villaägarna

Dataskyddsförordningen (GDPR) för samfällighetsföreningar

Villaägarnas Riksförbund
Postadress: Box 7118, 192 07 Sollentuna
Besöksadress: Rotebergsvägen 3
Telefon: 010-750 01 00
Org.nr: 802003-7118
Plusgiro: 46 94 00-6
Bankgiro: 227-7200
info@villaagarna.se
villaagarna.se

Innehåll

1 Inledning

Från och med den 25 maj 2018 gäller dataskyddsförordningen (GDPR) som lag i alla EU:s medlemsländer. I Sverige ersätts därmed personuppgiftslagen (PUL) av EU-förordningen. Samfällighetsföreningar hanterar personuppgifter och betraktas i såväl PUL som GDPR som personuppgiftsansvariga och ska alltså efter dataskyddsförordningens ikraftträdande iaktta de nya bestämmelserna.

2 Allmänt om personuppgifter

2.1 Personuppgifter

Personuppgifter är all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Det räcker att det är möjligt att räkna ut vem uppgiften handlar om för att uppgiften ska anses vara en personuppgift. Några exempel på personuppgifter är som följer:

- Namn
- Adress
- Fastighetsbeteckning
- Telefonnummer
- Personnummer
- E-postadress
- Registreringsnummer till en bil
- Fotografier och filmer

Samfällighetsföreningar behandlar personuppgifter, kanske främst genom upprättande av debiteringslängd men också medlemsförteckningar, i mötesprotokoll, listor med bilars registreringsnummer, namnlistor apropå städdagar etc.

2.2 Känsliga personuppgifter

Vissa personuppgifter betraktas som särskilt känsliga. Detta är uppgifter som till exempel vittnar om en persons hälsotillstånd (fysiska eller psykiska åkommor), sexuell läggning, religiös eller filosofisk övertygelse, fackföreningsmedlemskap eller etnicitet.

2.3 Personnummer

Personnummer är inte kategoriskt en känslig personuppgift men är ändå föremål för viss särreglering som har betydelse för när personnummer får behandlas. EU-förordningen har lämnat åt medlemsländerna att själva närmare reglera på vilka särskilda villkor behandling får ske.

2.4 Vem är personuppgiftsansvarig?

Dataskyddsförordningen definierar personuppgiftsansvarig som:

”en fysisk eller juridisk person, offentlig myndighet, institution eller annat organ som ensamt eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter(...)”

Vanligtvis är den juridiska person eller myndighet som behandlar personuppgifter i sin verksamhet att betrakta som personuppgiftsansvarig. För samfällighetsföreningar är alltså själva samfällighetsföreningens juridiska person att betrakta som personuppgiftsansvarig. Styrelsen, som företräder föreningen, har det yttersta ansvaret för att föreningen ska kunna följa dataskyddsförordningens regler men det är alltså fortfarande själva föreningen som är personuppgiftsansvarig, styrelsen är inte heller någon egen juridisk person.

3 Behandling av personuppgifter

3.1 Vad innebär behandling?

Att behandla personuppgifter innebär i princip all tänkbar hantering av personuppgifter. Dataskyddsförordningen definierar behandling som åtgärder såsom insamling, registrering, organisering, strukturering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning genom överföring, spridning eller tillhandahållande på annat sätt, justering eller sammanförande, begränsning, radering eller förstöring av personuppgifter. Några vanliga åtgärder som förekommer i samfällighetsföreningar och som innebär att personuppgifter behöver undergå behandling är:

- Upprättande och framläggande av debiteringslängd,
- upprättande av röstlängd,
- anteckningar i protokoll, till exempel reservationer,
- protokollföring av valda styrelseledamöter,
- utskick till medlemmarna,
- kontaktuppgifter till styrelsen på hemsida.

Det finns alltså i princip inte något utrymme för att hantera personuppgifter på ett sätt som inte innebär en behandling i dataskyddsförordningens mening.

3.2 När får en samfällighetsförening behandla personuppgifter?

Personuppgifter får registreras och behandlas om det finns en rättslig grund för behandlingen. Rättslig grund kan vara något av följande:

- Behandlingen är nödvändig för att ett avtal mellan personen och den personuppgiftsansvarige ska var uppfyllt,
- en rättslig förpliktelse som den personuppgiftsansvarige har eller
- en intresseavvägning där den personuppgiftsansvariges intresse av behandlingen väger tyngre än den registrerades intresse av skydd mot kränkningar av den personliga integriteten.
- Den personuppgiftsansvarige kan också ha erhållit samtycke för behandling av personens uppgifter

Till skillnad från föreningar med frivilligt medlemskap där grunden för behandling till stor del är avtal, utgör grunden för den mesta behandling som samfällighetsföreningar utför att föreningen har en rättslig förpliktelse att utföra behandlingen. Nedan följer några exempel där så är fallet:

3.2.1 Lagfartsförteckningar

Att beställa och ta emot en lagfartsförteckning är en behandling, insamling, av personuppgifter. Ändamålet är att kunna upprätta en korrekt debiteringslängd och den rättsliga grunden är den rättsliga förpliktelse styrelsen har att uttaxera för föreningens medelsbehov.

3.2.2 Uttaxering

En samfällighetsförening ska, enligt lagen om förvaltning av samfälligheter (SFL), uttaxera föreningens medlemmar för föreningens medelsbehov. Detta görs, enligt samma lag, genom upprättande och på stämma framläggande av en debiteringslängd som också ska innehålla uppgifter om de medlemmar som är betalningsskyldiga.

3.2.3 Röstlängd

De som har beslutanderätt på en samfällighetsförenings stämma är de som är medlemmar i föreningen och deltar på stämman. En röstlängd innehåller uppgifter om dessa medlemmar. Enligt SFL tas stämmobeslut genom att de medlemmar som deltar på stämman röstar i frågan och utfallet blir sedermera den ståndpunkt som en majoritet av medlemmarna på stämman biträtt. Även om det inte följer uttryckligen av SFL att en röstlängd ska upprättas följer det av flera andra bestämmelser att en sådan handling är i princip oumbärlig för att kunna avgöra att ett stämmobeslut tagits på ett behörigt sätt.

3.2.4 Stämmoprotokoll

Vid protokollföring kan man behöva skriva ned namn på medlemmar som deltagit i debatten på stämman, reserverat sig mot beslut eller valts till styrelseposter. Återigen framgår det inte svart på vitt att man har lagstöd för den här behandlingen. Att medlemmar har rätt att få reservationer förda till ett stämmoprotokoll är en allmän föreningsrättslig princip, även att föredraganden på stämman namnges i protokollet får vara hänförligt dit, det är emellertid inte en lika tillfredsställande grund för behandling som till exempel uttaxering. Att de valda styrelseledamöternas namn måste antecknas följer dels av stadgarnas föreskrifter att styrelsen utses av stämman, dels av föreningens skyldighet att registrera styrelseledamöterna hos samfällighetsregistret.

Tillhandahållandet av protokollet senast två veckor efter stämman är en behandling som följer av en rättslig förpliktelse enligt lag och innebär en behandling av de personuppgifter som står med i protokollet. Det kan därför vara bra att begränsa tillhandahållandet så tillvida att det inte skickas ut utan bara finns tillgängligt på någon plats som medlemmarna får information om.

Stämmoprotokollet kan också behöva skickas in till kronofogden vid begäran om direkt verkställighet för en utdebiterad avgift som inte betalats in.

3.2.5 Styrelseprotokoll

Styrelsen kan i sitt protokoll ha anledning att diskutera enskilda medlemmar, till exempel för att en medlem har skickat in en skrivelse till styrelsen eller då man har problem att få in medlemsavgift från en medlem. Då sådana frågor kan vara delikata bör man iaktta viss försiktighet i hur protokollet sedan hanteras. Vi avråder från att styrelseprotokollet är offentligt för någon annan än styrelsen, styrelsen bör under alla omständigheter inte skriva något i protokollet som styrelsen vid behov inte kan försvara, om protokollet visas upp för den som uppgifterna berör.

Har man en hemsida (avsnitt 7) med olika behörighetsnivåer (avsnitt 3.6.5) kan protokollet med fördel förvaras där enbart styrelsen kan läsa protokollet. Det är förstås viktigt att informera medlemmarna om styrelsearbetet men det finns lämpligare sätt än att skicka ut styrelseprotokoll, som närmast är ett internt arbetsdokument, till exempel nyhetsbrev.

3.3 När behandlar en samfällighetsförening känsliga personuppgifter?

Känsliga personuppgifter, sådana som nämnts under avsnitt 2.2, bör som utgångspunkt inte behandlas alls, det torde mycket sällan vara motiverat för en samfällighetsförening att hantera den typen av uppgifter.

Emellertid finns det situationer då även en samfällighetsförening skulle kunna behöva hantera känsliga personuppgifter. Ett exempel på det är när föreningen, i samband med en

städdag, bjuder på korv och läsk. Detta kan aktualisera behov att behandla både medlemmarnas filosofiska och religiösa övertygelser då korv torde kunna innehålla fläsk vars konsumtion är förbjuden enligt religioner som judendom och islam samt filosofiska övertygelser som till exempel veganism.

Ett annat exempel på en situation då föreningen faktiskt får in en känslig personuppgift är då någon meddelar att hon är sjuk, till exempel som skäl för frånvaro på ett styrelsesammanträde eller som motiv till att skicka ombud till stämman. Detta innebär att föreningen får in en uppgift om en persons hälsotillstånd.

3.4 Behandling av personnummer

Beträffande personnummer har dataskyddsutredningen föreslagit att sådana uppgifter ska få behandlas bara om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl. Förslaget överensstämmer i stort sett med PUL:s regler om behandling personnummer.

Det är emellertid tveksamt om en samfällighetsförening har något syfte med att behandla personnummer. Enda gången en samfällighet eventuellt skulle behöva använda personnummer torde vara vid indrivning av uttaxerade medel genom ansökan om direkt verkställighet, det är en förutsättning för att förfarandet ska kunna användas att den betalningsskyldige medlemmen med säkerhet kan identifieras. I de flesta fall torde dock uppgift om namn och fastighet som framgår av debiteringslängden vara tillräckligt för att identifiera den betalningsskyldige i indrivningssammanhang.

3.5 Kort om missbruksregeln

Den s.k. missbruksregeln, som återfinns i PUL och därmed upphör den 25 maj 2018, är ett undantag som innebär att man innan dataskyddsförordningens ikraftträdande kan använda enklare regler för personuppgifter i ostrukturerat material. Det gäller till exempel information om personer i e-post, på internet eller i en enkel lista som man har i datorn. Att missbruksregeln försvinner med införandet av GDPR innebär att samma regler som gäller för personuppgifter i databaser och ärendehanteringssystem, också ska användas för det som skrivs om personer i exempelvis e-post och på webbplatser. Om samfällighetsföreningen har en webbplats med utgivningsbevis, gäller dock inte GDPR för webbplatsen, men det innebär inte heller att man kan skriva vad som helst på webbplatsen. Vill du läsa mer om utgivningsbevis, se separat informationsskrift om utgivningsbevis.

3.6 Hur ska behandlingen gå till?

Om föreningen har haft bra rutiner och följt personuppgiftslagen så blir förändringarna som följer av införandet av GDPR inte så omfattande. Det finns emellertid några punkter som bör beaktas för att säkerställa att föreningen inte riskerar att bryta mot förordningen.

3.6.1 Ansvarig för personuppgiftsfrågor

Föreningen bör utse någon, företrädesvis i styrelsen, som har det övergripande ansvaret för att personuppgifter behandlas i enlighet med dataskyddsförordningen. Ett allmänt råd är att inte kalla denna person för personuppgiftsansvarig eller personuppgiftsbiträde eftersom detta är begrepp som har egna definitioner enligt GDPR (se avsnitt 2.4 samt 5). För att undvika begreppsförvirring kan man förslagsvis använda till exempel GDPR-ambassadör om man vill titulera den ansvarige för personuppgiftsfrågor på något sätt.

3.6.2 Identifiera och dokumentera personuppgifter

Föreningen bör inventera vilka personuppgifter som hanteras och sammanställa en dokumentation över detta så att det enkelt går att veta vilka uppgifter som förekommer i

verksamheten och var de finns. På så sätt är det också enklare att upprätthålla en legitim katalog med personuppgifter som är uppdaterad och inte innehåller uppgifter som inte längre behövs. Det skulle till exempel kunna vara onödigt att behålla gamla lagfartsförteckningar när de tjänat sitt syfte att upprätta en korrekt debiteringslängd.

3.6.3 Identifiera och dokumentera grunder för behandling

När föreningen har fastställt vilka personuppgifter som behandlas bör man undersöka och nedteckna vilken rättslig grund som finns för behandlingen av dessa personuppgifter. I avsnitt 3.2 har nämnts några grunder för olika behandlingar som är vanliga i samfällighetsföreningar. Genom att kartlägga och dokumentera sina rättsliga grunder för behandling kan man snabbt hänvisa till dessa och motivera behandlingen. Skulle man i arbetet med att identifiera grunder upptäcka att man saknar rättslig grund för behandling av vissa personuppgifter som föreningen förfogar över bör sådan behandling kunna upphöra utan att det får några större konsekvenser för den verksamhet som föreningen enligt lag ska bedriva.

3.6.4 Informera

De registrerade har rätt att få information om att deras personuppgifter behandlas. Föreningen behöver ha som rutin att informera medlemmarna om behandlingen både när personuppgifter samlas in och när den registrerade annars begär det. Informationen ska tillhandahållas den registrerade kostnadsfritt i en lättillgänglig, skriftlig form och vara av koncis, klar och tydlig, begriplig och lätt tillgänglig form, med användning av klart och tydligt språk. Mer detaljer om vilken information som ska lämnas finns i avsnitt 4.1.

3.6.5 Behörigheter

De personuppgifter som en samfällighetsförening behandlar behöver behandlas av en anledning. Emellertid bör inte alla i vem som helst alltid ha tillgång till alla dessa uppgifter. Det är därför påkallat att se över vem som har tillgång till de olika personuppgifter som föreningen hanterar. Har man till exempel en hemsida där föreningen lägger upp olika dokument kan det vara bra om det finns olika säkerhetsnivåer, förslagsvis en publik nivå som alla kan se med allmän information om föreningen, en högre nivå bakom inloggning som endast medlemmarna kommer åt där man förslagsvis lägger ut stämmoprotokoll, debiteringslängder och en ytterligare nivå där endast styrelsen har åtkomst där man har material som är ägnat för styrelsearbete, till exempel delägarförteckningar och styrelseprotokoll. Av detta följer att man även behöver säkerställa en rutin för att uppdatera behörigheter när medlemskretsen eller styrelsens sammansättning förändras.

3.6.6 Säkerhet

Personuppgifterna ska skyddas bland annat mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse. Den som behandlar personuppgifter ska därför vidta lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifterna.

Det är värt att fundera över var och hur man förvarar utrustning eller dokumentation som innehåller personuppgifter samt vem som har tillgång till den. Om e-post används i stor utsträckning kan det vara ett problem ur säkerhetssynpunkt. Fundera också över hur information sparas, både digitalt och i pappersform - och om det uppfyller första stycket.

3.7 Registerförteckning

Som framgår av avsnitt 3.6 ska samfällighetsföreningar i högre utsträckning än innan dokumentera sin personuppgiftsbehandling. Detta följer av att dataskyddsförordningen kräver att personuppgiftsansvariga ska föra ett register eller en förteckning över de

personuppgiftsbehandlingar som utförs i den verksamhet som den personuppgiftsansvarige ansvarar för. Förslagsvis kan man föra ett register i tabellform likt exemplet nedan:

Personuppgiftsansvarig: XXXX Samfällighetsförening
Kontaktuppgifter: Box XX XXXXX XXXXXXXXXXX, XXXXXX@XXXXXX.XX
Företrädare: XXXXXXXX XXXXXXXXX

Behandlingens namn	Ändamål med behandling	Kategori av personer	Kategori av personuppgifter	Känsliga personuppgifter	Kategori av mottagare av personuppgifter	Tid till radering (om möjligt)	Laglig grund för behandling	Personuppgiftsbiträde
Lagfartsförteckning, insamling	Lagfartsförteckning för upprätande av debiteringslängd	Medlemmar	Namn, adress, fastighetsbeteckning	-	Styrelsen	-	Rättslig förpliktelse att uttaxera för SFFs medelsbehov	-
Framläggande, debiteringslängd	Uttaxering enligt SFL 41 §	Medlemmar	Namn, adress, fastighetsbeteckning	-	Stämmodeltagare (medlemmar)	10 år (preskriptionstid för fordran)	Rättslig förpliktelse att uttaxera för SFFs medelsbehov	-

Härefter följer en beskrivning av de olika fält som förekommer i exemplet ovan:

3.7.1 Namn och kontaktuppgifter

Av registret ska framgå vem som är personuppgiftsansvarig. Detta torde med få undantag vara samfällighetsföreningen varför samfällighetsföreningens firma ska anges (det namnet föreningen har enligt stadgarna). Av kontaktuppgifter ska framgå hur man kommer i kontakt med föreningen, till exempel postadress eller mailadress. Företrädare är i första hand styrelsen eller den som föreningen utsett att vara ansvarig för personuppgiftsfrågor (se avsnitt 3.6.1).

3.7.2 Behandlingens namn

Det kan vara en god idé att namnge varje behandling så att det enkelt går att särskilja dem från varandra. En behandling kan kallas till exempel insamling, registrering, framtagning, läsning, användning, tillhandahållande, utlämning, spridning, justering, eller radering.

3.7.3 Ändamål med behandling

Ingen behandling bör ske på slentrian och beskrivningen av ändamålet ska fungera som underlag för att säkerställa att behandlingen är tillåten enligt någon rättslig grund. Det är alltså själva syftet med att utföra varje behandling som ska anges, exempelvis att de här personuppgifterna behöver genomgå den här behandlingen för att möjliggöra upprättande av debiteringslängd. Var hellre detaljerad än kortfattad.

3.7.4 Kategorier av personer

Här anges vilken kategori av personer vars uppgifter behandlas, exempel kan vara medlemmar, styrelsen, stämmodeltagare eller garageinnehavare, alltså något som urskiljer den aktuella gruppen av personer.

3.7.5 Kategorier av personuppgifter

Vilka slags personuppgifter som behandlas (se avsnitt 2.1). Är det till exempel en lista med namn och e-postadresser eller en förteckning med adresser och fastighetsbeteckningar?

3.7.6 Känsliga personuppgifter

Om det förekommer känsliga (särskilda) personuppgifter anges de i en egen kolumn.

3.7.7 Kategorier av mottagare av personuppgifter

Här anges vem som ska ta emot personuppgifterna. Särskilt påkallat att ange när uppgifter lämnas ut externt, till exempel till kronofogden eller till extern revision. Det är även att rekommendera att man anger interna mottagare, till exempel föreningens styrelse eller stämma.

3.7.8 Tid till radering (om det är möjligt att ange)

Personuppgifter ska inte lagras längre än vad som är nödvändigt med hänsyn till ändamålet. Om det är möjligt att förutse när personuppgifterna i behandlingen inte längre kommer att behövas anges den tiden här.

3.7.9 Laglig grund för behandling

Här kan man ange sin rättsliga grund som man bör ha identifierat för varje behandling (se avsnitt 3.2). Det är inte nödvändigt att ange det i registerförteckningen men det ska i vart fall nedtecknas någonstans.

3.7.10 Personuppgiftsbiträde

Om behandlingen utförs externt av ett personuppgiftsbiträde kan kontaktuppgifter till biträdet anges här alternativt en referens till personuppgiftsbiträdesavtalet.

4 Medlemmarnas rättigheter

4.1 Rätt till information

När föreningen behandlar personuppgifter har de registrerade rätt att få information om det. Detta gäller dels när uppgifterna samlas in från de registrerade, när uppgifterna samlas in från någon annan och när den registrerade själv begär information (registerutdrag).

Den information som ska ges när uppgifter samlas in är:

- Uppgift om vem som är personuppgiftsansvarig (samfällighetsföreningen och dess företrädare),
- uppgift om vem som är ansvarig för personuppgiftsfrågor,
- vilken typ av personuppgifter som samlats in (kategori till exempel namn, adress),
- om uppgifterna kommer från någon annan än den registrerade, var uppgifterna kommer från.
- ändamålet med behandlingen,
- rättslig grund för behandling (se 3.2),
- hur länge uppgifterna kommer lagras och
- i förekommande fall, vem uppgifterna utlämnas till, till exempel en organisation eller myndighet.

När den registrerade själv begär ett registeruttdrag ska följande information lämnas ut.

- Vilken typ av personuppgifter som samlats in,
- ändamålet med behandlingen,
- varifrån uppgifterna kommer,
- hur länge uppgifterna kommer att lagras och
- vem uppgifterna har lämnats ut till.

Den registrerade ska även få information om sina möjligheter att begära rättelse eller radering av personuppgifterna samt rätten att inge klagomål till Datainspektionen.

4.2 Rätt till rättelse

Den registrerade har rätt att få felaktiga personuppgifter rättade samt att komplettera med personuppgifter som är relevanta för ändamålet med behandlingen.

4.3 Rätt att raderas

Om en person begär att uppgifter som avser honom eller henne tas bort ska den personuppgiftsansvarige sörja för att dessa uppgifter raderas förutsatt att de inte längre behövs för de ändamål som uppgifterna samlades in för.

Uppgifter som samlats in med stöd av samtycke ska raderas om samtycket återkallas.

Uppgifterna ska även raderas om behandlingen inte varit tillåten i första taget. Beträffande medlemmar i en samfällighetsförening bör det inte vara aktuellt att radera uppgifter som behövs för den behandling som har rättslig grund förrän personerna inte längre är medlemmar i samfällighetsföreningen.

5 Externa tjänster

Någon som, utanför den egna organisationen, behandlar personuppgifter för den personuppgiftsansvariges räkning kallas i dataskyddsförordningen för personuppgiftsbiträde. Det kan till exempel vara en extern revisionsbyrå eller en tjänsteleverantör som förfogar över listor över medlemmarnas adresser, namn eller dylikt.

Även om behandlingen sker externt är det fortfarande den personuppgiftsansvarige som har det huvudsakliga ansvaret för behandlingen av personuppgifterna. Ett biträde kan bli skadeståndsskyldigt mot den personuppgiftsansvarige enligt avtal eller genom allmänna skadeståndsregler.

5.1 Personuppgiftsbiträdesavtal

För att uppfylla de krav som ställs upp i dataskyddsförordningen ska man upprätta ett personuppgiftsbiträdesavtal mellan den personuppgiftsansvarige och den som behandlar personuppgifterna för den ansvariges räkning.

Det är den personuppgiftsansvarige som ansvarar för att avtalet finns. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktionerna och att biträdet måste vidta de säkerhetsåtgärder som den personuppgiftsansvarige ska vidta.

Bland våra infoskrifter för samfällighetsföreningar finns mallar för personuppgiftsbiträdesavtal:
https://www.villaagarna.se/Radgivning/Informationsskrifter/samfallighetsforeningar/

6 Utskick med e-post

E-post som innehåller personuppgifter omfattas av dataskyddsförordningen. Epostmeddelanden är ett vanligt sätt att skicka ut information, det är emellertid inte något speciellt säkert sätt att göra det på ur IT-säkerhetssynpunkt. E-postmeddelanden liknas ofta vid öppna vykort som vem som helst kan läsa på vägen. Dock vore det opraktiskt och omständligt för de flesta föreningar att upphöra med den formen av kommunikation eller att börja kryptera samtliga e-postmeddelanden. Under alla omständigheter bör man se över vilken information man hanterar med e-post.

6.1 Massutskick

Det kan förstås vara motiverat att skicka ut e-post till hela medlemskretset i ett enda massutskick. Det man ska tänka på är att e-postadresser är personuppgifter. Använd därför 'hemlig kopia' för att medlemmarna inte ska bli mottagare av varandras e-postadresser i onödan.

6.2 Se över vad som skickas ut

Det är förstås viktigt för en samfällighetsförening att nå ut med information till medlemmarna. Det är förstås fullt rimligt att styrelsen skickar ut mail om till exempelvad man bestämt på ett styrelsemöte eller om en kommande stamspolning eller dylikt, sådan information är inte heller sådan att den behöver innehålla personuppgifter.

6.2.1 Styrelseprotokoll

Något som bör undvikas är att maila ut diverse protokoll till medlemmarna. Styrelseprotokoll är i regel inte offentliga men en del föreningar har ändå gjort så att man håller dessa tillgängliga för medlemmarna på olika sätt, till exempel genom att maila ut dem. Styrelseprotokoll är förstås viktigt att upprätta för att få stringens och struktur i styrelsearbetet men de är tänkta att vara arbetsdokument för styrelsearbetet och tjänar dåligt som information till medlemmarna. Vetskapen om att protokollen ska offentliggöras i sin råa form skulle dessutom kunna hämma styrelsearbetet. Dessutom skulle protokollen kunna innehålla personuppgifter. Det är bättre att använda sig av ett nyhetsbrev eller dylikt utskick för att medlemmarna ska få ta del av nödvändig information.

6.2.2 Stämmoprotokoll

Stämmoprotokollen känns kanske inte lika självklara. Enligt lag ska stämmoprotokollet hållas tillgängligt för medlemmarna senast två veckor efter stämman. Att hålla någonting tillgängligt innebär emellertid inte nödvändigtvis att det ska delas ut. I lagens mening är den rättsliga förpliktelsen uppfylld om protokollet finns att läsa på en plats som medlemmarna får information om. Det kan vara försvarbart att medlemmarna får stämmoprotokollet hem till sig, men e-post är sannolikt inte ett gynnsamt sätt att skicka protokollet med hänsyn till säkerhet vid behandling.

6.2.3 Debiteringslängd

För debiteringslängden gäller ett liknande resonemang som för stämmoprotokollet. Längden är en utpräglad lista med personuppgifter och lagen föreskriver endast att den ska framläggas på stämman samt (enligt normalstadgarna) finnas tillgänglig under kallelsetiden. Man kan tycka att det är rimligt att skicka hem längden till medlemmarna eftersom det där framgår när medlemmarna ska betala sina medlemsavgifter men med beaktande av dataskyddsförordningen är det alltså bättre att hålla sig till minsta möjliga och att i stället avisera på annat sätt när medlemsavgifterna ska betalas in.

7 Hemsidor

Hemsidor kan faktiskt vara ett bra sätt att bättre iaktta dataskyddsförordningens krav på säkerhet vid behandling av personuppgifter eftersom man har större möjligheter att skydda vissa uppgifter bakom inloggning och till och med ha olika säkerhetsnivåer för till exempel allmänheten, medlemmarna och styrelsen. Man öppnar upp för att kunna tillhandahålla till exempel stämmohandlingar utan att behöva hantera de säkerhetsproblem som finns med epost. Däremot har man en ytterligare administration med att hålla sina behörigheter uppdaterade (se avsnitt 3.6.5).

Det kan också vara värt att tänka på att samtycke bör inhämtas om man till exempel ska publicera en bild på hemsidan från en städdag eller ange kontaktuppgifter till någon privatperson.

Skulle samfällighetsföreningen ha en webbplats med utgivningsbevis, gäller dock inte GDPR för webbplatsen, men det innebär inte heller att man kan skriva vad som helst på

webbplatsen. Vill du läsa mer om utgivningsbevis, se separat informationsskrift om utgivningsbevis.

8 Tredje land (Utanför EU och EES)

De flesta tar kanske inte med sig samfälligheten på solsemestern men det kan vara värt att nämna att i princip all behandling måste ske inom EU och EES. Åker till exempel en styrelseledamot till ett tredje land får han eller hon alltså lämna styrelsearbetet hemma under tiden.

9 Sanktioner

Med dataskyddsförordningens ikraftträdande införs större möjligheter för tillsynsmyndigheten att ta ut sanktionsavgifter utöver de redan existerande sanktionerna varning, reprimand och föreläggande. Överträdelser av reglerna kan dessutom innebära skadeståndsskyldighet. Dataskyddsinspektionen är tillsynsmyndighet.

9.1 Varning

Tillsynsmyndigheten kan utfärda varningar om en planerad behandling av personuppgifter som myndigheten får kännedom om sannolikt kommer att bryta mot bestämmelserna i förordningen.

9.2 Reprimand

Myndigheten kan utfärda reprimander (tillsägelser) om en pågående behandling av personuppgifter som myndigheten får vetskap om bryter mot bestämmelserna.

9.3 Föreläggande

Myndigheten förelägga den personuppgiftsansvarige eller personuppgiftsbiträdet att tillmötesgå den registrerades begäran att få utöva sina rättigheter enligt denna förordning.

En personuppgiftsansvarig eller ett personuppgiftsbiträde kan också föreläggas att se till att behandlingen sker i enlighet med bestämmelserna i dataskyddsförordningen och om så krävs på ett specifikt sätt och inom en specifik period.

Den personuppgiftsansvarige kan också föreläggas att meddela den registrerade att en personuppgiftsincident har inträffat.
Myndigheten kan införa en tillfällig eller definitiv begränsning av, inklusive ett förbud mot, behandling.

Föreläggandet kan också avse rättelse eller radering av personuppgifter samt begränsning av behandling och krav på att den personuppgiftsansvarige också ska underrätta mottagare till vilka personuppgifterna har lämnats ut om dessa åtgärder.

9.4 Sanktionsavgift

Myndigheten kan besluta att ett företag som bryter mot reglerna i dataskyddsförordningen ska betala en administrativ sanktionsavgift.

Avgiften kan som mest vara 20 miljoner euro eller, när det rör bolag, fyra procent av den globala årsomsättningen, beroende på vilket belopp som är högst.

Hur hög sanktionsavgiften blir beror dels på vilken bestämmelse överträdelsen gäller, dels på omständigheterna i det enskilda fallet. Datainspektionen kommer bland annat att titta på hur allvarlig överträdelsen är, hur stor skada som skett, om det är fråga om känsliga personuppgifter och om överträdelsen är avsiktlig.

Eventuella tidigare överträdelser som den personuppgiftsansvarige gjort sig skyldig till ska också vägas in i bedömningen. Om den personuppgiftsansvarige tidigare fått ett föreläggande att rätta sig efter och underlåtit att göra så kommer även det att påverka.

Avgiften ska under alla omständigheter vara effektiv, proportionerlig och avskräckande så organisationens storlek har betydelse. Det är inte troligt att en samfällighetsförening, vid en överträdelse, skulle hamna i närheten av några maxbelopp om det ens skulle gå så långt som till en sanktionsavgift.

9.5 Skadestånd

En person som lidit skada till följd av en överträdelse kan ha rätt till ersättning av den personuppgiftsansvarige för den uppkomna skadan. Även ett personuppgiftsbiträde kan hållas ansvarig för sådan skada om biträdet agerat utanför personuppgiftsbiträdesavtalets ramar. Talan om skadestånd förs i domstol.