dokumenteras i som sedan avslutas och sparas i Public360 (församlingens system för diarieföring). Dataskyddsombudet ska tillfrågas och få lämna uppfattning i frågan.
**2. Åtgärder för att minska framtida risk/ förebygga.** Om det i åtgärdsplanen har konstaterats att det är möjligt att vidta åtgärder för att minska risken för att samma sak inträffar igen, ska dessa vidtas. Det är ledningsgruppen som ansvarar för att göra denna bedömning och besluta om åtgärder. Dessa ska dokumenteras, vilket också innebär en bedömning av risknivå (det vill säga sannolikhet och konsekvens om något inträffar). Är risken allvarlig kommer den sannolikt också att tas upp i dataskyddsombudets rapporter och kontrollplan.
**3. Uppföljning.** På kommande ledningsgruppsmöten utvärderas både vad som gjorts under en incident och vilka åtgärder som vidtagits för att minska risk, samt vilken effekt de fått.

Dokumentation ska sparas. Allvarliga incidenter kan också behöva dokumenteras i årsredovisningen.

Täby församling
POSTADRESS: BOX 208, 18323 TÄBY
BESÖKSADRESS: Attundavägen 3
TELEFON: +46(8)58003500