Policy för personuppgiftshantering enligt GDPR
för
Malmö Pingstförsamling

2018-05-22

1 Inledning och syfte

Syftet med denna policy är att säkerställa att Malmö Pingstförsamling hanterar personuppgifter i enlighet med EU:s dataskyddsförordning (General Data Protection Regulation – GDPR) med ikraftträdande 2018-05-25.

Policyn omfattar alla behandlingar där personuppgifter hanteras och omfattar såväl strukturerad som ostrukturerad data.

2 Tillämpning och revidering

- Församlingsledningen ansvarar för att behandlingen av personuppgifter följer denna policy.
- Policyn ska fastställas av församlingsledningen minst en gång per år och uppdateras vid behov.
- Församlingsledningen är ansvarig för processen kring årlig uppdatering av policyn till följd av nya och förändrade regelverk.
- Policyn är tillämplig för församlingens styrelseledamöter, föreståndare, anställda, särskilt utsedda volontärer med ansvar för personuppgiftshantering samt uppdragstagare som berörs av församlingens verksamhet.
- Denna policy är förankrad hos alla medarbetare.

3 Organisation och ansvar

Församlingsledningen har det yttersta ansvaret för innehållet i denna policy och för att den implementeras och efterlevs av verksamheten.

Församlingsledningen har uppdragit åt församlingens föreståndare att ha det övergripande ansvaret för implementeringen av denna policy i församlingens verksamhet. Församlingens föreståndare ansvarar därvid särskilt för att:

- tillse att denna policy delges alla anställda medarbetare samt särskilt utsedda volontärer med ansvar för personuppgiftshantering,
- tillse att en samlad förteckning över personregister inom församlingen förs och uppdateras löpande, inklusive gallring av personuppgifter som inte längre är behövliga för det syfte de samlats in *(Registerförteckningen, se bilaga),*
- tillse att önskemål från en enskild person om utlämnande av våra personuppgifter rörande personen handläggs och besvaras inom 30 dagar,

- tillse att eventuella personuppgiftsincidenter anmäls till Datainspektionen senast inom 72 timmar samt att eventuella övriga nödvändiga åtgärder med anledning av incidenten vidtas, samt
- tillse att personuppgiftsbiträdesavtal tecknas med underleverantörer till församlingen som hanterar personuppgifter. Därvid ska våra krav på att personuppgifter hanteras enligt GDPR alltid vara en del i kravspecifikationen vid upphandling av sådana tjänster och i eventuella avtal om sådana tjänster.

Föreståndaren har rätt att ta hjälp av andra medarbetare eller särskilt utsedda volontärer med ansvar för personuppgiftshantering för fullgörandet av dessa uppgifter.

Alla församlingens styrelseledamöter, anställda medarbetare samt särskilt utsedda volontärer med ansvar för personuppgiftshantering ansvarar för att de agerar i enlighet med denna policy och vad den vill säkerställa.

4 Begrepp

Begrepp	Betydelse
Personuppgift	En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Indelas i: *1. Grunduppgifter* – basuppgifter för identifiering av en fysisk person, t ex namn, personnummer*, e-post, adress, arbetsgivare, löneuppgifter, fotografier, ip-adresser, aktivitetsloggar, bankuppgifter, information om familj *2. Särskilda ("känsliga") personuppgifter* – sådana personuppgifter som enligt GDPR klassas som integritetskänsliga, såsom religiös övertygelse, hälsouppgifter, medlemskap i fackförening, politiska åsikter, etniskt ursprung. *Personnummer kan vara en känslig personuppgift.
Registrerad	Den som en personuppgift avser, dvs den fysiska person som direkt eller indirekt kan identifieras genom personuppgifterna i ett register.
Personuppgiftsbehandling	En åtgärd eller kombination av åtgärder beträffande personuppgifter, oberoende av om de utförs automatiserat eller ej. Exempelvis: insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, begränsning, justering eller sammanförande, radering eller förstöring, utlämning genom överföring, spridning eller tillhandahållande på annat sätt,. GDPR:s krav träffar även personuppgifter i ostrukturerat

	material, såsom i löpande text, bild, ljud/filmupptagningar, i e-mail, på hemsida, i wordfiler och i fysisk dokumentation.
Informationsplikt	GDPR ställer krav på att den registrerade ska informeras om: • Den personuppgiftsansvariges identitet och kontaktuppgifter till denne, • Ändamålet med uppgiftsbehandlingen, • Den rättsliga grunden för uppgiftsbehandlingen, • Om det finns andra mottagare som ska ta del av personuppgifterna (såsom underleverantörer, samarbetspartners etc), • Hur länge uppgifterna är tänkta att sparas, • Sina rättigheter enligt GDPR att få tillgång till, ändra, radera eller begära begränsning av viss behandling av sina personuppgifter samt sin rätt att närsomhelst återkalla ev samtycken.
Personuppgiftsansvarig	Den som bestämmer för vilka ändamål personuppgifterna ska behandlas och hur behandlingen ska gå till. Den personuppgiftsansvarige ska se till att GDPR följs och att de registrerade kan tillvarata sina rättigheter.
Personuppgiftsbiträde	Den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Biträdet ska följa instruktionerna från den personuppgiftsansvarige vid behandlingen och kan inte själv bestämma för vilka ändamål eller hur personuppgifterna behandlas.
Personuppgiftsincident	En personuppgiftsincident är en säkerhetshändelse som har påverkat sekretessen och integriteten för eller tillgängligheten till personuppgifter. Exempel på incidenter är förlust av laptop, mobil eller annan teknisk utrustning, e-post med personuppgifter som skickats till fel mottagare, radering av data eller dataintrång. Om det är troligt att personuppgiftsincidenten kommer att medföra negativa konsekvenser för den registrerade i form av risk för den registrerades rättigheter och friheter måste incidenten anmälas till Datainspektionen inom 72 timmar. Om det är osannolikt att sådana risker uppkommit för den registrerade med anledning av incidenten behöver någon sådan anmälan inte ske.

5 Personuppgiftsbehandling

- Varje personuppgiftsbehandling i församlingens verksamhet ska ske enligt följande principer:

    - **Laglighet och öppenhet**
      Stäm av att hanteringen av personuppgifter sker med stöd av en rättslig (”laglig”) grund enligt GDPR. Det finns olika rättsliga grunder i GDPR, såsom:
        - ***rättslig förpliktelse***
          (dvs när man är skyldig enligt lag att registrera personuppgifter, såsom ex vis för bokföringsskyldighet eller för vigslar),
        - ***berättigat intresse***
          (såsom ex vis hantering av personuppgifter för medlemskontakt),
        - ***fullgörande av avtal***
          (såsom ex vis hantering av personuppgifter för anställd personal),
        - ***samtycke***
          (avser ett aktivt och informerat samtycke från den registrerade avseende viss särskilt beskriven uppgiftshantering).

      Kravet på öppenhet innebär en informationsplikt kring hanteringen av personuppgifter (se ovan under begrepp i avsnitt 4). I stor utsträckning uppfylls denna informationsplikt genom en allmän informationstext på församlingens hemsida med en länk till denna policy. Komplettera i förekommande fall med riktad information i svarsmail e dyl.

    - **Ändamålsbegränsning**
      Beskriv syftet med hanteringen av uppgifterna samt nödvändighet och avgränsning av uppgifterna. Detta är särskilt viktigt avseende ”känsliga” personuppgifter.

    - **Uppgiftsminimering**
      Samla inte in obehövliga uppgifter.

    - **Korrekthet och aktualitet**
      Säkerställ att uppgifterna är korrekta och aktuella.

    - **Lagringsminimering** (”rätten att bli bortglömd”)
      Säkerställ att personuppgifter gallras bort när de inte längre behövs för sitt ursprungliga ändamål. Tidpunkten för gallring av personuppgifter blir därmed en bedömningsfråga i förhållande till ändamålet med behandlingen av personuppgifterna.

    - **Integritet och konfidentialitet**
      Säkerställ att personuppgifterna inte hamnar i orätta händer och dokumentera hur detta säkerställs. Ex vis genom begränsning av

behörigheter, låst dörr till arkivförvaring, IT-skydd som kryptering, brandväggar, lösenordshantering osv.

- För registrering av personuppgifter avseende barn under 16 års ålder krävs målsmans samtycke. Samtycket ska lämnas genom aktivt godkännande av den relevanta personuppgiftsbehandlingen. Bevisning om lämnat samtycke ska bevaras så länge uppgifterna behandlas.
- Församlingens personuppgiftsbehandlingar dokumenteras löpande i *Registerförteckningen (se bilaga)*
- Församlingens hantering av personuppgifter i form av bilder regleras i en särskild *Bildpolicy (se bilaga)*. Bildpolicyn ska vara föremål för årlig översyn. För detta ansvarar församlingsledningen.
- En registrerad har rätt till utdrag, rättelse, radering och begränsning av behandling av sina personuppgifter. Föreståndaren ansvarar för att en sådan begäran hanteras utan dröjsmål och senast 30 dagar efter att begäran mottagits.
- Eventuella incidenter rörande personuppgifter som församlingen behandlar ska utan dröjsmål rapporteras till föreståndaren. Om incidenten bedöms medföra negativa konsekvenser för den registrerade i form av risk för den registrerades friheter och rättigheter ska föreståndaren utan onödigt dröjsmål och senast inom 72 timmar anmäla incidenten till Datainspektionen samt i övrigt vidta nödvändiga åtgärder med anledning av incidenten.
- På församlingens hemsida lämnas information om församlingens personuppgiftshantering. Denna ska uppdateras årligen. För detta ansvarar församlingsledningen.
- För ”känsliga” personuppgifter, såsom uppgifter om religiös övertygelse eller hälsotillstånd, gäller följande:
    - ”Känsliga” personuppgifter får inte delas genom en icke godkänd delningstjänst i molnet såsom Dropbox eller Google Drive
    - ”Känsliga” personuppgifter får inte skickas utanför organisationen med okrypterad e-post
    - Dokument som innehåller ”känsliga” personuppgifter ska lösenordsskyddas om de sänds med e-post
    - ”Känsliga” personuppgifter som inkommer via e-post ska inte lagras i mailsystemet utan sparas ned i relevant register och tas bort från mailsystemet.