

Giva Sveriges riktlinjer för personuppgiftshantering

(GDPR)

Version 3.0

Innehåll

1. Introduktion.....	3
Bakgrund.....	3
Syfte	3
Avgränsning	4
2. Inledning	4
Skilj på behandling av personuppgift och kommunikation med en person.....	4
Handledning för arbetet med personuppgifter.....	5
Dataskyddsförordningen i praktiken	5
3. Organisationens ansvar.....	5
Ansvarsstruktur inom organisationen.....	6
Ansvarsförhållandet mellan riksförening och lokalföreningar.....	7
Personuppgiftsregister (register över behandling som görs inom organisationen)	7
Information om organisationens ansvar	8
Personuppgiftsbiträdesavtal	8
4. Principer för behandling av personuppgifter	9
5. Rättslig grund för behandling.....	10
Samtycke	11
Fullgörande av avtal.....	11
Rättslig förpliktelse.....	12
Berättigat intresse	13
6. Sparande av personuppgifter.....	14
Spara med berättigat intresse som rättslig grund	14
Spara med annan rättslig grund	14
7. Gallring av personuppgifter.....	15
8. Integritetspolicy och informationstexter.....	16
Fullständig information till registrerade	16
Information till allmänheten och givarna/medlemmarna	18
9. Säkerhet och inbyggt dataskydd.....	18
10. Publicering av bilder, filmer och ljud.....	19
11. Publicering på sociala medier	20
12. Medlemsregister.....	21
Bilaga 1.....	22

1. Introduktion

Bakgrund

Dataskyddsförordningen (GDPR) uppmuntrar branschorganisationer att ta fram uppförandekoder för att specificera tillämpningen av förordningen och på så sätt underlätta för framför allt små och medelstora organisationer att följa förordningen. Giva Sverige har därför utvecklat dessa riktlinjer till stöd för medlemmarnas efterlevnad av dataskyddsförordningen.

Giva Sverige strävar efter att skapa en trygg och säker miljö för givande som värnar förtroendet för organisationer som arbetar med insamling av gåvor från allmänheten och finansiering från företag. Insamling av gåvor ska bedrivas transparent, etiskt och professionellt. Dessutom arbetar Giva Sverige aktivt för att minska hindren för gåvoinsamling, vilket kan innebära att förenkla processer och reducera administrativa bördor för dessa organisationer.

Dessa riktlinjer är utformade för att balansera två centrala mål: att säkerställa att hantering av personuppgifter sker på ett ansvarsfullt sätt och att underlätta för organisationer att bedriva sin verksamhet effektivt. Genom att följa riktlinjerna kan medlemmarna både säkerställa att de följer GDPR och stärka sitt förtroende hos givare, allmänhet och beslutsfattare.

Syfte

Syftet med Giva Sveriges riktlinjer för personuppgiftshantering är att fungera som en vägledning för ideella organisationer som arbetar med insamlingsverksamhet att behandla personuppgifter på ett korrekt sätt med hänsyn till de specifika förutsättningar som gäller för organisationer med gåvofinansiering och samtidigt värna om givarens personliga integritet.

Riktlinjerna bygger på Giva Sveriges tolkning och bedömning av lagstiftningen med avseende på generell insamlingsverksamhet. Varje medlemsorganisation måste själv ta ställning till och tolka lagstiftningen utifrån sin verksamhet och behandling av personuppgifter.

GDPR är fortfarande vad som kan kallas en relativt ny lagstiftning. Detta innebär att tolkningen av lagen inte är entydig då alla tillsynsmyndigheter inom den inre marknaden inte har en samsyn på hur den ska tolkas. I takt med att lagen prövas i domstol kommer den att bli tydligare, vilket kan föra med sig att dessa riktlinjer återigen kan komma att behöva ändras för att möta utvecklingen.

Avgränsning

Giva Sveriges riktlinjer omfattar endast GDPR och inte lagstiftning som utarbetas för elektronisk marknadsföring/kommunikation. Riktlinjerna omfattar dessutom enbart de delar av dataskyddsförordningen som har störst betydelse för ideella organisationers möjlighet att bedriva insamlingsverksamhet. Exempelvis är artikel 30 grundläggande. Enligt denna ska varje personuppgiftsansvarig föra ett register över behandling som utförts under organisationens ansvar.

Behandling av personuppgifter för andra ändamål, t.ex. personal, volontärer och andra verksamhetsområden, ligger utanför dessa riktlinjers räckvidd.

2. Inledning

EU:s dataskyddsförordning (GDPR) är en anpassning till den digitala utveckling som har präglat samhället under de senaste decennierna. Till skillnad från tidigare lagstiftning på området omfattar dataskyddsförordningen i princip all behandling av personuppgifter, dvs. analog som digital, strukturerad som ostrukturerad¹. Det betyder att organisationen behöver dokumentera – och hitta rutiner för behandling av – alla typer av personuppgifter inom organisationen, för såväl givare som medlemmar. Det gäller även sådana personuppgifter som förekommer t.ex. i löptext, i epostmeddelande, m.m. Konsekvenserna om organisationen **inte** gör det kan komma att bli mycket kännbara.

Skilj på behandling av personuppgift och kommunikation med en person

Det är viktigt att notera att dataskyddsförordningen **endast** reglerar **behandling** av personuppgift och *inte marknadsföring/kommunikation*. Med behandling avses allt som görs med en personuppgift, t.ex. segmentering, registrering av en gåva eller gallring av givardatabas. I samband med marknadsföring/kommunikation med en individ krävs alltid behandling av personuppgift, men för själva marknadsföring/kommunikationen – dvs. den faktiska åtgärden att kommunicera med någon, t.ex. att ringa, skicka brev eller skicka e-postmeddelande – gäller **dessutom** marknadsföringslagen och lagen om elektronisk kommunikation.

I samband med marknadsföring/kommunikation till enskilda individer räcker det således inte att uppfylla kraven i dataskyddsförordningen; marknadsföringslagen och lagen om elektroniska kommunikation måste också följas. Denna lagstiftning omfattas dock inte av

¹ Det finns några få undantag: Manuellt registrerade personuppgifter som inte är strukturerade i system och som inte gjorts tillgängliga för sökning eller sammanställning enligt särskilda kriterier. Om det skulle strida mot tryck- eller yttrandefriheten. Journalistiska ändamål eller konstnärligt eller litterärt skapande. Om det i en annan lag eller förordning finns bestämmelser som avviker från GDPR gäller de bestämmelserna i stället för reglerna i GDPR. Och avslutningsvis om behandling av personuppgifter görs uteslutande för privata ändamål gäller inte heller GDPR.

dessa riktlinjer.

Handledning för arbetet med personuppgifter

För mer information om vad varje organisation konkret behöver göra för att behandla personuppgifter korrekt enligt dataskyddsförordningen, har Giva Sverige tagit fram en handledning till sina medlemmar. Den togs fram 2018 i samband med införandet av dataskyddsförordningen som ett stöd för att komma igång med arbetet. Kontakta gärna Giva Sverige på info@givasverige.se för att få tillgång till handledningen. Dessutom finns mycket bra information och stödmaterial på Integritetsskyddsmyndighetens hemsida.

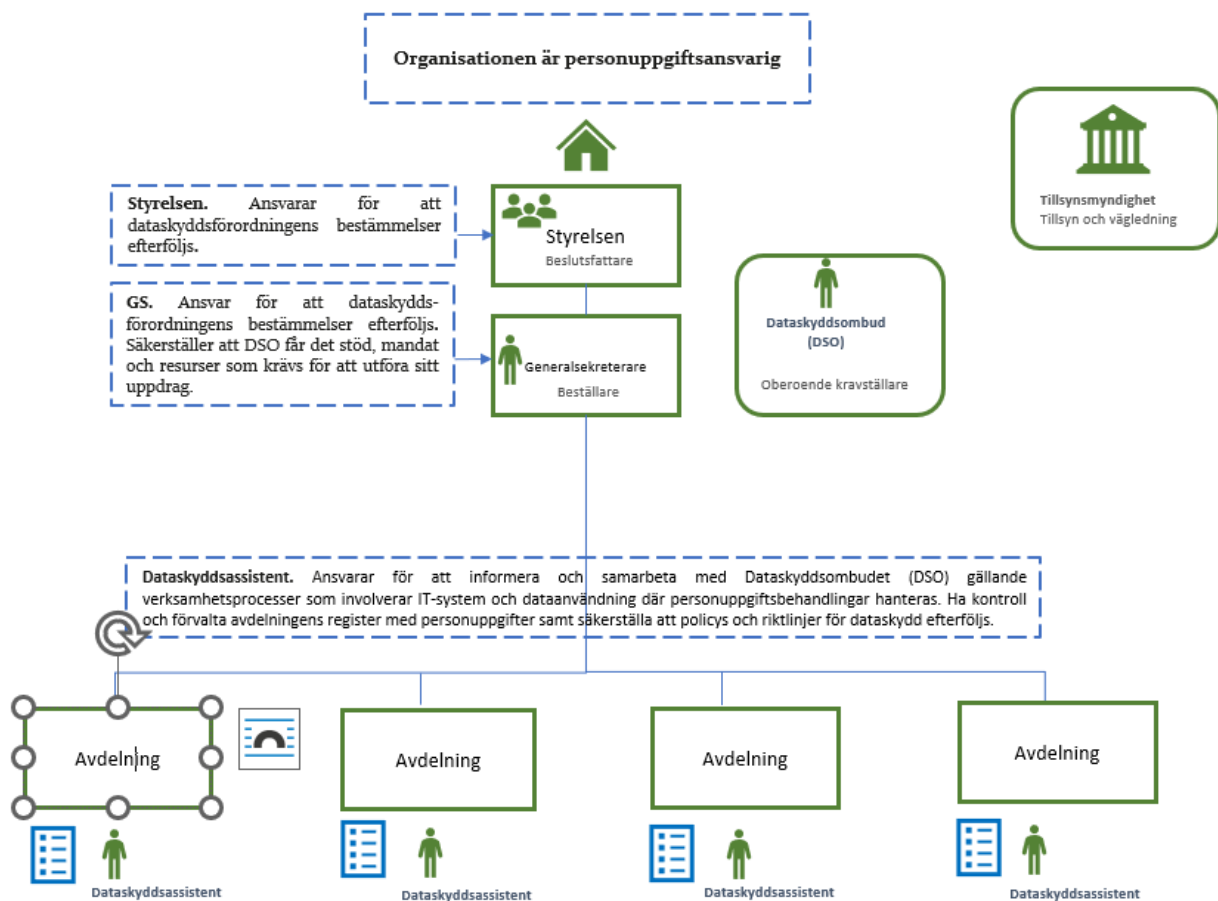
Dataskyddsförordningen i praktiken

Utöver handledningsdokumentet utarbetar Giva Sverige även praktiska råd som kan underlätta för medlemsorganisationerna i den praktiska implementeringen av dataskyddsförordningen, framför allt genom en Q&A och löpande utbildningar. Det bygger bland annat på exempel från olika medlemsorganisationer och från internationella motsvarigheter till Giva Sverige.

3. Organisationens ansvar

Varje organisation har ett ansvar att genomföra ett antal tekniska och organisatoriska åtgärder för att försäkra sig om – och kunna visa – att dataskyddsförordningen följs (Art. 5.2). Detta ansvar har i stor utsträckning att göra med dokumentation, rutiner, information och säkerhet. Bland åtgärderna märks:

- Personuppgiftsregister (Art. 30, skäl 82)
- Integritetspolicy (Art. 5.1a; Art. 5.2; skäl 39; Art. 12)
- Information om integritetspolicy (Art. 13- 14)
- Riskminimering (Art. 24-25, Art. 32-33 samt Art. 35)



(Barncancerfonden 2018)

Ansvarsstruktur inom organisationen

Giva Sveriges riktlinje för att medlemmarna ska kunna ta detta ansvar är att de ska utse en funktion med ansvar för samordning av **dataskyddsfrågor** inom organisationen. Den funktion som utses ska ha ett tydligt ansvar för att bidra till att dokumentation och rutiner skapas och hålls uppdaterade samt att organisationen därigenom håller sig informerad om utveckling i relation till dataskyddsförordningen.

För att arbetet med dataskydd ska kunna fungera så smidigt som möjligt inom organisationen är det bäst att tillsätta en arbetsgrupp för dataskyddsfrågor med representanter från olika delar av verksamheten. Detta för att säkerställa att hela organisationen kontinuerligt bevakar och anpassar behandling av personuppgifter på ett korrekt sätt.

Giva Sveriges bedömning är att de flesta ideella organisationer/medlemsorganisationer däremot **inte** behöver tillsätta ett formellt dataskyddsbud (DSO) i dataskyddsförordningens mening. Ett dataskyddsbud bör bara tillsättas i de fall det verkligen krävs, t.ex. om organisationen har som kärnverksamhet att regelbundet, systematiskt och i stor omfattning övervaka enskilda personer **eller** om det i organisationens kärnverksamhet ingår att behandla känsliga personuppgifter, t.ex. stor omfattning av

hälsouppgifter, uppgifter om etnisk eller religiös tillhörighet.

Ansvarsförhållandet mellan riksförening och lokalföreningar

För organisationer med riksförening och lokala föreningar som helt eller delvis behandlar samma personuppgifter är det viktigt att fastställa vem som är att anse som personuppgiftsansvarig. Personuppgiftsansvarig är den organisation som bestämmer ändamålet med behandlingen av personuppgifterna och hur behandlingen ska gå till.

För organisationer där riksorganisation och lokalorganisationer har gemensamt ansvar för vissa personuppgifter, t.ex. inhämtning eller uppdatering av medlemsuppgifter, måste de gemensamt bestämma vem som är personuppgiftsansvarig enligt dataskyddsförordningen. Det kan vara riksorganisationen, lokalorganisationen eller så kan de dela på ansvaret.

Om ansvaret ligger hos den ena parten, blir den andra parten personuppgiftsbiträde. I det fallet måste ett skriftligt avtal upprättas mellan parterna, ett s.k. personuppgiftsbiträdesavtal. Ett personuppgiftsbiträde behandlar personuppgifter för den personuppgiftsansvarigas räkning och ska kunna ge tillräckliga garantier för att behandlingen uppfyller kraven i dataskyddsförordningen.

Om man inom organisationen kommer fram till att riksföreningen och de lokala föreningarna har ett delat ansvar kommer alla parter att betraktas som personuppgiftsansvariga, s.k. gemensamt personuppgiftsansvar. Detta innebär att alla parter är ansvariga för att dataskyddsförordningen följs och personuppgifterna behandlas korrekt (Art. 26). Dock är det viktigt att man dokumenterar vilken part som är ansvarig för att tillse att GDPR efterföljs, då det kan vara enklare för en part att göra detta. Ett exempel är att man fastställer *vem* av parterna som är ansvarig för att säkerställa att man har informerat den enskilde medlemmen om hur behandlingen av dennes personuppgifter kommer att ske och hur denne utnyttjar sina rättigheter.

Personuppgiftsregister (register över behandling som görs inom organisationen)

Grunden för all dokumentation enligt dataskyddsförordningen GDPR är det Personuppgiftsbehandlingsregister (ett register över behandlingarna av personuppgifter som organisationen genomför) som lagen kräver att alla personuppgiftsansvariga upprättar (Art. 30). Trots att flera av Giva Sveriges medlemmar är små organisationer med få behandlingar, är Giva Sveriges riktlinje att alla medlemsorganisationer upprättar ett Personuppgiftsbehandlingsregister eftersom det skapar struktur, tydlighet och transparens (se bilaga 1).

Registret ska innehålla information om de olika sätt på vilka organisationen hanterar personuppgifter. Det ska t.ex. framgå vem som är ansvarig för ett visst register eller IT-system internt, vad registret/systemet används till, vilka typer av personer som förekommer i registret/systemet, vilka typer av uppgifter som finns i registret/systemet och med vilken

rättslig grund som uppgifterna hanteras. Registret bör föras strukturerat och digitalt, samt uppdateras löpande.

Information om organisationens ansvar

Det är viktigt att organisationen informerar om sitt ansvar när det gäller dataskydd. Detta ska ske i första hand när nya givare/medlemmar donerar/ansluter sig till organisationen för första gången. Detta görs enklast genom en kortfattad information där man sammanfattar organisationens integritetspolicy och ger individen möjlighet att ta del av den fullständiga integritetspolicyen genom att länka till den.

Dessutom så ska organisationen informera samtliga givare/medlemmar om man genomför förändringar av integritetspolicyen som kommer att innebära stora förändringar för individens integritet, som exempelvis ni vill byta rättslig grund för behandlingen. Detta ska göras innan den nya integritetspolicyen träder i kraft genom en kort sammanfattning om vad man ändrar och en länk till den nya policyen.

Personuppgiftsbiträdesavtal

För sådana personuppgifter för vilka organisationen använder en underleverantör ska personuppgiftsbiträdesavtal upprättas. Giva Sveriges riktlinje är att organisationen ska kartlägga alla leverantörer, med vilka organisationen delar personuppgifter, och upprätta personuppgiftsbiträdesavtal med dessa. Det gäller t.ex. IT-leverantörer, webbyråer, reklambyråer, givardatabasleverantörer, epost- och sms-tjänsteleverantörer m.fl.

Organisationen bör upprätta ett eget personuppgiftsbiträdesavtal för användning i relation till de leverantörer som inte själva har tagit fram ett personuppgiftsbiträdesavtal.

Vissa större internationella verksamheter har valt att ta fram en bilaga till det ursprungliga leverantörsavtalet eller användarvillkoren, oftast kallat Data Processing Addendum (DPA) som de anser ersätter biträdesavtalet. Vissa verksamheter erbjuder möjlighet att signera bilagan, andra publicerar den bara på sin webbplats. Det är viktigt att läsa igenom bilagan och kontrollera att villkoren stämmer överens med GDPR och organisationens integritetspolicy. Endast om de gör det kan tjänsten användas. Viktigt är också att löpande kontrollera eventuella uppdateringar av villkoren.

När det gäller betalcanaler är det upp till organisationen att bedöma om biträdesavtal behöver upprättas. De som behandlar betalningar har oftast en egen relation till givarna och därmed ett eget personuppgiftsansvar. Se din organisations avtal med banken för specifik information om ansvarsfördelning er emellan. De har i sin tur personuppgiftsbiträdesavtal med sina olika betalcanalsleverantörer såsom Bankgirot, Postgirot, Swish m.fl.

4. Principer för behandling av personuppgifter

GDPR kräver att organisationen ska dokumentera användningen av personuppgifter. Syftet bakom detta krav är att organisationen ska kunna visa att den tar hänsyn till de principer för behandling av personuppgifter som ställs upp i förordningen.

- **Laglighet, korrekthet och öppenhet**

Giva Sveriges riktlinje är att organisationen på ett rättvist, öppet, klart och tydligt sätt ska kunna redovisa vilka personuppgifter som samlas in, varför och med vilken rättslig grund (Art. 5.1a samt skäl 39, 58 och 60). Det innebär att organisationen ska ha följande dokumentation på plats: Personuppgiftsbehandlingsregister, Integritetspolicy och Risk- och konsekvensanalys(er).

Vidare ska organisationen informera de registrerade om de personuppgifter som behandlas t.ex. i samband med marknadsföring/kommunikation samt vid särskilda tillfällen såsom t.ex. vid dataintrång eller om den rättsliga grunden för behandling behöver ändras. Hänsyn ska tas också till annan lagstiftning, såsom bokföringslagen, liksom Giva Sveriges och andra relevanta organisationers etiska regler.

- **Ändamålsbegränsning**

Giva Sveriges riktlinje är att organisationen alltid ska kunna redovisa ett tydligt avgränsat ändamål för vilket personuppgifterna behandlas, t.ex. marknadsföring (Art. 5.1b; 6.4; 13.3; 14.4 och 89.1 samt skäl 39 och 50). Ändamålen ska vara skriftligen dokumenterat i Personuppgiftsbehandlingsregistret och kommunicerat till givaren när uppgifterna samlas in samt när givaren begär det. Personuppgifterna får inte behandlas för andra ändamål än det som angivits. Om ändamålet ändras måste givaren informeras.

- **Uppgiftsminimering**

Giva Sveriges riktlinje är att organisationen enbart ska samla in personuppgifter som är nödvändiga för att nå ändamålen med behandlingen (Art. 5.1c samt skäl 39). Uppgifterna ska vara relevanta och adekvata och dokumenterade i Personuppgiftsbehandlingsregistret. De ska inte sparas längre än nödvändigt och det ska finnas rättslig grund för behandling. Det är inte tillåtet att samla in personuppgifter för ett obestämt framtida behov. Och uppgifterna får inte behandlas om de är så gamla att de inte längre är relevanta för de ursprungliga ändamålen.

- **Korrekta personuppgifter**

Giva Sveriges riktlinje är att organisationen ska ha dokumenterade rutiner för att säkerställa att personuppgifterna de behandlar är riktiga och korrekta dvs. att de uppdateras (rättas eller raderas) på ett systematiskt och kontinuerligt sätt (Art. 5.1d samt skäl 39). Rutinerna för uppdatering ska dokumenteras i Personuppgiftsbehandlingsregistret.

- **Lagringsminimering**

Giva Sveriges riktlinje är att organisationen ska ha dokumenterade tidsfrister och rutiner för lagring av personuppgifter dvs. hur länge organisationen sparar uppgifterna i sina register/system (Art. 5.1e samt skäl 39). I de fall det inte går att uppge en exakt lagringstid ska tiden för lagring anges på ett sådant sätt att givaren kan göra en uppskattning av lagringstiden. Uppgifterna får i inget fall sparas under en längre tid än vad som är nödvändigt för ändamålen. När uppgifterna inte längre behövs för de ändamålen ska de gallras, d.v.s. raderas, avidentifieras eller arkiveras i enlighet med Art. 89. Arkivering enligt Art. 89 innebär att personuppgifterna kan sparas längre endast om det finns arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål samt lämpliga skyddsåtgärder för de registrerades rättigheter (läs mer om gallring under punkten 7 nedan). Tidsfrister och rutiner för lagring ska dokumenteras i Personuppgiftsbehandlingsregistret.

- **Integritet och konfidentialitet**

Giva Sveriges riktlinje är att organisationen ska ha kontroll över var och hur personuppgifter samlas in och sparas samt vem som har tillgång till dem (Art. 5.1f och 32 samt skäl 39 och 83). Dessutom ska organisationen vidta adekvata skyddsåtgärder så att inte obehöriga får tillgång till uppgifterna. Det kan handla om att minimera antalet uppgifter (rutiner för uppgiftsminimering); begränsa åtkomst (rutiner för behörighetskontroll); skydda personuppgifter (rutiner för autentisering, anonymisering, kryptering m m); bygga system som är användarvänliga och har tydligt fokus på integritet (Privacy by Design) samt att göra riskanalyser (PIA) och konsekvensbedömningar (DPIA). Säkerhetsåtgärder samt risk- och konsekvensbedömningar ska dokumenteras i Personuppgiftsbehandlingsregistret.

5. Rättslig grund för behandling

GDPR har sex (6) rättsliga grunder för behandling av personuppgifter. Grunderna är jämbördiga och det betyder att de har samma "tyngd" dvs. ingen grund är starkare än någon annan. För rättvis behandling av personuppgifter måste organisationen ha stöd i någon av dessa rättsliga grunder. Giva Sveriges bedömning är att fyra (4) av grunderna är aktuella för Giva Sveriges medlemmar:

- Samtycke (Art. 6.1a)
- Fullgörande av avtal (Art. 6.1b)
- Rättslig förpliktelse (Art. 6.1c)
- Berättigat intresse (Art. 6.1f)

Samtycke

Samtycket är den av de rättsliga grunderna som är den mest långlivade samtidigt som den kan vara den som är den med kortast livslängd. Samtycket gäller nämligen till dess att den som givit samtycket återkallar det. Samtidigt så är samtycket den grund som kräver mest av den som samlar in det, då denne endast får göra det den har informerat individen om – det finns inget utrymme för tolkning. I GDPR definieras samtycke som en frivillig, specifik, informerad och otvetydig viljeyttring, genom vilken givaren, antingen genom ett uttalande eller genom en entydig bekräftande handling, godtar behandling av sina personuppgifter (Art. 4.11).

Det innebär att samtycke i form av t.ex. förkryssade rutor inte längre fungerar som samtycke till behandling av personuppgifter då samtycke kräver en aktiv handling från den vars samtycke önskas. Samtycke enligt GDPR får inte vara tvingande och t.ex. krävas för genomförande av avtal eller tillhandahållande av tjänst, det måste finnas ett alternativ. Förordningen kräver att fråga om samtycke ska särskiljas och ställas separat i en text som rör flera olika frågor (Art. 7, skäl 32, 33, 42 och 43).

Krav på samtycke

I vissa fall kräver GDPR samtycke för att organisationen ska få behandla personuppgifter:

- Barns personuppgifter i samband med informationssamhällets tjänster (Art. 8)
- Personuppgifter som avslöjar ras² eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse eller medlemskap i fackförening och behandling av genetiska uppgifter, biometriska uppgifter för att entydigt identifiera en fysisk person, uppgifter om hälsa eller uppgifter om en fysisk persons sexualliv eller sexuella läggning (Art. 9.1)
- Det finns dock undantag från samtyckeskravet i Art. 9.1 för medlemskap i organisationer som t.ex. är ett religiöst samfund (Art. 9.2)

Då GDPR utöver kraven ovan (Art. 8-9) inte ställer krav på samtycke för behandling av personuppgifter är Giva Sveriges bedömning är att medlemsorganisationerna i första hand ska luta sig mot en annan rättslig grund än samtycke när det är möjligt. Detta för att minimera resurskrävande administration och information.

Fullgörande av avtal

När det gäller den rättsliga grunden avtal, kan den användas för behandling av personuppgifter som kan knytas direkt till de personuppgifter som krävs för fullgörandet av avtalet. En gåva är ett exempel på avtal mellan givaren och organisationen. För att gåvan ska genomföras är det nödvändigt för organisationen att erbjuda möjlighet till inbetalning av

² Notera att "ras" är en term som används i den officiella svenska förordningstexten och inte är ett val av Giva Sverige.

gåvan. Det sker ofta genom att skicka betalningsunderlag med post eller epost till givaren, vilket innebär processande av namn- och adressuppgifter som en nödvändighet för att fullgöra avtalet. Efter det att gåvan betalats torde det inte gå att använda fullgörande av avtal som rättslig grund för vidare kommunikation med givaren. För det behövs annan rättslig grund.

Tack för gåva är en del i avtalet

Giva Sveriges riktlinje är att en bekräftelse på att en gåva kommit organisationen tillhanda är att betrakta som en formell del i gåvotransaktionen. Giva Sverige anser därför att organisationen har rätt att skicka ett tackmeddelande till givaren som ett kvitto på gåvan, t.ex. i form av ett sms³. Det gäller även i samband med gåvor som skänks direkt via betalkanal dvs. gåvor från givare vars personuppgifter organisationen inte har i sina system (t.ex. gåvor via Swish, sms, spontana inbetalningar etc.). För att det ska vara möjligt för organisationen att registrera personuppgifter som inkommit direkt via t.ex. Swish i sin givardatabas för vidare behandling, krävs att organisationen informerar givaren om detta. Informationen ska förmedlas i tack-meddelandet, där det ska framgå med vilken rättslig grund organisationen registrerar och behandlar personuppgifterna. Den rättsliga grunden kommer oftast att vara berättigat intresse (för användning i informations- och marknadsföringssyfte, se längre ner i detta kapitel), men kan också vara samtycke. Denna information ska också innehålla en länk till Integritetspolicyen vilket därmed möjliggör för individen att kunna ta del av den fullständiga informationen om hur organisationen avser att behandla dennes personuppgifter.

Om organisationen hävdar samtycke som rättslig grund måste tackmeddelandet ge möjlighet till samtycke enligt de krav som ställs för detta (se ovan). Om organisationen hävdar berättigat intresse som rättslig grund måste tack-meddelandet informera om hur givaren kan avböja fortsatt behandling och – om möjligt – avregistrera sig direkt.

Rättslig förpliktelse

När det gäller den rättsliga grunden rättslig förpliktelse, krävs att behandlingen är nödvändig på grund av en annan lag. Giva Sveriges bedömning är att det i insamlingshänseende mest relevanta exemplet på rättslig förpliktelse är bokföringslagens krav på att spara räkenskapsinformation i sju år. Givaren måste få information om vilka personuppgifter som samlas in med grund i rättslig förpliktelse.

³ Det går även att kontakta organisationens bank och be om deras hjälp att infoga en hänvisning till organisationens integritetspolicy i den betalningsbekräftelse som kommer från Swish. T.ex. har Swedbank hjälpt någon medlemsorganisation med detta.

Berättigat intresse

När det gäller den rättsliga grunden berättigat intresse, ger den möjlighet att behandla personuppgifter från en individ om organisationen på ett tydligt sätt har **informerat** givaren **om ändamålet** dvs. vad man avser att göra med personuppgifterna samt **varför** organisationen anser sig ha **berättigat intresse**.

Ett exempel på ändamål för vilket berättigat intresse kan hävdas som rättslig grund för behandling av personuppgifter är direktmarknadsföring. Det framgår uttryckligen av dataskyddsförordningen, skäl 47. I direktmarknadsföring kan mycket av det insamlingsorganisationen gör innefattas, t.ex. existerande och potentiella givare/medlemmar (te x brev) samt riktad marknadsföring av olika typer.⁴ I samband med direktmarknadsföring måste organisationen dock informera individen om möjligheten att avböja sådan.

Andra exempel på ändamål för vilka Giva Sverige bedömer att berättigat intresse kan användas som rättslig grund för behandling av personuppgifter, men där individen *inte* måste erbjudas möjlighet att avböja behandling, är:

- Tack för gåva
- Profilerings, segmentering och analys
- Prospekt research
- Undersökning

Intresseavvägning

När organisationen väljer att använda berättigat intresse som rättslig grund för behandling av personuppgifter, ska detta ska dokumenteras i form av en intresseavvägning.

Intresseavvägningen innehåller i tre huvudsakliga steg:

1. Vilket intresse (ändamål) anser organisationen är berättigat?
2. Är det nödvändigt för organisationen att behandla personuppgifter för ändamålet?
3. Inskränker behandlingen den registrerades rättigheter i något avseende?

Om intresseavvägningen visar att det är nödvändigt att behandla personuppgifterna för att nå ändamålet och den registrerades intressen, rättigheter och friheter inte väger tyngre med beaktande av deras rimliga förväntningar, är sannolikheten stor att berättigat intresse föreligger.

Precis som med alla rättsliga grunder måste givaren – i linje med principen om laglighet, korrekthet och öppenhet – informeras om personuppgiftsbehandling med stöd i berättigat intresse. I informationen måste syftet och det berättigade intresset vara tydligt uttalat. Dock krävs inte någon aktiv handling från den registrerades sida, såsom i samband med samtycke,

⁴ När det gäller kalla utskick med epost och sms eller kalla samtal är det viktigt att också hålla koll på marknadsföringslagstiftning och Giva Sveriges riktlinjer för detta.

för att bekräfta att informationen gått fram.

6. Sparande av personuppgifter

Dataskyddsförordningens huvudregel är att behandling av personuppgifter endast får fortgå så länge som det är *nödvändigt* för angivna ändamål (Art. 5.1e, skäl 39). Det betyder att organisationen endast får lagra (spara) personuppgifter så länge som det är nödvändigt. Hur länge det är framgår dock inte, utan det är personuppgiftsansvarig som måste analysera och motivera de egna behoven.

Spara med berättigat intresse som rättslig grund

När Giva Sverige analyserat behoven i insamlingsbranschen är Giva Sveriges riktlinje att personuppgifter, som sparas med berättigat intresse som rättslig grund, får sparas i upp till 36 månader (3 år) efter det att den senaste gåvan registrerades.

Bakgrunden till Giva Sveriges rekommendation är att givande av gåvor uppträder cykliskt och ofta med långa intervall. Data visar att i upp till 36 månader är personer som gett en gåva mer benägna att ge igen än personer som aldrig gett. Om organisationen behöver förnya insamling av personuppgifter oftare kommer kostnaden för administration att öka avsevärt. En ökad administrationskostnad ligger inte i givarens intresse; givaren vill att så stor del som möjligt av gåvan ska gå till ändamålet. Det torde gälla även om givaren inte väljer att skänka en gåva under en period dvs. oavsett om givaren ger eller inte vill hen med största sannolikhet att en så stor del de gåvor som skänks till organisationen ska gå till ändamålet. Sparande av personuppgifter i 36 månader har dessutom varit gängse i insamlingsbranschen under många år.

Giva Sveriges rekommendation om lagring i upp till 36 månader (3 år) betyder inte att organisationen uppmanas att spara alla personuppgifter som har berättigat intresse som rättslig grund så länge. Organisationens behov gör en behovsanalys för olika typer av givande då dataskyddsförordningens skäl 39 säger att det ska tillses att den period under vilken personuppgifterna lagras är begränsad till ett strikt minimum. T.ex. när det gäller testamenten rekommenderar Giva Sverige istället att personuppgifterna lagras så länge det behövs för att testamentet ska kunna behandlas och därefter gallras från personuppgifter.

Spara med annan rättslig grund

För personuppgifter som behandlas med annan rättslig grund än berättigat intresse gäller annan lagringstid (tid för sparande). Samtycke gäller till dess det att den registrerade återkallar sitt samtycke, fullgörande av avtal så länge avtalstiden löper och rättslig förpliktelse så länge den rättsliga förpliktelsen gäller, t.ex. bokföringslagen 7 år.

Den registrerade måste få information om lagringstid i samband med all behandling av personuppgift.

7. Gallring av personuppgifter

I enlighet med dataskyddsförordningens skäl 39 ska den personuppgiftsansvariga införa tidsfrister för regelbunden kontroll eller radering av personuppgifter för att säkerställa att de inte sparas längre än nödvändigt.

Giva Sveriges riktlinje är att gallring av personuppgifter ska ske regelbundet och vara en integrerad del i organisationens dataskyddsarbete. Om den registrerade inte varit aktiv inom 36 månader (3 år) ska personuppgifterna tas bort från givardatabasen. Om tiden för lagring är en annan ska personuppgifterna tas bort efter den lagringstiden. Gallring av personuppgifter kan dessutom ske stegvis. Om en delmängd av en personuppgift inte är nödvändig att behålla kan den tas bort innan personuppgiften tas bort helt.

Det finns tre alternativa metoder som organisationen kan använda sig av för gallring av personuppgifter:

- **Radering**
Radering innebär att personuppgifterna raderas helt från givardatabasen. I sammanhang där givaren uttryckligen kräver att alla personuppgifter ska raderas är detta alternativ det som ska tillämpas. Ofta finns det dock ett intresse att vissa data sparas, t.ex. i anonymiserad form eller för arkivändamål, se nedan.
- **Anonymisering**
Anonymisering innebär att en delmängd av personuppgifterna är kvar i givardatabasen, men i en form där givaren oidentifierats dvs. där samtliga uppgifter som kan identifiera givaren (även indirekt) har tagits bort. Vid anonymisering går det inte att återskapa ursprungsinformationen om givaren, men uppgifterna kan fortfarande användas för t.ex. statistik eller analys av givarbeteenden.
- **Arkivering**
Arkivering innebär att personuppgifterna är kvar i databasen för att organisationen bedömer att personuppgifterna kan vara av allmänt intresse eller för att de kan komma att behöva användas för vetenskapliga, historiska eller statistiska ändamål (Art. 5.1b, skäl 50 samt skäl 158, 159, 160 och 162). Dock måste ett antal tekniska (t.ex. pseudonymisering) och organisatoriska (t.ex. behörighetsbegränsning) skyddsåtgärder iakttas vid arkivering (Art. 89).

Giva Sveriges bedömning är att varken radering eller arkivering av personuppgifter är något som är aktuellt i någon större utsträckning för Giva Sveriges medlemmar när det gäller givardata. Radering utesluter analys och statistik, och arkivering behövs inte användas som grund om uppgifterna anonymiseras eftersom GDPR då inte längre är tillämplig.

Arkivering, och då huvudsakligen för vetenskapliga eller historiska forskningsändamål eller för statistiska ändamål, behöver bara användas i de sammanhang då det finns särskild anledning att *inte* anonymisera uppgifterna.

Om arkivering används är Giva Sveriges riktlinje att organisationen ska göra en ny intresseavvägning för att säkerställa vidare behandling inte kränker den registrerades rättigheter och friheter (Art. 6.4). Den registrerade behöver dock inte informeras på nytt om arkiveringsändamålet.

8. Integritetspolicy och informationstexter

Ett genomgående krav i GDPR är kravet på öppenhet (Art. 5.1a; Art. 5.2; skäl 39; Art. 12; Art. 13-14; Art. 15-22 samt Art. 34). Öppenheten manifesteras lämpligen genom en informationssida på webben (ofta kallad "integritetspolicy", "Privacy Notice" eller "personuppgiftspolicy"). Genom en sådan sida visar organisationen sitt övergripande ansvar i integritetsfrågor. Utöver informationssidan kräver GDPR att personuppgiftsansvarig informerar den registrerade i samband med att personuppgifter samlas in (Art. 13-14) och behandlas. Det handlar om information för t.ex. webben, annonser, kampanjer, utskick, tackmeddelanden m m.

Fullständig information till registrerade

Giva Sveriges riktlinje är att organisationen ska ta fram information för personuppgiftshantering som är unik för organisationen, dvs. baseras på de ändamål, behandlingar och rutiner som organisationen har, och som är riktad till externa användare. Informationen ska ge en detaljerad beskrivning av varför och hur organisationen behandlar personuppgifter samt hur organisationen möter den registrerades rättigheter. Följande områden ska täckas in av informationen:

- **Allmänt**
Kortfattad beskrivning varför informationen är viktig för organisationen och verksamheten samt vilken roll organisationen har i relation till givaren (oftast personuppgiftsansvarig).
- **Personuppgifter som behandlas**
Exempel på vilka personuppgifter som inhämtas och behandlas samt hur och i vilket syfte (t.ex. givande eller medlemskap).
- **Ändamålen för behandling**
Lista hur personuppgifterna som samlas in användas, t.ex. för att:
 - Fullgöra beställningar av tjänster via plattform som erbjuds av organisationen;

- Möjliggöra god service, som att hantera givarfrågor, rätta felaktiga uppgifter eller skicka information t.ex. nyhetsbrev;
 - Analysera givarbeteende i marknadsföringssyfte eller för att skicka erbjudanden av generell eller riktad karaktär;
 - Administrera och analysera givarprofiler samt genomföra marknadsundersökningar;
 - Administrera system och ta fram statistik om givarbeteende på aggregerad nivå (dvs. utan att identifiera givare som individ);
 - M.fl.
- **Uppgifter som kan överföras utanför den inre marknaden (EU och EES)**
Information om vilka personuppgifter som kan överföras utanför den inre marknaden (dvs. EUs medlemsstater samt Norge, Island och Lichtenstein), t.ex. via en molntjänst.
 - **Rättslig grund, lagring och gallring av personuppgifter**
Information om vilken/vilka rättslig(a) grund(er) som används, hur länge personuppgifter lagras samt hur och när personuppgifterna gallras.
 - **Samtycke som rättslig grund**
Information om att, i de fall samtycke används som rättslig grund, samtycket ska erhållas via ett separat stycke som berör exakt hur personuppgifterna ska användas och hur de samlas in.
 - **Cookies**
Information om hur organisationen använder cookies på webbplatsen/-erna eller i appar.
 - **Länkar till andra webbplatser**
Information om att vid länkar från organisationens webbplats till andra webbplatser, så gäller deras GDPR-information.
 - **Givarens rättigheter och val**
Information om givarens rättigheter, t.ex. vart givaren ska vända sig för att t.ex. tacka nej till direktmarknadsföring; be att få uppgifter rättade eller raderade eller be om ett registerutdrag. Det ska även finnas information om givarens rätt att klaga till tillsynsmyndigheten.
 - **Kontaktuppgifter**
Informationen om hur organisationen kan kontaktas.
 - **Datum som informationen börjar gälla**

Information till allmänheten och givarna/medlemmarna

I samband med insamling av personuppgifter ska organisationen informera allmänheten och givarna/medlemmarna om integritetspolicyn och hur personuppgifter behandlas.

Informationen ska utformas på ett kortfattat, lättåtkomligt och lättbegripligt sätt, med ett tydligt och enkelt språk (Art. 13–14). Den kan förmedlas elektroniskt, t.ex. på webbplatsen eller som en del av ett kampanjutskick med post, epost eller sms. Giva Sveriges riktlinje är att informationstexten ska innehålla:

- Kontaktuppgifter personuppgiftsansvarig
- Ändamål med och rättslig grund för behandling
- Information om berättigat intresse
- Andra som ev. får del av personuppgiften (t.ex. molnleverantörer)
- Om personuppgiften delas med tredje land (land utanför EU)

Informationen ska vidare innehålla en länk eller annan hänvisning till organisationens fullständiga integritetspolicy av vilken bl.a. givarens rättigheter och hur dessa utövas ska framgå på ett tydligt sätt. Det finns flera olika sätt som sådana här informationstexter eller integritetsmeddelanden kan utformas:

Lager av information

För att integritetsmeddelandet ska vara lättillgänglig är en möjlighet att använda lager av information på webbplatsen och framförallt på mobila enheter. Det innebär att informationen levereras stegvis med ett första lager i form av en rubrik av typen "Hur använder vi dina uppgifter?"; det andra lagret i form av en kortfattad information om hur uppgifterna används och delas, t.ex. "Administrera din gåva, förenkla ditt besök på vår webbplats och – baserat på berättigat intresse – skicka information till dig om nya möjligheter att skänka en gåva"; och det tredje lagret hänvisar till integritetspolicyn med en länk.

Just-in-time

Ett annat sätt att göra integritetsmeddelandet lättillgänglig är att skapa popup-meddelanden i de formulär på webbplatsen där personuppgifter samlas in, t.ex. ett meddelande av typen "Vi registrerar ditt personnummer för att kunna särskilja din gåva från andras gåvor", "Vi behöver ditt personnummer för att säkerställa att uppgifterna om dig är korrekta i vårt register" eller "Vi behöver ditt personnummer för att kunna säkerställa din identitet" som kommer fram i form av en pratbubbla när besökaren sveper med musen över fältet för personnummer.

9. Säkerhet och inbyggt dataskydd

GDPR kräver att lämpliga tekniska och organisatoriska åtgärder tas för att värna dataskyddsprinciperna på ett effektivt sätt och för att integrera nödvändiga skyddsåtgärder i behandlingen (Art. 32). Åtgärderna ska dock stå i proportion till behandlingen.

Giva Sveriges riktlinje är att organisationen ska göra kontinuerliga riskanalyser av sin behandling av personuppgifter (Privacy Impact Analysis, PIA) och med stöd i dessa fortlöpande identifiera lämpliga säkerhetsåtgärder. I riskanalyserna ska särskild hänsyn tas till risk för oavsiktlig eller olaglig förstöring, förlust eller ändring eller obehörigt röjande eller obehörig åtkomst. Om en risk bedöms vara hög ska organisationen alltid göra en konsekvensbedömning (Data Protection Impact Analysis, DPIA)⁵, Art. 35. Det kan gälla t.ex. behandling av känsliga personuppgifter eller i samband med införandet av ny teknik i organisationen. Men det kan vara bra att genomföra konsekvensanalyser även i andra sammanhang, då de är ett bra sätt att förebygga risker innan de uppkommer. Risk- och konsekvensanalyser ska dokumenteras.

Lämpliga säkerhetsåtgärder som minskar risken med behandling kan handla om rutiner för att:

- Minimera antalet uppgifter, dvs. enbart behandla personuppgifter som är nödvändiga för ändamålet (vilket omfattar mängden insamlade personuppgifter, behandlingens omfattning, tiden för deras lagring och deras tillgänglighet);
- Begränsa åtkomst, dvs. behörighetskontroll;
- Skydda personuppgifter, dvs. att autentisera, pseudonymisera (att personuppgifterna inte kan kopplas till en specifik individ utan att kompletterande information, som förvaras tekniskt och organisatoriskt avskilt, krävs) eller kryptera personuppgifterna;
- Inbyggt dataskydd (Privacy by Design), dvs. att vid upphandling av nya system tillse att dessa är användarvänliga och har inbyggt fokus på integritet;
- Dataskydd som standard (Privacy by Default), dvs. system och rutiner för att personuppgifter inte behandlas i onödan, t.ex. i form av förvalda inställningarna som är satta så att inte mer information än nödvändigt samlas in, delas ut eller visas.

10. Publicering av bilder, filmer och ljud⁶

GDPR betraktar teckningar, foton, filmer och ljudfiler som personuppgifter om de avbildar människor eller innehåller röster från människor. Men ändamålet med behandling avgör om GDPR är tillämplig eller ej.

⁵ För svensk vägledning kring konsekvensbedömning, se integritetsskyddsmyndighetens webbplats: <https://www.imy.se/lagar--regler/dataskyddsforordningen/konsekvensbedomningar-och-forhandssamrad/sa-har-gor-man-en-konsekvensbedomning/>

⁶ Att Giva Sverige särskilt tar upp denna kategori av personuppgifter beror på att flera medlemmar frågat specifikt om vägledning i hantering av bilder, filmer och ljud. Integritetsskyddsmyndigheten har bra information om bilder och ljud på sin webbplats: <https://www.imy.se/verksamhet/dataskydd/vi-guidar-dig/publicera-bilder-filmer-och-ljud-pa-internet/>

Om ändamålen är journalistiska, konstnärliga eller litterärt eller akademiskt skapande så undantas de från GDPR, oavsett om tryckfrihetsförordningen (TL) eller yttrandefrihetsgrundlagen (YGL) gäller i sammanhanget. Ett exempel på journalistiska ändamål skulle kunna vara användning av bilder och ljud i t.ex. medlemstidningar. Gränsdragningen mellan vad som är att betrakta som journalistiska ändamål och mer allmänna informationsändamål är dock inte alldeles tydlig, vilket gör att det kan vara bra att ha som utgångspunkt att GDPR ändå gäller.

När GDPR är tillämplig krävs rättslig grund för behandling av bilder, filmer och ljud. De rättsliga grunder som är aktuella är samtycke eller berättigat intresse. Vilken grund som ska användas bestäms utifrån en rimlighetsbedömning. Om det gäller bilder på en person eller några få personer som är tydligt identifierbara behövs samtycke. Om det gäller mingelbilder räcker berättigat intresse oftast som grund för behandling. Om samtycke används bör det vara skriftligt.

Oavsett vilken rättslig grund som används, krävs att de vars uppgifter behandlas får rimlig information om behandlingen. Informationen kan t.ex. finnas med i inbjudan till event och/eller förmedlas på event genom tydliga skyltar, så att deltagarna görs medvetna om att fotografering/filmning och/eller ljudupptagning sker samt att bild eller ljud kan komma att användas för publicering i medlemstidning, på webbplats eller liknande.

När det gäller bilder, filmer och ljud (t.ex. bildbanker eller marknadsföringsmaterial) som producerats före 25 maj 2018, för vilka rättslig grund enligt GDPR inte är tydliggjord, krävs en analys av om organisationen kan använda berättigat intresse eller om samtycke krävs för att behålla och använda materialet. Giva Sveriges bedömning är att berättigat intresse torde fungera som rättslig grund för äldre material, men att skriftligt samtycke bör inhämtas om materialet ska fortsätta användas för publicering och om det innehåller bilder, filmer eller ljud på en person eller några få tydligt identifierbara personer.

11. Publicering på sociala medier⁷

När det gäller sociala medier är den specifika sociala medieplattformen oftast personuppgiftsansvarig för sina tjänster.

Undantagsvis kan det sociala mediet vara personuppgiftsbiträde till organisationen. I de fallen utgör de sociala mediernas villkor ett slags personuppgiftsbiträdesavtal (se s 6). Ett exempel på detta är Facebooks tjänst "datafil för anpassade målgrupper". Eftersom de sociala medieplattformarnas villkor är ensidigt uttryckta är det extra viktigt att regelbundet

⁷ Att Giva Sverige särskilt tar upp denna kategori av personuppgifter beror på att flera medlemmar frågat specifikt om vägledning i sociala medier. Integritetsskyddsmyndigheten har bra information om bilder och ljud på sin webbplats: <https://www.imy.se/verksamhet/dataskydd/vi-guidar-dig/publicera-bilder-filmer-och-ljud-pa-internet/>

kontrollera att de motsvarar organisationens integritetspolicy och når upp till kraven i dataskyddsförordningen. Om så inte är fallet ska tjänsten inte användas.

I övrigt när det gäller sociala medier och integritet, så är det alltid organisationens ansvar att behandla personuppgifter på ett sätt som inte är kränkande (enligt lagen om elektroniska anslagstavlor, den s k BBS-lagen). Det betyder bl.a. att användarkommentarer på organisations profil ska tas bort "skyndsamt" om de är kränkande. Därför krävs lämpliga säkerhetsåtgärder i arbetet med sociala medier, t.ex. instruktioner kring hur kommentarsfält är tänkta att användas och regler kring vad som kan tas bort, och hur, eller inte får förekomma. Organisationen kan också uppmuntra till att rapportera kränkande innehåll och ha rutiner för att hantera klagomål. Som intern säkerhetsåtgärd behöver organisationen även ge instruktioner till dem som arbetar med de sociala medierna angående hur de ska skötas (policy för sociala medier eller annan typ av handledning).

Avslutningsvis när det gäller sociala medier kan konstateras att (privata) kampanjer via sociala medier visserligen kan ge organisationen en hel del intäkter, men att de inte bygger givarregister. Det är det sociala mediet som är personuppgiftsansvarigt och det är det sociala mediet, och inte organisationen, som får personuppgifterna i samband med kampanjerna.

12. Medlemsregister

Medlemskap i en ideell förening baseras normalt sett på fullgörande av avtal som rättslig grund. Det betyder att när en medlem i en förening avslutar sitt medlemskap bör medlemmens uppgifter i medlemsregistret tas bort. Inget hindrar att uppgifter om medlemmen får finnas kvar till dess att denne exempelvis har betalat utestående medlemsavgifter och lämnat tillbaka lånad utrustning. Om den tidigare medlemmen inte uttryckligen tackat nej till att återigen bli medlem kan organisationen spara hans personuppgifter i upp till 36 månader (3 år) efter senast utgången medlemskap. Den rättsliga grunden för detta är berättigat intresse, vilket baserar sig på samma analys som den som gjorts för givare dvs. många medlemmar återkommer som aktiva inom 36 månader (3 år). Att analysen är densamma för medlemmar som för givare grundar sig på att i många av Giva Sveriges medlemsorganisationer behandlas medlemmar och givare på samma sätt; många gånger är det medlemmarna som är givare.

Bilaga 1.

Exempel på förhållande mellan registrerade, syften och IT-system

