Svenska kyrkan
I UTLANDET

MANUAL FÖR BEHANDLING AV PERSONUPPGIFTER

Svenska kyrkans församling i Bryssel

Antagen den 2021-12-15

1. INTRODUKTION

1.1 Manualens innehåll

Att ”behandla personuppgifter” inkluderar i stort sett all befattning med information om individer. Vi behandlar personuppgifter om bl.a. våra församlingsmedlemmar, besökare på gudstjänster eller basarer, volontärer och anställda. Exempel på behandlingar är när vi skriver ner en församlingsmedlems namn, tar ett foto av en gudstjänstbesökare, för minnesanteckningar från ett själavårdssamtal, betalar ut löner till anställda, sparar e-postadresser för utskick eller skriver upp matallergier inför ett volontärmöte.

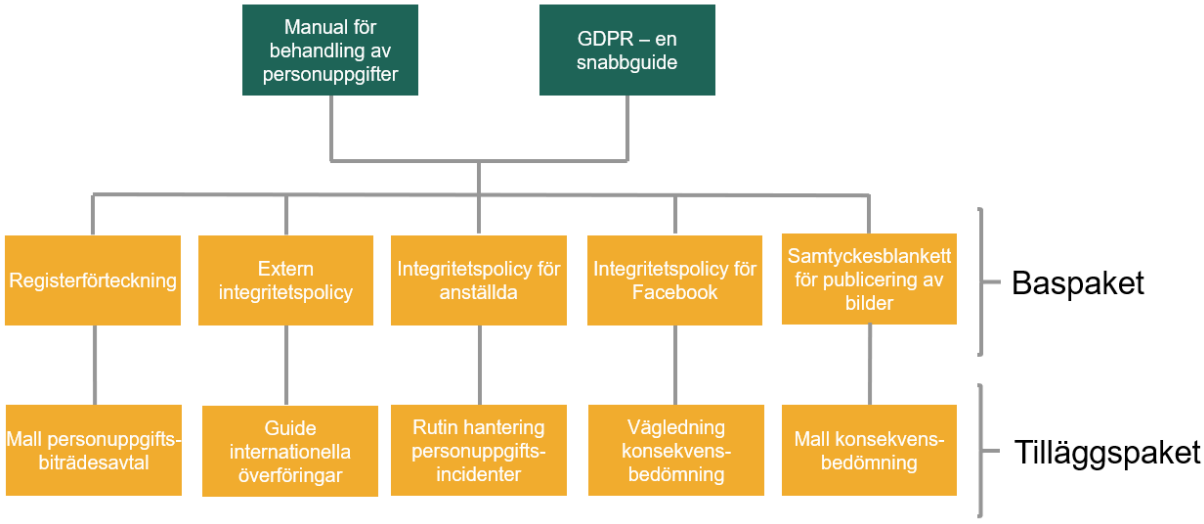
När vi får eller samlar in information om individer är det viktigt att vi gör det av rätt anledningar och på rätt sätt så att deras personliga integritet skyddas. Vi ska därför följa de riktlinjer och principer som beskrivs i denna *Manual för behandling av personuppgifter* (”**Manual**”).

Manualen är baserad på EU:s dataskyddsförordning (“**GDPR**”), som gäller i alla länder inom EU/EES. Även om annan lokal dataskyddslagstiftning kan vara tillämplig i länder utanför EU/EES utgör manualen en standard som alla Svenska kyrkans utlandsförsamlingar ska följa i tillämpliga delar. Manualen innehåller följande avsnitt:

- Principer för all behandling av personuppgifter
- Rättsliga grunder för behandling av personuppgifter
- Behandling av känsliga personuppgifter
- Individernas rättigheter
- Informationssäkerhet och skyddet av personuppgifter

1.2 Dokument som ska implementeras i församlingens verksamhet

För att vi ska kunna skydda individers personuppgifter på bästa sätt och säkerställa att vi följer GDPR finns det ett antal dokument som ska implementeras i verksamheten. Manualen går igenom och hänvisar till dessa. Vilka dokument som måste implementeras i verksamheten beror på församlingens storlek och verksamhet. Samtliga församlingar ska implementera **baspaketet**. Församlingar inom EU/EES som har minst 300 medlemmar och 3 anställda ska även implementera **tilläggspaketet**. Paketen innehåller följande dokument.



I den här Manualen beskrivs innehållet i båda paketen.

Det är kyrkoherden som är ytterst ansvarig för att församlingen lever upp till denna Manual, men alla som arbetar i församlingen ska känna till innehållet i Manualen och följa den.

Om vi har frågor om Manualen eller något av de andra dokumenten kan vi alltid vända oss till Svenska kyrkans kansli. Kansliet har ett team med jurister som har stor kunskap om dataskyddsfrågor. Vi når dem via dataskyddsjuristen Petter Gredmark, petter.gredmark@svenskakyrkan.se.

2. PRINCIPER FÖR ALL BEHANDLING AV PERSONUPPGIFTER

När vi behandlar personuppgifter finns det ett antal grundläggande principer som vi alltid måste beakta.

1. Vi har alltid en rättslig grund för att samla in och behandla personuppgifter (*laglighet*).

2. Vi har lämnat öppen och tydlig information om hur och varför vi behandlar personuppgifter (*öppenhet*).

3. Vi ber inte om individers personuppgifter för ett ändamål för att sedan använda dem för något annat ändamål (*ändamålsbegränsning*).

4. Vi samlar bara in de personuppgifter som vi verkligen behöver. Vi samlar inte in extra personuppgifter som kan vara “bra att ha” (*uppgiftsminimering*).

5. Den information vi har om individer är korrekt och uppdaterad. Vi raderar personuppgifter som vi inte behöver (*korrekthet*).

6. Vi sparar inte personuppgifter längre än de behövs eller för att de ”kan vara bra att ha” i framtiden (*lagringsminimering*).

7. Vi ser till att bara den som behöver se personuppgifterna kommer åt dem samt skyddar personuppgifterna från att förstöras, försvinna eller komma i orätta händer (*integritet och konfidentialitet*).

Det är vårt ansvar som församling att se till att vi följer dessa grundläggande principer. För att kunna visa att vi tar detta ansvar dokumenterar vi, genom denna Manual och tillhöriga dokument, hur vi efterlever dem.

3. RÄTTSLIGA GRUNDER FÖR BEHANDLING AV PERSONUPPGIFTER

Det måste alltid finnas en rättslig grund när vi behandlar personuppgifter. Den rättsliga grunden ska identifieras och dokumenteras innan behandlingen påbörjas. Vi dokumenterar våra behandlingar i vårt *Register över personuppgiftsbehandlingar*.

Det finns fyra tänkbara rättsliga grunder för vår personuppgiftsbehandling.

Rättslig grund	**Beskrivning**
Avtal	Personuppgiftsbehandlingen är nödvändig för att vi ska kunna fullgöra våra skyldigheter enligt ett avtal som vi ingått med individen, exempelvis ett anställningsavtal.
Intresseavvägning	Det finns ett berättigat intresse för oss eller någon annan att behandla personuppgifterna får något visst ändamål, och vårt intresse väger tyngre än individens intresse av att behandlingen inte utförs.
Rättslig förpliktelse	Vissa personuppgifter måste vi behandla för att kunna uppfylla en skyldighet vi har enligt lag eller kollektivavtal, exempelvis krav på att spara vissa personuppgifter av bokföringsskäl.
Samtycke	I vissa situationer, när inte någon annan rättslig grund kan användas, behöver vi samla in ett samtycke från individen. För att vara giltigt måste samtycket ha varit frivilligt att lämna, individen måste förstå vad den samtycker till och vi måste dokumentera samtycket. *Vi förlitar oss på samtycke för att publicera bilder från evenemang såsom bröllop och dop. Dokumentet "**Samtyckesblankett för publicering av bilder**" (se nedan under baspaketet) måste skrivas under av personer som deltar på evenemang där bilder tas för församlingens räkning.*

4. BEHANDLING AV KÄNSLIGA PERSONUPPGIFTER

Det finns vissa personuppgifter som till sin natur är mer känsliga än andra, exempelvis information om etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening eller hälsa.

Utgångspunkten är att det är förbjudet att behandla känsliga personuppgifter, men det finns undantag. Vi får till exempel behandla vissa känsliga personuppgifter om våra medlemmar

i egenskap av religiöst samfund, då det krävs enligt arbetsrätten eller om individen har samtyckt till behandlingen.

5. INDIVIDERNAS RÄTTIGHETER

Alla de personer vars personuppgifter vi behandlar har ett antal rättigheter enligt GDPR. Dessa beskrivs i tabellen nedan. Vi måste hantera alla frågor eller begäran om att utöva en rättighet så snabbt som möjligt och som huvudregel inom en månad. I undantagsfall har vi två månader på oss att svara.

Rättighet	Beskrivning
Registerutdrag	Rätt att få veta vilka personuppgifter vi behandlar om personen och på vilket sätt uppgifterna behandlas.
Rättelse	Rätt att få felaktiga uppgifter rättade och att själv komplettera med relevanta personuppgifter som saknas.
Radering	Rätt att begära att vi raderar personuppgifter som vi lagrar i strid med GDPR, till exempel om personuppgifterna inte längre än nödvändiga för det ändamål de samlades in för.
Begränsning av behandling	Rätt att i vissa fall kräva att behandlingen av personuppgifter begränsas, vilket innebär att uppgifterna markeras så att dessa i framtiden endast får behandlas för vissa avgränsade ändamål.
Dataportabilitet	Rätt för den som har lämnat sina personuppgifter till oss att i vissa fall få ut personuppgifterna i ett allmänt använt och maskinläsbart format, och att personuppgifterna överförs till en annan aktör.
Rätt att göra invändningar	Rätt att i vissa fall invända mot vår personuppgiftsbehandling om vi har baserat den på intresseavvägning. Vid invändning får vi endast fortsätta att behandla uppgifterna om det går att visa att det finns avgörande berättigade skäl till att uppgifterna måste behandlas som väger tyngre än den enskildes intressen.
Rätt att återkalla samtycke	Du har rätt att när som helst återkalla ett samtycke du lämnat till oss för en viss behandling. Vi kommer då omgående att upphöra med behandlingen. Att du återkallar samtycket påverkar inte lagligheten av behandlingen fram tills du återkallade ditt samtycke.

6. INFORMATIONSSÄKERHET OCH SKYDDET AV PERSONUPPGIFTER

Vi ska alltid skydda de personuppgifter vi behandlar på bästa möjliga sätt. Det kan vi göra genom att begränsa vilka som har möjlighet att ta del av personuppgifterna, kryptera data, förvara handlingar i låsta skåp och genom att ha back-up system. Vi kan också skydda

personuppgifter genom att noggrant välja vilka leverantörer som vi anlitar för att behandla personuppgifter åt oss och att inte spara personuppgifter i vår inkorg i mailen eller i öppna molntjänster.

BASPAKETET

1. INLEDNING

Baspaketet innehåller sju dokument som ska hjälpa församlingen att säkerställa att de grundläggande principerna för behandling av personuppgifter efterlevs, att församlingen har kartlagt sin personuppgiftsbehandling, att individer får information om vår behandling av deras personuppgifter och att vi har inhämtat ett giltigt samtycke när det krävs för behandlingen.

2. GRUNDLÄGGANDE PRINCIPER FÖR BEHANDLING

För att lättare få grepp om vilka skyldigheter vi som församling har när vi behandlar personuppgifter och vilka dokument vi måste implementera finns följande dokument.

- ”**GDPR – en snabbguide**”

  Kortfattad och lättillgänglig guide till GDPR, som förklarar och illustrerar de viktigaste principerna för personuppgiftsbehandling.

- ”**Manual för behandling av personuppgifter”**

  Denna Manual, vilken beskriver de grundläggande principerna och rättsliga grunderna för behandling av personuppgifter. Manualen går också igenom innehållet i de ”dokumentpaket” som ska implementeras i församlingen.

3. KARTLÄGGNING AV VÅRA PERSONUPPGIFTSBEHANDLINGAR

- “**Registerförteckning**”

  För att få en förståelse över vilka personuppgifter vi behandlar och varför genomför vi en kartläggning av samtliga behandlingar och dokumenterar i ett register. Registret innehåller ett antal kategorier av information om varje typ av personuppgiftsbehandling vi genomför. Vi uppdaterar registret regelbundet och ser till att det är korrekt. Registret underlättar även för nyanställda att sätta sig in i och förstå vilken personuppgiftsbehandling som församlingens verksamhet innebär.

4. HUR VI UPPFYLLER VÅR INFORMATIONSSKYLDIGHET

Genom följande tre dokument ser vi till att vi uppfyller vår informationsskyldighet gentemot individer vars personuppgifter vi behandlar. Vi informerar dem om hur vi behandlar deras personuppgifter vid insamling av uppgifterna.

- “**Extern integritetspolicy**”

  Policyn innehåller grundläggande information som ska ges till ”externa personer” vars personuppgifter vi behandlar, dvs. församlingsmedlemmar, volontärer, besökare, leverantörer, etc. Policyn ska uppdateras regelbundet för att korrekt beskriva vår personuppgiftsbehandling. Den externa integritetspolicyn görs

tillgänglig för alla besökare på vår hemsida och Facebooksida. Om personuppgifter samlas in via blanketter så hänvisar vi till hemsidan på blanketten.

- "**Integritetspolicy för anställda**"

  Policyn beskriver hur vi behandlar våra anställdas personuppgifter och ska göras tillgänglig för alla anställda.

- "**Integritetspolicy för Facebooksida**"

  Policyn innehåller information om våra personuppgiftsbehandlingar via Facebook och ska publiceras på vår Facebooksida. När vi använder Facebook är både vi som församling och Facebook personuppgiftsansvariga, ibland separat och ibland gemensamt. Ansvarsfördelningen och den behandling som sker beskrivs i policyn.

5. VI SAMLAR IN SAMTYCKE NÄR DET BEHÖVS

- "**Samtyckesblankett för publicering av bilder**"

  All behandling av personuppgifter förutsätter en rättslig grund. För att vi ska kunna publicera bilder av församlingsmedlemmar, besökare på gudstjänster, dop eller bröllop, anställda eller volontärer krävs att vi inhämtar samtycke. Det finns regler för hur ett sådant samtycke ska se ut. Därför använder vi blanketten för samtycke för publicering av bilder innan vi tar sådana fotografier.

TILLÄGGSPAKETET

1. INLEDNING

Församlingar som har 300 medlemmar och 3 anställda behandlar typiskt sett en större mängd personuppgifter och har en organisation med förutsättningar att implementera ytterligare dokument för att säkerställa att personuppgiftsbehandlingen följer bestämmelserna i GDPR. Tilläggspaketet innehåller fem dokument: en mall för personuppgiftsbiträdesavtal, en guide för internationella överföringar, en beskrivning av vad som utgör en personuppgiftsincident och när en incident måste rapporteras samt en vägledning och mall för konsekvensbedömningar.

2. NÄR NÅGON ANNAN BEHANDLAR PERSONUPPGIFTER PÅ VÅRT UPPDRAG (PERSONUPPGIFTSBITRÄDEN)

- "**Mall för personuppgiftsbiträdesavtal**"

  Om vi anlitar IT-leverantörer eller andra leverantörer som behandlar personuppgifter på vårt uppdrag, exempelvis en molntjänstleverantör, ska vi ingå ett skriftligt personuppgiftsbiträdesavtal med leverantören. Dokumentet kan användas som utgångspunkt för det avtal som ingås med leverantören.

3. INTERNATIONELLA ÖVERFÖRINGAR

- "**Guide för internationella överföringar**"

  Om en församling i ett land inom EU/EES för över personuppgifter till en leverantör, annan församling eller annan mottagare som befinner sig i ett land utanför EU/EES måste vi säkerställa att överföringen sker i enlighet med GDPR. Det kan vi t.ex. göra genom att ingå EU-kommissionens standardklausuler eller om EU-kommissionen har beslutat att landet till vilket överföringen görs har en adekvat skyddsnivå. Dokumentet innehåller mer utförlig information om vad vi måste tänka på innan vi överför personuppgifter från ett land inom EU/EES till en mottagare i ett land utanför EU/EES.

4. PERSONUPPGIFTSINCIDENTER

- "**Rutin för hantering av personuppgiftsincidenter**"

  Vi har en skyldighet att skydda personuppgifter från att de obehörigen förstörs, ändras eller sprids. Om det ändå skulle inträffa har en personuppgiftsincident skett. Exempel på personuppgiftsincidenter är phishing- eller hackerattacker, att ett dokument som innehåller personuppgifter tappas bort, att ett mejl med personuppgifter skickas till fel mottagare eller att en dator eller mobiltelefon som innehåller personuppgifter blir stulen.

  Om vi upptäcker en personuppgiftsincident som inte är bagatellartad måste församlingar inom EU/EES rapportera incidenten till tillsynsmyndigheten inom 72 timmar från att den upptäcktes. Vi ska även meddela de individer som drabbats, om incidenten är av allvarligare natur. Dokumentet innehåller mer utförlig information om personuppgiftsincidenter och hur vi ska agera när de inträffar.

5. KONSEKVENSBEDÖMNING

- "**Vägledning för när konsekvensbedömning bör göras**"

  Innan vi påbörjar en ny typ av personuppgiftsbehandling som sannolikt kan leda till hög risk för enskildas integritet måste vi göra en konsekvensbedömning. En konsekvensbedömning ska exempelvis normalt sett göras innan vi börjar att använda kamerabevakning. Konsekvensanalysen är ett viktigt verktyg för att förebygga dataskyddsrisker innan behandlingen påbörjas.

  Vägledningen innehåller riktlinjer för vilka situationer vi kan ställas för i praktiken där en konsekvensbedömning kan behöva göras.

- "**Mall för konsekvensbedömning**"

  Mallen används som utgångspunkt för en konsekvensbedömning och de överväganden som måste göras och dokumenteras.