



UPPSALA
POLITICES
STUDERANDE

Handbok för personuppgiftshantering

Syftet med denna handbok är att klarlägga rutiner och riktlinjer för föreningens personuppgiftshantering, något som är ett lagstadgat krav enligt dataskyddsförordningen GDPR. Handboken kan ses som en utfyllnad av det som stadgas i integritetspolicyn vars syfte är att översiktligt redogöra för hur och vilka personuppgifter som behandlas. Alla förtroendevalda i föreningen ska ta del av och ha tillgång till denna handbok, allt för att säkra en god personuppgiftshantering som värnar om medlemmarnas integritet och rättigheter kopplat till sina personuppgifter.

Denna handbok kan komma att behöva uppdateras och utvecklas. Ändringar i handboken sker genom styrelsebeslut. Syftet med detta är inte att försvåra nödvändiga ändringar eller förbättringar, utan snarare att samtliga styrelseledamöter ska ha en uppdaterad och enhetlig version som medlemmar kan ta del av på efterfrågan. Styrelsen ansvarar för att handboken är uppdaterad i enlighet med gällande dataskyddsförordning eller motsvarande lagstiftning. Förtroendevalda ansvarar själva för att skriva om utskottsspecifika rutiner i sina rutinhandböcker.

1. Vad är en personuppgift?

Personuppgifter är all slags information som kan knytas till en fysisk person som är i livet. Exempelvis personnummer, namn och mailadress. Även foton på personer och ljudinspelningar som lagras elektroniskt, trots att inga namn nämns, klassas som personuppgifter. En av de personuppgifter som ses som extra känsliga är hälsa - dit räknas bland annat allergier.

2. När behandlar vi en personuppgift?

Varje åtgärd eller serie av åtgärder som vidtas i fråga om personuppgifter, vare sig det sker på automatisk väg eller inte, till exempel insamling, registrering, organisering, lagring, bearbetning eller ändring, återvinning, inhämtande, användning, utlämnande genom

översändande, spridning eller annat tillhandahållande av uppgifter. Alltså, har vi en personuppgift så behandlar vi en personuppgift.

3. När får vi behandla en personuppgift?

Personuppgifter får bara samlas in för ”särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål”, säger förordningen. Alltså, uppgifter som samlas in för ett visst syfte, får inte sedan användas för helt andra syften och insamlingen måste motiveras med ett syfte.

Vi måste också ha stöd i förordningen för att hantera personuppgifter. Det finns ett par olika rättsliga grunder som vår förening kan använda. En viktig sådan för vår förening är informerat samtycke. I vår förening ber vi personen i fråga om att få registrera personuppgifter. Ett samtycke är enligt förordningen ”varje slag av frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken den registrerade, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av personuppgifter som rör honom eller henne”.

När vi samlar in uppgifter om en person så måste vi *informera* personen i fråga. I förordningen GDPR finns en lång lista över vilken information som ska ges, men mycket kort ska vi tala om att vi samlar in personuppgifter, vilka uppgifter det handlar om och varför vi gör det. Kommer vi att lämna uppgifterna vidare till andra, måste vi tala om det. Det är exempelvis viktigt att vara tydlig med att personuppgifterna kommer att delas vidare med UPS riksorganisation PolRiks.

En viktig regel i förordningen är också att en inte får *spara personuppgifter* för länge. När de inte längre behövs för det syfte som de en gång samlades in för, så ska de tas bort. För vår förening gäller det exempelvis att när en person inte längre är medlem måste dennes uppgifter tas bort från it-systemen. Förr, när personuppgiftslagen gällde, var praxis att personuppgifter om en tidigare kund/medlem i normala fall fick användas för marknadsföringsändamål under ett års tid efter att kund/medlemsrelationen har upphört.

Tänk på att *skydda* personuppgifterna som vi behandlar, så att de inte stjäls eller oavsiktligt ändras eller kommer på avvägar. Ett nytt krav i förordningen är att om vi råkar ut för en personuppgiftsincident så måste vi rapportera det till Datainspektionen. En sådan incident kan till exempel vara ett usb-minne med personuppgifter som tappats bort, ett dataintrång på en av företagets servrar eller att någon i UPS obehörigt tagit del av personuppgifter.

Rutiner

Medlemsregister

Om en förtroendevald behöver tillgång till det aktuella medlemsregistret eller enskild medlems personuppgifter under verksamhetsåret får denne kontakta sekreterare. Att skicka hela medlemsregister via mail ska helst undvikas. En avvägning måste göras ifall det är nödvändigt att skicka hela medlemsregistret och om det kan lösas på annat vis är detta att föredra. Om ett medlemsregister skickas till en annan förtroendevald anger sekreterare i samband med detta när mottagaren måste radera medlemsregistret.

Google Drive

I föreningen används molntjänsten Google Drive för lagring av diverse dokument där det kan förekomma personuppgifter. Huvudregeln är att en inte bör lagra eller inneha dokument med personuppgifter såtillvida att det inte finns en rättslig grund för det. I slutet av varje verksamhetsår, innan överlämning till sin efterträdare, ska berörd förtroendevald gå igenom sin Drive och rensa eventuella dokument med personuppgifter vars lagring saknar rättsligt stöd. Utskottsordförande och ämbetspersoner ansvarar endast för att se till att detta följs i sina egna, stängda mappar. Presidiet ansvarar för att se efter mappen ‘’Arkivet’’.

Varje post i UPS har en rutinhandbok innehållandes uppgifter till företrädare på respektive post. Det är endast den senast reviderade versionen av respektive rutinhandbok som lagras.

Protokoll

På styrelsemöten nedtecknas alltid deltagarnas för- och efternamn i deltagarlistan och sparas på en kopia på Google Drive. Protokollen finns även tillgängliga på föreningens hemsida. Nedteckning av namn och lagring av dessa protokoll är av vikt som dokumentation på vad som förekommit på föreningens styrelsemöten och delning är av vikt för transparensen gentemot medlemmarna. Om en medlem eller annan adjungerad person deltar på ett styrelsemöte ska denna göras medveten om att dennes namn kan protokollföras. Om personen inte vill att namnet ska förekomma protokollförs personen som observatör.

Deltar någon på ett årsmöte kan även deras för- och efternamn protokollföras. Årsmötesprotokollen finns publika på föreningens hemsida och lagras på föreningens Google Drive tills vidare.

Mail

När en skickar ett mail som massutskick för t.ex. en inbjudan får en inte göra det så att samtliga mottagare ser andras mailadresser. För att göra detta anges den egna mailadressen i mottagarfältet och målgruppen anges i fältet "dold kopia". Detta tillvägagångssätt kan leda till att utskicket hamnar i mottagarens skräppost. Därför kan det vara viktigt att uppmana personer i andra kanaler att dubbelkolla sin skräppost.

Mailhistorik sparas i högst två år tillbaka i tiden för att sedan raderas. Syftet med lagringen är att underlätta för efterträdaren. Om äldre mail än så ska sparas måste rättslig grund och syfte med detta identifieras. Detta görs förslagsvis enligt följande procedur:

1. *Identifiera* de personuppgifter som finns i e-posten.
2. Avgör vilket *ändamål* du ska ha dessa uppgifter till.
3. Avgör vilket *rättsligt stöd* som en fortsatt behandling av uppgiften har.
4. Avgör *hur länge* mailet ska sparas innan det raderas.
5. *Flytta* informationen från mailinkorgen om informationen ska sparas under en längre tid.

Fotografier

När fotografier tas i uppdrag av UPS på UPS evenemang ska samtycke i största möjliga mån inhämtas. Samtycket inhämtas främst muntligt genom att fråga personerna i fråga om de vill medverka på bild. Vid mingelbilder är det svårare att insamla särskilda samtycken. Därav ska deltagare på evenemanget göras medvetna om det kommer tas bilder vid ett specifikt evenemang samt vem en ska kontakta om en inte vill medverka på bild överhuvudtaget. Denna information framgår förslagsvis vid anmälan till evenemanget.

När fotoalbum publiceras i UPS sociala medier ska det framgå i beskrivningen till albumet hur en går tillväga om en vill att någon specifik bild som en förekommer på ska tas bort. När styrelsen informerats om detta ska bilden i fråga tas bort.

Fotoalbum som tagits i uppdrag av UPS på UPS evenemang lagras på föreningens Google Drive i mappen "Arkivet" som enbart förtroendevalda har tillgång till.

Formulär

Ibland skickas formulär ut till medlemmar om exempelvis anmälan till sittningar, studiebesök, resor, utvärderingar etc. När detta görs och personuppgifter ingår i svaren måste det framgå i vilket syfte informationen samlas in, om den kommer att delas vidare och i så fall till vem/vilka, hur länge informationen kommer att sparas och vart en vänder sig ifall en vill att informationen ska raderas tidigare än så. Personuppgifterna i formulären sparas tills dess att evenemanget är över och/eller personuppgifterna inte längre behövs.

Hälsouppgifter

Hälsouppgifter så som allergier, specialkost eller liknande är särskilt känsliga uppgifter. Därför är det extra viktigt att formulär och dokument där dessa finns lagrade raderas efter att evenemanget ägt rum. När medlem frågas om specialkost bör frågan lyda “Finns det något du inte kan/vill äta?” för att uppmåna till ett svar som inte innehåller anledningen till att detta inte kan ätas. Till exempel är det önskvärt att inte få svar som “är laktosintolerant” eller “kan av religiösa skäl inte äta nötkött”. När specialkost rapporteras till nationer etc formulera det som exempelvis “ej gluten” och inte “glutenintolerant”.