

Vad innebär dataskyddsförordningen GDPR?

Syftet är att stärka skyddet för (levande) fysiska personer avseende behandling av deras personuppgifter. Mycket påminner om tidigare PUL men i några väsentliga delar är kraven högre, och undantag som fanns i PUL för "ostrukturerad data" (missbruksregeln) gäller inte längre. Med ostrukturerad data menas bland annat löpande text, enklare listor, bilder och filmer, protokoll och epost. Både lokalavdelningen och förbundet nationellt måste definiera tydligare varför och hur vi hanterar personuppgifter. Vi får inte hantera (samla in, lagra, eller publicera) uppgifter som inte behövs för eller inte är relevanta för verksamheten. Det måste vara tydligt för den person vi behandlar uppgifter om; att vi gör det, vilka uppgifter vi behandlar, varför samt vilka rättigheter personen har gentemot oss som hanterar uppgifterna. Myndigheten Datainspektionen har större möjlighet för tillsyn och kan utdöma sanktioner och högre viten än tidigare. Den nya lagen beskriver också hur exempelvis stölder av personuppgifter eller intrång i register måste anmälas.

Informera mer, spara mindre – de viktigaste principerna

Lagtexten innehåller en lång rad regler och krav för hur personuppgifter får hanteras i en organisation. Dessa ger dock inte särskilt mycket vägledning hur vi som ideell förening bäst behandlar personuppgifter om medlemmar, deltagare, ledare, anhöriga och andra, i eller nära vår verksamhet. Dessutom saknas fortfarande vägledning, tillämpning och praxis för sådant som är säregnet för ideella föreningar och svenskt föreningsliv. Det gör att många frågor ännu är obesvarade och förväntningarna på ideella föreningar måste motsvara de förutsättningarna.

För att ändå kunna ta sig an alla dessa regler, skäl och annan juridisk text i förordningen kan vi sammanfatta det i några grundläggande principer:

- Samla in och hantera personuppgifter endast om det uppfyller villkoren i lagen.
- Bestäm i förväg vad personuppgifterna ska användas till och använd inte uppgifterna för något annat ändamål.
- Informera de personer vars uppgifter ni samlar in, vad uppgifterna ska användas till och att de har rättigheter till sina egna uppgifter.
- Samla inte in fler personuppgifter än vad som behövs. Samla aldrig in personuppgifter därför att det kan vara "bra att ha".
- Se till att personuppgifterna är korrekta och uppdaterade.
- Radera personuppgifter som inte längre behövs.
- Skydda uppgifterna från otillåten användning och obehörig åtkomst.
- Skriv ner hur ni i föreningen har tänkt i er hantering av personuppgifter.

Om vi förenklar dessa grundläggande principer ännu lite till, så kommer ni långt genom att bara tänka på de här tre punkterna:

1. Samla inte in fler personuppgifter än nödvändigt och enbart för ett visst, i förväg bestämt, ändamål.
2. Spara inte uppgifter längre än nödvändigt.
3. Skydda de personuppgifter ni hanterar i föreningen.

Medlemsregister

Medlemsregistret är det enskilt största systemet för hantering av personuppgifter i Förbundet, och på förbunds nivå måste vi göra det vi kan för att allt som hanteras i och av oss ska följa dataskyddsförordningen. Det är viktigt att komma ihåg att förordningen omfattar all hantering och lagring av personuppgifter, även utanför medlemsregistret. Det kan till exempel vara medlemslappar, lägeranmälningar, medlemslistan i pärmen, protokoll, hemsida, mail, molntjänster osv. Här tillkommer också personuppgifter som i förordningen betraktas som känsliga eller särskilt skyddsvärda och därmed ställer högre krav, som uppgifter om hälsa och allergi, personnummer, skyddade identiteter samt uppgifter om barn under en viss ålder (som regeringen inte fastställt än).

Checklista för föreningen

Det här är fem grundläggande frågor att ställa i föreningen när ni börjar ert arbete med dataskyddsförordningen och hur er förening förhåller sig till den. Styrelsen i en förening ansvarar för att lagen följs men fundera på om ni kan utse en person eller arbetsgrupp som leder arbetet. Under några av frågorna finns dokument att ladda ner som stöd i ert arbete.

Hur ser det ut idag?

Vilka samlar in personuppgifter och hur? Vilka sköter medlemsregistreringen? Vilka personuppgifter behandlar vi? I vilka andra system och register behandlar vi dessa personuppgifter och på vilken laglig grund? Hur avgör vi vilka uppgifter vi behöver samla in? Behöver vi uppdatera information, utskick eller material till medlemmar och allmänhet?

Dokument för nedladdning:

Instruktioner till inventeringen av församling och förening (Word) Förslag inventeringsmall Dataskyddsförordningen (Excel)

Vilka risker finns?

Vilken typ av uppgift har störst risk att leda till skador eller kränkningar för individen om de sprids? Vilken av sätten att behandla uppgifter vi använder idag bär störst risker för att misslyckas med att leva upp till kraven? Börja arbeta med dessa först.

Vad får vi inte längre hantera eller spara?

Samlar vi in uppgifter idag som vi inte längre får samla in? Ligger information och skräpar eller sparar vi på uppgifter som inte behövs längre? Vad behöver arkiveras? Om ni inte längre har berättigat ändamål eller lagstöd ska uppgifter raderas. Uppgifter som behöver sparas men inte behövs för daglig verksamhet ska arkiveras.

Vilken målsättning har vi?

Sätt mål för hur ni ska behandla personuppgifter genom t.ex. instruktioner och rutinbeskrivningar. Exempel på dokumentation som kan behövas ta fram är en instruktion för arkivering/gallring som beskriver hur och när ni ska gallra personuppgifter. Det är också bra att ta fram rutinbeskrivningar för hur ni ska upptäcka och rapportera en personuppgiftsincident mm. Detta kan samlas ihop till en integritetspolicy eller liknande.

Hur ska det göras och av vem?

Se över system för att säkerställa att en målsättning/policy ni sätter följs och att åtgärder ni bestämt blir gjorda. Dokumentera arbetet så att ni både själva och för Datainspektionen kan visa vad ni har gjort och vill göra. Viktigt att komma ihåg att också utbilda ledare och ev. anställda i hur personuppgifter ska hanteras.

Tips på för fördjupning: www.datainspektionen.se