Guide till Personuppgiftsbiträdesavtal

FRAMTAGEN AV PROJEKTET ANPASSNING TILL DATASKYDDSFÖRORDNINGEN

INTERNWWW.SVENSKAKYRKAN.SE/DATASKYDD | GDPR-PROJEKTET@SVENSKAKYRKAN.SE

Svenska kyrkan

Denna guide syftar till för att förklara vilken kontext Svenska kyrkans personuppgiftsbiträdesavtal bör användas i. Mer information om personuppgiftsbiträden finns på Datainspektionens webbplats och i dataskyddsförordningen artikel 28 samt GDPR-projektets intranätssida internwww.svenskakyrkan.se/dataskydd.

Ett exempel från en rekryteringsbyrå:

GDPR-säkra era rekryteringsprocesser med hjälp av [företagsnamn]

Väljer du att låta oss hantera er rekrytering så kommer ni att få ett personuppgiftsbiträdesavtal som säkerställer att vi ***gör vår del****, samt att* ***rekryteringsverktyget****, som hanterar all data, är* ***säkert och stabilt****. Skulle det mot förmodan* ***ske intrång kommer vi att återkoppla*** *till er direkt och* ***skulle en kandidat vilja bli glömd, raderad eller förflyttad så bistår vi*** *givetvis med detta.* ***När kandidaterna inte längre är aktuella kommer de att anonymiseras*** *enligt GDPR –* ***vi hanterar detta automatiskt*** *åt dig.*

Det ovan innebär alltså att biträdet hjälper till att behandla personuppgifter åt oss, närmare bestämt i rekryteringssammanhang. Detta är något som vi måste ställa krav på för alla våra personuppgiftsbiträden, och det regleras av dataskyddsförordningen (”GDPR”). Svenska kyrkan behöver enligt GDPR ställa krav på våra personuppgiftsbiträden genom ett avtal. Svenska kyrkan har en mall för det avtalet, ett så kallat personuppgiftsbiträdesavtal. För att bedöma om det behövs ett sådant avtal måste vi först bedöma om motparten är personuppgiftsbiträde.

Vem är personuppgiftsbiträde?

Den juridiska person (förening, företag, privatperson om denne är i enskild filma, församling) som behandlar *personuppgifter* för den *personuppgiftsansvariges* räkning. Personuppgifter är alla uppgifter som kan direkt eller indirekt hänföras till en fysisk levande person, så som en specifik medlem i Svenska kyrkan. Den personuppgiftsansvarige är oftast en juridisk person, oftast kyrkostyrelsen eller kyrkorådet för en viss församling.

Den personuppgiftsansvarige är enligt GDPR den som bestämmer **ändamål** och **medel** för behandlingen, det vill säga **varför** behandlingen görs (vilka syften tjänar behandlingen), och **hur** den görs (vilka uppgifter, vilka personkategorier, hur länge, var i världen görs den, vilka behandlingar (insamling, lagring, sortering, överföring till andra aktörer)).

Utgångspunkten är att kyrkorådet eller motsvarande styrelse är personuppgiftsansvarig, men detta är föremål för utredning av GDPR-projektet. Man kan också utgå från att arbetsgivaren är personuppgiftsansvarig för behandlingar som den utför, utifrån ett exempel där dotterbolaget följer en generell policy som moderbolaget har fastställt kan dotterbolaget vara ensamt ansvarig.

Personuppgiftsbiträdet är den som behandlar personuppgifter för den personuppgiftsansvariges räkning, vilket innebär att biträdet är någon som *inte* bestämmer över ändamålet och medlet för den personuppgiftsbehandlingen. Biträdet utför behandlingen på uppdrag av den personuppgiftsansvarige och i linje med den ansvariges instruktioner. Vem som är ansvarig och vem som är biträde är något som måste bedömas i varje specifik situation sett till de faktiska omständigheterna, oavsett

vad som står i något avtal eller uppdragsbeskrivning. Det är därför mycket svårt, rentav bland det svåraste med GDPR, att säga vem som bär ansvaret rent generellt. Det är dock mycket viktigt att vara medveten om vilka situationer vi *kan* vara personuppgiftsansvariga i, så att vi kan ingå nödvändiga avtal och ha nödvändiga dialoger med våra respektive personuppgiftsbiträden.

Vem är inte personuppgiftsbiträde?

Observera att leverantörer, producenter, tjänsteföretag, föreningar, inomkyrkliga enheter, och andra aktörer *inte nödvändigtvis* är personuppgiftsbiträden till oss.

Det är som utgångspunkt alltid möjligt att outsourca frågan om ”medel” eller ”hur”, d v s att biträdet själv bestämmer vilket tekniskt sätt som är mest lämpligt att utföra personuppgiftsbehandlingen. Det kan vara till exempel att ett molntjänstlagringsföretag själv bestämmer ”medlen”, så som hur och var personuppgifterna ska lagras rent tekniskt.

(I vissa fall behöver vi dock detaljstyra även hur behandlingarna görs, till exempel om molntjänstlagringen utgör en säkerhetsrisk genom att vara baserad i utlandet och vi använder den till att lagra känsliga personuppgifter. Det är därför viktigt att tänka på vilka *behandlingar* vi vill att personuppgiftsbiträdet ska utföra för oss.)

Så länge leverantören inte bestämmer frågan om ”varför”, d v s bestämmer ändamålet med behandlingen, så kan leverantören anses vara biträde. Om leverantören själv rent faktiskt har bestämt både *ändamål* **och** *medel* för en behandling så är biträdet i stället själv personuppgiftsansvarig för den behandlingen. Ett sådant kan vara om vår leverantör själv bestämmer sig för att göra reklam för sin verksamhet direkt till privatpersonerna som leverantören behandlar personuppgifter om för vår räkning. Då har biträdet gått utanför sitt uppdrag och är själv ansvarig för den behandlingen.

Om vi har köpt en färdig programvara så måste vi undersöka om företaget som producerat programvaran behandlar personuppgifter om oss, och varför. Om det är för att vi har gett företaget instruktioner att behandla personuppgifter så är vi personuppgiftsansvariga och företaget är personuppgiftsbiträde (är det ett större företag så kan det regleras genom företagets standardvillkor, och då är det svårt för oss att vara medvetna om att motparten bara är personuppgiftsbiträde).

Om vi inte har gett några instruktioner och företaget behandlar personuppgifter genom programvaran och vi har godkänt att hjälpa till att samla in personuppgifter så att programvaran kan användas, och vi därmed behandlar personuppgifter för företagets räkning, så kan vi vara personuppgiftsbiträde till företaget i stället!

Varför spelar det roll?

Om vi har ett personuppgiftsbiträde som bryter mot GDPR så är det vi som personuppgiftsansvariga som är ansvariga. GDPR ställer krav på oss att vara medvetna om framförallt fyra saker gällande personuppgiftsansvar:

1. Svenska kyrkan behöver vara medveten om sitt eget ansvar i förhållande till personuppgifter.
   a. Är vi personuppgiftsansvariga, och i så fall för vilka behandlingar?
   b. Har vi personuppgiftsbiträden och i så fall för vilka behandlingar?
   c. Har våra biträden underbiträden, som i sin tur har underbiträden, som i sin tur har underunderbiträden och så vidare? (Vi ansvarar för alla nivåer!)
2. Är vi personuppgiftsbiträde? I så fall för vilka behandlingar?

3. Ingå avtal, både med våra egna personuppgiftsbiträden, och med de som vi själva är personuppgiftsbiträden till. Detta ska göras innan 25 maj 2018.
4. Ge instruktioner så att personuppgiftsbiträdesavtalet kan följas i praktiken.
   a. Följ instruktioner som vi får när vi själva är personuppgiftsbiträden.
5. Var medveten om skyldigheterna som personuppgiftsbiträden har
   a. Behandla inga personuppgifter som inte framgår av instruktionerna
   b. upprätta behandlingsregister (detta gör vi enklast genom inventeringen),
   c. ha dialog med den personuppgiftsansvarige som vi är biträde till
   d. bistå den personuppgiftsansvarige när enskilda begär ut sina personuppgifter
   e. uppfyll krav på säkerhetsåtgärder.

Innehållet i själva avtalet

Avtalet måste enligt GDPR innehålla som minimum:

1. Att personuppgiftsbiträdet måste följa instruktionerna
2. Att personuppgiftsbiträdet måste vidta säkerhetsåtgärder
3. Att personuppgiftsbiträdet måste ha sekretessförbindelse för alla personer som behandlar personuppgifterna, oavsett om det är i biträdets organisation eller underbiträden
4. Att personuppgiftsbiträdet måste ha vårt samtycke till att anlita underbiträden
5. Att personuppgiftsbiträdet måste bistå oss när enskilda hävdar sina rättigheter, så som rätten till registerutdrag, rättelse av uppgifter, dataportabilitet eller att bli glömd/raderad.
6. Att personuppgiftsbiträdet måste återlämna eller förstöra, beroende på vad vi väljer, när uppdraget är avslutat
7. Att personuppgiftsbiträdet måste tåla granskning av behandlingarna, inklusive inspektioner på plats, så att vi som ansvariga kan garantera att våra personuppgifter behandlas enligt våra instruktioner på ett korrekt sätt.
8. Att personuppgiftsbiträdet måste ansvara för att följa instruktionerna och lagstiftningen. Om biträdet uppfyller de kraven så är det vi som uppdragsgivare (d v s personuppgiftsansvarig) som bär hela ansvaret om något skulle hända som leder till sanktionsavgifter/böter eller skadeståndskrav.

Vad gäller för Svenska kyrkan?

Svenska kyrkan värnar om den personliga integriteten, samt behandlar väldigt många känsliga personuppgifter. Därför ska vi ställa höga krav på våra leverantörer och andra motparter som är våra personuppgiftsbiträden. Ju större krav vi kan ställe, desto större krav måste vi ställa. Vårt avtal med leverantörer av unika kyrkliga tjänster ställer hårda krav.

Vilka krav borde vi ställa?

Några av dessa hårdare krav vi ställer i vårt standard-personuppgiftsbiträdesavtal är:

Rapportering utan onödigt dröjsmål, möjligt att ha ännu hårdare säkerhetsåtgärder än vad som krävs enligt lag, detaljerade instruktioner, ingen överföring utanför EU/EES utan vårt skriftliga medgivande, inget anlitande av underbiträden utan vårt skriftliga medgivande, möjlighet för oss att ändra i biträdesavtalet om det krävs för att uppfylla våra interna policyer eller beslut, radering/återlämning av personuppgifter inom 30 dagar från att huvudavtalet (som biträdesavtalet är en del av/bilaga till) har upphört att gälla.

För dessa krav behövs också mer detaljerade instruktioner så att vi har svart på vitt att veta om vi har gett instruktioner att vårt biträde t ex ska behandla ”barn antecknade i avvaktan på dop” eller inte. Detta är viktigt för att bevisa vad vi har instruerat dem att göra, vilket är det som avgör vem som ska betala böter och/eller skadestånd för den behandlingen. Ju otydligare instruktioner vi ger, desto större kan vårt ansvar vara. Detaljerade instruktioner är också vanligt förekommande, där bland annat IT- och telekomföretagens standardavtal innehåller sådana.

Måste vi alltid ställa de här kraven?

Vissa företag är faktiskt omöjliga att förhandla med, och därför kan vi inte använda vårt avtal med dessa företag utan måste i stället godkänna deras standardavtal. Då måste vi göra en bedömning av om företaget är tillräckligt pålitligt för att behandla våra personuppgifter, eller om vi måste hitta en annan aktör. Det är också viktigt att komma ihåg att inte alla leverantörer är personuppgiftsbiträden. Det är bara våra faktiska biträden som vi behöver ha avtal med.

Biträdet vill inte gå med på våra krav!

Det är inte så ovanligt, eftersom dessa krav är helt nya i och med dataskydds-förordningen/GDPR. Både personuppgiftsansvariga och personuppgiftsbiträden, i alla sektorer, måste uppfinna hjulet gällande de här frågorna. Svenska kyrkans standard-personuppgiftsbiträdesavtal har jämförts med IT- & Telekomföretagens standardbiträdesavtal samt förhandlats med många motparter. Om du behöver hjälp i dessa frågor, kontakta ditt stift, eller om du arbetar på kyrkokansliet direkt till GDPR-projektet@svenskakyrkan.se eller motsvarande linjeverksamhet.

Instruktioner till personuppgiftsbiträdet

Biträdesuppdraget kretsar kring instruktioner. Utan instruktioner finns inget biträdes-förhållande, eftersom biträdet måste behandla personuppgifterna enligt den person-uppgiftsansvariges instruktioner. Dessa instruktioner kan enligt förordningen vara muntliga eller underförstådda. För att vi ska kunna bevisa vad vi faktiskt har gett för instruktioner så ska instruktionerna enligt vårt personuppgiftsbiträdesavtal vara skriftliga (”dokumenterade”).

Vi lämnar dessa instruktioner till våra personuppgiftsbiträden genom att fylla i Bilaga 1 till Personuppgiftsbiträdet. Där kan vi välja att vara generella eller specifika.

Generella instruktioner kan vara t ex att behandlingen av personuppgifter får bara göras i den mån det krävs för att tillhandahålla Tjänsten. Om Tjänsten (det som ska presteras av leverantören) enligt Huvudavtalet (det avtal som reglerar vad leverantören levererar) är en lagringstjänst så kan instruktionerna vara att ”de personuppgifter som användare av Tjänsten för in i system X ska lagras och tillhandahållas på begäran av användare”.

Om det är ett mer komplext spektrum av tjänster som ska levereras så kan det behövas mer komplexa instruktioner. Det är viktigt att personuppgiftsbiträdet förstår vad instruktionerna innebär, och därför bör det alltid finnas en dialog. Det är dock viktigt att komma ihåg att eftersom vi är personuppgiftsansvariga så är det alltid vi som avgör vad instruktionerna ska vara. Om vi låter biträdet bestämma instruktionerna har biträdet de facto och enligt GDPR blivit personuppgiftsansvarig (och då kan båda parterna vara ”gemensamt personuppgiftsansvariga” eller ”delat personuppgiftsansvariga” vilket är två andra sorteras ansvarsförhållanden).

Om vi *kan* vara specifika i våra instruktioner så *bör* vi vara det, för att tydligt visa exakt vad vi bär ansvaret för och vad personuppgiftsbiträdet bär ansvar för.

Om biträdet anser att instruktionerna är i strid med dataskyddsförordningen eller annan relevant lagstiftning så har biträdet skyldighet enligt avtalet att meddela oss det och därefter invänta nya instruktioner.

Det bör vara den person som ansvarar för avtalet och kontakten med motparten som ger instruktionerna, men instruktionerna bör diskuteras i Svenska kyrkans relaterade verksamhet så som genom kontakt med förvaltningsledare, sakkunniga.

Exempel på instruktioner till personuppgiftsbiträdet

ÄNDAMÅL

[Ändamål 1: För att kyrkan ska kunna kontakta sina medlemmar]
[Ändamål 2: För att administrera kyrkoavgift]

TYP AV PERSONUPPGIFTER

[Alla ändamål: Personuppgifter som förs in i Kbok av användare eller administratörer i övrigt som tillhör den Personuppgiftsansvariges organisation.]
[Ändamål 1: Kontaktuppgifter, så som namn och arbetsrelaterat telefonnummer (dock inte privat).]
[Ändamål 2: Identifikationsuppgifter, så som namn, personnummer, personid.]
[Ändamål 1: Familjebild]

KATEGORI AV REGISTRERADE

[Vårdnadshavare, kontaktuppgifter, identifikationsuppgifter och familjebild]
[Medlemmar, kontaktuppgifter, identifikationsuppgifter.]

BEHANDLINGSAKTIVITETER

[Automatiskt: överföring genom integration till Kyrksam.]
[På begäran av användare: visa uppgifter från SPAR.]

PLATS FÖR BEHANDLINGEN

[Servrarna ska vara i Sverige och tillgängliga för tillgång och ändring från utomlands inklusive från länder utanför EU/EES.]

INFORMATIONSSÄKERHET

[Följ Svenska kyrkans informationssäkerhetspolicy]