

DSF (GDPR) – Ny lag om personuppgifter



Innehåll

| | |
|--|----------|
| Dataskyddsförordningen | 3 |
| Behandling av personuppgifter | 3 |
| Vilka är de viktigaste nyheterna för din förening? | 3 |
| Förbundets personuppgiftsansvarige och integritetspolicy | 4 |
| Läs mer | 4 |
| Checklista och förebyggande åtgärder | 5 |
| Vad är en personuppgift? | 6 |
| Vad är känsliga personuppgifter? | 6 |

Dataskyddsförordningen

Dataskyddsförordningen DSF (ofta även kallad GDPR, som är en förkortning av det engelska namnet) är en ny lagstiftning som stärker individens rättigheter över hur organisationer samlar in och hanterar personuppgifter. Genom denna blir det hårdare krav på hanteringen av personuppgifter. DSF träder i kraft den 25 maj 2018 och ersätter då Personuppgiftslagen (PUL).

DSF kommer att gälla för alla EU:s medlemsländer.

På det stora hela kommer de registrerade att ha samma rättigheter som idag men rättigheterna förstärks med dataskyddsförordningen. DSF visar på rätten av ett aktivt samtycke med att använda information om individen. En övergripande tanke med de nya reglerna är att tydligare betona att det företag, myndighet eller annan organisation som behandlar personuppgifter aktivt måste ta ansvar för att se till att förordningens regler följs och att kunna visa det (ansvarsskyldighet). Det kan ske genom att man tar fram en särskild dataskyddspolicy och att man så långt som möjligt bygger in integritetsvänliga lösningar i sina system.

Behandling av personuppgifter

En personuppgift är en direkt eller indirekt hänvisning till en nu levande person. Att registrera, lagra, organisera, radera, ändra eller översända personuppgifter i någon form räknas som en behandling. Lagen gäller oavsett om behandlingen sker manuellt eller automatiskt. Det spelar heller ingen roll om handlingen är strukturerad (ett register eller databas) eller ostrukturerad (mejl, word, excel, foton).

Vilka är de viktigaste nyheterna för din förening?

Skulle föreningen bli utsatt för dataintrång eller på något sätt tappa kontroll över personuppgifter så måste du informera de personer som uppgifterna gäller och Datainspektionen, om incidenten är allvarlig. Exempel på allvarlig incident kan exempelvis vara att uppgifterna som läckt leder till att personer utsätts för diskriminering, id-stölder, bedrägeri eller finansiella förluster.

Incidenten måste anmälas inom 72 timmar. Någon anmälan behöver dock inte göras om det är osannolikt att incidenten leder till några risker för enskildas rättigheter. Skulle ni misstänka eller upptäcka att en incident har skett eller kan ske, kontakta först förbundets Personuppgiftsansvarige (se kontaktuppgifter nedan).

Befintliga krav som även fanns i PUL och är bra att känna till är att **en person har rätt att begära:**

- Registerutdrag på sina personuppgifter
- Få felaktiga uppgifter rättade
- Få sina personuppgifter raderade
- Neka att personuppgifterna används

Personuppgifter får inte sparas längre än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Det innebär att uppgifter om avslutade "förhållanden" måste gallras fortlöpande.

I normala fall får personuppgifter om en tidigare medlem användas för marknadsföringsändamål under ett års tid efter det att medlemskapet har upphört. Som huvudregel gäller att en e-postadress får användas i marknadsföringssyfte endast om personen samtyckt till det på förhand.

Förbundets personuppgiftsansvarige och integritetspolicy

Vid frågor eller funderingar, kontakta förbundets personuppgiftsansvarige Ulf Brändström, ulf.brandstrom@astmaoallergiforbundet.se, 08-506 28 214

Förbundets nya integritetspolicy <https://astmaoallergiforbundet.se/wp-content/uploads/2018/05/Integritetspolicy-2018-1.pdf>

Läs mer

Mer information finns på <http://www.datainspektionen.se/dataskyddsreformen> och vi rekommenderar att du läser vidare via länken och sätter dig in vad som krävs nu när den nya lagen träder i kraft då detta är en viktig ny lagförändring.



Checklista och förebyggande åtgärder

- Gå igenom på ett styrelsemöte vad den nya lagstiftningen innebär för just din förening.
- Välj en person som ansvarar för arbetet att hantera och skydda personuppgifter.
 - Särskilda krav kommer att gälla för den person i föreningen som har tillgång till det webbaserade medlemsregistret. Särskild information kommer att gå ut till denne.
- Kartlägg var ni hanterar personuppgifter. Detta gäller såväl digitalt som på papper.
- Skriv ned hur ni hanterar personuppgifter.
- Bestäm vad personuppgifterna ska användas till.
- Samla in och hantera endast personuppgifter som ni har rätt till.
- Informera de personer vars uppgifter du samlar in. Föreningen kan också hänvisa till förbundets integritetspolicy och ange att man följer den. Eller använd den policyn som utgångspunkt för att göra en egen.
- Samla inte in fler personuppgifter än vad som behövs (se faktaruta nedan kring vad som klassas som känsliga personuppgifter).
- Se till personuppgifterna är korrekta och uppdaterade.

- Radera personuppgifter som inte längre behövs. Detta kan exempelvis vara om ni haft en aktivitet där ni behövt ta in information kring personers matallergier eller andra anpassningsbehov.
- Se till att uppgifterna inte sprids till obehöriga, till exempel personer och företag utanför organisationen. Det gäller även kommuner, myndigheter och liknande aktörer.
- Se till att personuppgifter inte sprids i onödan till andra medlemmar och andra föreningar inom förbundet utan att det finns ett tydligt syfte.
- Minimera antalet personuppgifter som lagras och hanteras.
- Begränsa vilka som får tillgång till personuppgifterna.
- Skydda uppgifterna. Tänk på att ha en brandvägg och/eller ett virusprogram på din dator.
- Förvara personuppgifter som är på papper i ett låst utrymme.
- När du mejlar många, se till att skicka hemlig kopia till mottagarna så att inte alla ser alla andras e-postadresser.
- Säkerställ att andra utanför föreningen som får tillgång till medlemmarnas personuppgifter har rutiner för att skydda och radera uppgifterna efter slutfört uppdrag.
- Spara inga uppgifter längre än nödvändigt, vare sig på papper eller på dator. Ha som rutin att radera gamla medlemslistor, deltagarlistor och liknande varje år för saker som hänt föregående år.
- Utbilda nya styrelseledamöter eller personer som ska hjälpa till med aktiviteter som därför behöver tillgång till personuppgifter blir informerade om förbundets integritetspolicy.

Vad är en personuppgift?

Personnummer.

Namn.

Kontaktuppgifter (adress, e-post, telefon).

Familjetillhörighet.

Betalningsinformation.

Medlemsnummer.

Aktivitetslistor med kontaktuppgifter.

Vad är känsliga personuppgifter?

Var extra försiktig med att registrera eller hantera så kallade känsliga personuppgifter, till exempel:

Hälsouppgifter, såsom diagnos, symtom eller andra besvär.

Politiska åsikter, religion eller facklig tillhörighet.

Sexualitet.

Ras eller etniskt ursprung.

Om man behöver registrera eller hantera någon känslig personuppgift, såsom allergier, är det bra om personen ifråga muntligt eller skriftligt har samtyckt till att ni hanterar dessa uppgifter.

Obs! Alla personuppgifter som rör barn under 16 år kräver alltid en förälders eller målsmans samtycke.