

Policy för personuppgiftshantering

Antagen av styrelsen för Föreningen Djursholms Kapellvänner

Inledning och syfte

Syftet med denna policy är att säkerställa att Föreningen Djursholms Kapellvänner hanterar personuppgifter i enlighet med Dataskyddsförordningen (General Data Protection Regulation – GDPR). Policyn omfattar all behandling av personuppgifter och omfattar såväl strukturerad som ostrukturerad data.

Denna policy är förankrad i föreningens styrelse, samt är kommunicerad till föreningens medlemmar.

Organisation och ansvar

Styrelsen ansvarar för att behandlingen av personuppgifter i föreningen följer denna policy.

IT-ansvarig är av styrelsen utsedd till ansvarig för att implementera och följa upp policyn i föreningen, så att den efterlevs i den dagliga verksamheten och uppdateras vid behov.

Alla i föreningens styrelsemedlemmar ansvarar för att de agerar i enlighet med denna policy och det den vill säkerställa.

Tillämpning och revidering

Denna policy är tillämplig för föreningens styrelseledamöter och övriga personer med förtroendeuppdrag eller anställning inom föreningen, samt uppdragstagare som berörs av vår verksamhet.

Policyn ska fastställas av styrelsen minst en gång per år och uppdateras vid behov. Styrelsens utsedda ansvariga person håller i processen kring årlig uppdatering av policyn till följd av nya och förändrade regelverk.

Begrepp

Begrepp	Betydelse
Personuppgift	En personuppgift är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.
Registrerad	Den som en personuppgift avser, det vill säga 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 – såsom insamling, registrering, organisering och strukturering.

Personuppgiftsbehandling

- Varje personuppgiftsbehandling sker enligt följande principer:
 - Laglighet
 - Ändamålsbegränsning
 - Uppgiftsminimering
 - Korrekthet
 - Lagringsminimering
 - Integritet och konfidentialitet
- All hantering av personuppgifter sker enligt rättslig grund: samtycke, avtal, rättslig förpliktelse eller intresseavvägning.
- Personuppgifter lagras i ett medlemsregister tills dess att registrerad avslutar sitt medlemskap.
- Uppgifter av värde ur ett historiskt perspektiv lagras och arkiveras för framtiden, t ex föreningens verksamhetsberättelse och styrelseprotokoll.
- Då registrerad begär att raderas ur föreningens medlemsregister ska detta ske utan onödigt dröjsmål.
- Krav på att personuppgifter hanteras enligt Dataskyddsförordningen ska alltid säkerställas vid upphandling och utveckling av IT-lösningar och tjänster, och ska vara en del i kravspefifikationen och eventuella avtal.
- Uppföljning och utvärdering av hantering av personuppgifter ska ske minst årligen.
- Eventuella incidenter rörande personuppgifter som föreningen behandlar ska utan dröjsmål rapporteras till IT-ansvarig, som i sin tur ansvarar för att anmälan kommer in skyndsamt till Datainspektionen, samt att i övrigt nödvändiga åtgärder vidtas med anledning av incidenten.

Rättigheter för den enskilde

Som registrerad har den enskilde följande rättigheter:

- Rätt till tillgång. Den registrerade kan begära ut vilka personuppgifter som finns lagrade om densamma.
- Rätt till rättelse. Den registrerade kan begära att dess personuppgifter rättas ifall uppgifterna är felaktiga eller ofullständiga.
- Rätt till begränsning och rätt att göra invändningar. Den registrerade har rätt att begära en begränsning av användandet av personuppgifter samt att göra invändningar, till exempel att slippa direktmarknadsföring av föreningens verksamhet.
- Rätt till radering. Den registrerade kan begära att alla personuppgifter om densamma raderas. Uppgifterna skall då raderas utan dröjsmål.

Personuppgiftsbiträden

I de fall det är nödvändigt för föreningen att kunna erbjuda vissa tjänster delas personuppgifter med tredje part som är så kallade personuppgiftsbiträden. Ett personuppgiftsbiträde är ett företag eller organisation som behandlar informationen för föreningens räkning och enligt föreningens instruktioner. När personuppgifter delas med personuppgiftsbiträden sker det endast för ändamål som är förenliga med de ändamål för vilka föreningen har samlat in informationen, det vill säga att kunna uppfylla åtaganden enligt medlemskapet. Föreningen har skriftliga avtal med alla personuppgiftsbiträden genom vilka de garanterar säkerheten och sekretessen för personuppgifter.

Föreningen har personuppgiftsbiträden inom följande områden:

- Bokföring och redovisning