Kommentarer kring den nya dataskyddsförordningen, GDPR.

Med anledning av att en ny dataskyddsförordning, GDPR, gemensam för EU, träder i kraft 2018-05-25, så kommer här några kommentarer som kan vara till hjälp för församlingar och andra som använder Koinonia. Inga garantier kan ges att nedanstående tolkningar är korrekta, varje församling bör själv läsa tillämpliga delar av förordningen. Nedanstående består av korta sammanfattningar av artiklar i GDPR samt i vissa fall citat ur förordningen och det svenska tillägget, samt mina personliga bedömningar av dess tillämpning.

Mer om GDPR, och förordningen i sin helhet, finns att läsa eller ladda ned här:
http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/

Det finns ett svenskt tillägg, dataskyddsutredningens direktiv, SOU 2017:39, (mer omfattande än själva förordningen), och det finns att läsa här:
http://www.datainspektionen.se/dataskyddsreformen/forberedelser/pagaende-utredningar/

GDPR är ett dokument på 88 sidor, och de första 31 sidorna består av 173 punkter med skäl till förordningen och vad den bör innehålla. Förordningen börjar på sidan 32 och består av 99 artiklar som berör olika aspekter av dataskyddet. De svenska kompletterande bestämmelserna i Dataskyddsutredningens direktiv, SOU 2017:39, består av 507 sidor! Min bedömning är dock att man som enskild församling/organisation, i nuläget bör rikta större fokus på GDPR.

1. **Den nya lagen** träder i kraft 2018-05-25. Samtidigt upphör den gamla personuppgiftslagen, PUL, samt den gamla personuppgiftsförordningen att gälla. Se SOU 2017:39, s. 78.

2. **Känsliga uppgifter**. GDPR ger varje medlemsstaterna handlingsutrymme att utforma specifika bestämmelser gällande det som klassas som *känsliga uppgifter*. Vad som i Sverige räknas som *känsliga uppgifter* framgår här:
   http://www.datainspektionen.se/dataskyddsreformen/dataskyddsforordningen/kansliga-personuppgifter-uppgifter-om-brott-och-personnummer/detta-ar-kansliga-personuppgifter/
   Att registrera medlemmar i en kyrka är alltså *känsliga uppgifter.*

3. **Rätten att föra register över medlemmar.** GDPR artikel 9:1 uttalar ett allmänt förbud för registrering av känsliga uppgifter. Artikel 9:2 anger vilka undantag som finns, och 9:2 d anger ett undantag för religiösa föreningar, GDPR s. 38. Obs! att undantaget gäller både för registrering av de som är medlemmar och de som har regelbunden kontakt med föreningen. Lämpliga skyddsåtgärder ska vidtas och uppgifterna får inte lämnas ut utan den registrerades samtycke. Däremot behövs inget samtycke för själva registreringen. Punkten d säger att kravet är att de ska vara medlemmar eller ha regelbunden kontakt.

4. **Personuppgiftsansvarig**. Det ska finnas en person som är och benämns Personuppgiftsansvarig. Se definitioner, GDPR artikel 4:7, s. 33. Kan vara en eller flera personer. Har ansvar för att all behandling av registret sker enligt förordningen, se GDPR artikel 24, s. 47. Den personuppgiftsansvarige har också ansvar gentemot den registrerade, att tillhandahålla all information som finns om den registrerade i systemet, vid en begäran. Detta ska ske inom en månad. Se GDPR artikel 12, s. 39. Ett undantag finns, för löpande text som är utkast eller minnesanteckningar, de omfattas inte av rätten till registerutdrag. Texten bör dock vara färdigställd inom ett år och då kunna utlämnas. Se SOU 2017:39, 13.4.2, s. 206.
   Koinonia: Det finns en inbyggd funktion för att skriva ut ett registerutdrag, när någon begär det. I Koinonia, se under menyn Utskrift, Registerutdrag.

5. **Personuppgiftsbiträde**. Övriga som arbetar med registret kan vara s.k. personuppgiftsbiträden, se definitioner, GDPR artikel 4:8, s. 33. Personuppgiftsbiträden handlar på uppdrag av den personuppgiftsansvarige. Ansvaret beskrivs i GDPR artikel 28, s. 49. Det kan också finnas andra personer som arbetar med registret och de arbetar då under den personuppgiftsansvariges eller något personuppgiftsbiträdes överinseende, GDPR artikel 29, s. 50.

6. **Dataskyddsombud**. GDPR artikel 37, s. 55, säger att det under vissa omständigheter ska utses ett dataskyddsombud. En av dessa omständigheter är, citat:

   c) den personuppgiftsansvariges eller personuppgiftsbiträdets kärnverksamhet består av behandling i stor omfattning av särskilda kategorier av uppgifter i enlighet med artikel 9 och personuppgifter som rör fällande domar i brottmål och överträdelser, som avses i artikel 10.

   Artikel 9 berör känsliga uppgifter, vilket stämmer på en församlings register, men det ska samtidigt vara ”i stor omfattning”, och det torde inte gälla de flesta församlingar. Däremot kanske ett samfund, om det har tillgång till många församlingars register. Detta är alltså en bedömningsfråga. Om ett dataskyddsombud utses ska dennes kontaktuppgifter meddelas tillsynsmyndigheten. Krav på dataskyddsombudets kvalifikationer finns i 37:5 och dataskyddsombudets ställning och uppgifter finns GDPR artikel 38 och 39.

7. **Dokumentation**. GDPR, artikel 30, s. 50, säger i korthet att ett register ska upprättas av den personuppgiftsansvarige, med namn och kontaktuppgifter på personuppgiftsansvarig och dataskyddsombud. Registret ska också innehålla uppgifter om ändamålet med behandlingen, beskrivning av kategorierna av registrerade och personuppgifter, om uppgifter ska lämnas ut och till vilka i så fall, m.m. Samma gäller personuppgiftsbiträdet, som också ska dokumentera namn, kontaktuppgifter och en del annat. Dokumentet ska finnas i elektronisk form, (ett dokument/register i en dator). Allt detta kan göras enkelt genom ett vanligt dokument, som innehåller det som föreskrivs. När detta upprättas, läs då GDPR, artikel 30, s. 50-51, vad som ska vara med!

   Obs! GDPR artikel 30:5, s. 51, har ett undantag från skyldighet att upprätta dessa register, om organisationen har färre än 250 medlemmar! Dock gäller inte detta undantag om behandlingen inte är tillfällig, eller uppgifterna är av känslig natur, så slutsatsen blir ändå att ett dokument måste upprättas, och det ska kunna göras tillgängligt för tillsynsmyndighet på begäran.

8. **Säkerhet**. Nödvändiga skyddsåtgärder ska vidtas för att säkerställa att kraven i dataskyddsförordningen uppfylls och den registrerades rättigheter skyddas. Detta gäller även om registret inte innehåller känslig information. Så här lyder texten, GDPR artikel 25, s. 48:

   1.Med beaktande av den senaste utvecklingen, genomförandekostnader och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige, både vid fastställandet av vilka medel behandlingen utförs med och vid själva behandlingen, genomföra lämpliga tekniska och organisatoriska åtgärder – såsom pseudonymisering – vilka är utformade för ett effektivt genomförande av dataskyddsprinciper – såsom uppgiftsminimering – och för integrering av de nödvändiga skyddsåtgärderna i behandlingen, så att kraven i denna förordning uppfylls och den registrerades rättigheter skyddas.

   2.Den personuppgiftsansvarige ska genomföra lämpliga tekniska och organisatoriska åtgärder för att, i standardfallet, säkerställa att endast personuppgifter som är nödvändiga för varje specifikt ändamål med behandlingen behandlas. Den skyldigheten gäller mängden insamlade personuppgifter, behandlingens

omfattning, tiden för deras lagring och deras tillgänglighet. Framför allt ska dessa åtgärder säkerställa att personuppgifter i standardfallet inte utan den enskildes medverkan görs tillgängliga för ett obegränsat antal fysiska personer.

3.En godkänd certifieringsmekanism i enlighet med artikel 42 får användas för att visa att kraven i punkterna 1 och 2 i den här artikeln följs.

Vilka säkerhetsåtgärder som ska vidtas, ska bestämmas utifrån hänsyn till en rad omständigheter enligt 1 ovan. Samma text återkommer i GDPR, artikel 32, s. 51, som behandlar säkerhet i samband med behandlingen:

1. Med beaktande av den senaste utvecklingen, genomförandekostnaderna och behandlingens art, omfattning, sammanhang och ändamål samt riskerna, av varierande sannolikhetsgrad och allvar, för fysiska personers rättigheter och friheter ska den personuppgiftsansvarige och personuppgiftsbiträdet vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken, inbegripet, när det är lämpligt…

Punkten 3 ovan säger att ett sätt att uppfylla kraven kan vara att använda en godkänd certifieringsmekanism. GDPR artikel 42 handlar om certifieringsmekanismer. Artikel 42:1 säger att kommissionen ska uppmuntra till införandet av certifieringsmekanismer, samtidigt som artikel 42:2 säger att certifieringen ska vara frivillig. Det finns alltså inte något krav på certifiering! Kraven är att nödvändiga skyddsåtgärder ska vidtas för att uppfylla kraven i förordningen, och detta ska göras med hänsyn till graden av känslighet och de risker som finns att obehöriga kan få tillträde till uppgifterna.

Med detta sagt så är min bedömning att registreringen av medlemmar i en kyrka i Sverige inte är av så känslig natur att en speciell certifieringsmekanism för åtkomst till registret är nödvändig, utan det torde räcka med en speciell inloggning i det registerprogram som används.
Koinonia: Här kan man använda det inbyggda behörighetssystemet i Koinonia i kombination med aktivering av låsmekanismen av databaserna, som också finns. Se under menyn Inställningar, Egenskaper, fliken Behörighet. Möjligheter till ”psedonymisering” finns också, genom en funktion för att ”avpersonifiera” personer som inte längre är medlemmar. Då kan viss data finnas kvar i arkivregistret så att statistiken fungerar. När arkivregistret är öppet, se menyn Editera, Radera i Arkivregister.

9. **Personuppgiftsincidenter**. Om uppgifter läcker ut, otillåtet dataintrång etc, så ska detta anmälas till tillsynsmyndigheten inom 72 timmar. Se GDPR artikel 33, s. 52.
10. Den **registrerades rättigheter** finns beskrivna i GDPR artikel 14-18, s. 41-44.
11. **Avlidna personer**. Förordningen gäller ej avlidna personer. Medlemsstaterna fastställer själva bestämmelser för behandlingen av personuppgifter rörande avlidna personer. Har ännu ingen uppgift om vad som gäller här. Påminner också om funktionen som finns att ”avpersonifiera” personer i arkivregistret, se ovan, slutet av punkt 8.

Kungsängen 2017-11-22

Claes Bystedt

Senast uppdaterad: 2017-11-27. Detta dokument kan komma att uppdateras.