Föreningar och små organisationer behöver följa några grundläggande principer.

(https://www.datainspektionen.se/vagledningar/for-foreningar-och-sma-organisationer/det-har-behover-ni-gora/)

- **Ändamålsbegränsning:**
  Samla bara in uppgifter för specifika ändamål och behandla inte uppgifterna senare för ett annat ändamål.
  Exempel: Om ni har samlat in uppgifter för att administrera medlemskap ska ni inte senare behandla uppgifterna för att profilera medlemmar för till exempel riktad marknadsföring.

- **Uppgiftsminimering:**
  Samla bara in de uppgifter som är relevanta för ändamålet.
  Exempel: Om ni bara behöver namn och telefonnummer för att administrera medlemskap ska ni inte registrera personnummer för att "det kan vara bra att ha".

- **Korrekthet:**
  Se till att ha korrekta uppgifter och uppdatera dem vid behov.
  Exempel: Se till att ha lämpliga rutiner på plats för att säkerställa att felaktiga personuppgifter rättas.

- **Lagringsminimering:**
  Spara inte uppgifterna under en längre tid än nödvändigt.
  Exempel: Om en medlem avslutar sitt medlemskap ska ni radera medlemmens personuppgifter om uppgifterna inte längre behövs för att administrera eller avsluta medlemskapet.

Information till medlemmar

- Vem som är personuppgiftsansvarig och hur man kontaktar den personuppgiftsansvarige (oftast föreningens styrelse)
- vilka personuppgifter ni behandlar (till exempel namn och adress)
- varför ni behandlar dessa personuppgifter (för vilket ändamål och med vilken rättslig grund)
- vilka mottagare som ska ta del av uppgifterna (till exempel en samarbetspartner)
- om ni tänker överföra personuppgifter till ett så kallat tredjeland (land utanför EU/EES).

Information till medlemmar om deras rättigheter. De har bland annat rätt att

- få tillgång till sina personuppgifter (vilka uppgifter och hur de behandlas)
- få felaktiga personuppgifter rättade
- få sina personuppgifter raderade om uppgifterna inte längre är nödvändiga
- få veta hur länge ni kommer att lagra personuppgifterna
- lämna in klagomål till Datainspektionen.

För att uppfylla informationsplikten behöver ni gå ut med ovanstående information till såväl nya som gamla medlemmar!

Dokumentation av arbetet med personuppgifter

Rutiner för att behandla personuppgifter (kallas register över behandling) ska vara skriftligt, och tillgängligt i elektroniskt format för Datainspektionen och hållas uppdaterat. Registret ska innehålla information om

- namn och kontaktuppgifter till den personuppgiftsansvarige (oftast styrelsen)
- varför ni behandlar personuppgifter (syftet med behandlingen av personuppgifterna)
- vilka kategorier av personer och personuppgifter ni behandlar (till exempel uppgifter om medlemmar i en bostadsrättsförening och deras adress och telefonnummer)
- eventuella externa mottagare av personuppgifterna och om ni för över uppgifter till ett så kallat tredjeland (land utanför EU/EES)
- tidsfrister för radering, det vill säga hur länge uppgifterna sparas (om möjligt)
- vilka säkerhetsåtgärder ni använder när ni behandlar personuppgifterna (om möjligt).

Skydda personuppgifterna

Föreningen är ansvarig för att skydda personuppgifterna som ni behandlar på ett bra sätt. Detta gör ni genom att vidta lämpliga tekniska och organisatoriska säkerhetsåtgärder. Vad som är en lämplig säkerhetsnivå beror på bland annat vilken typ av personuppgifter det handlar om, hur omfattande personuppgiftsbehandlingen är och varför ni behandlar personuppgifterna. Det beror också på vilka risker behandlingen kan innebära för medlemmarnas rättigheter och friheter.

Exempel på säkerhetsåtgärder:

- kryptera känsliga personuppgifter
- begränsa åtkomst till personuppgifterna
- installera skydd mot skadlig kod (antivirus).

Rapportera personuppgiftsincidenter

Om ni råkar ut för en "personuppgiftsincident" måste ni rapportera det till Datainspektionen inom 72 timmar. En personuppgiftsincident är en säkerhetsincident som leder till oavsiktlig eller olaglig förstöring, förlust eller ändring av de personuppgifter som ni behandlar. Den kan innebära risker för medlemmarnas friheter och rättigheter.

Exempel på personuppgiftsincidenter:

- Ni tappar bort ett USB-minne med personuppgifter.
- Någon gör ett dataintrång på er server.
- Någon obehörig tar del av personuppgifterna.

Behov av ett dataskyddsombud

Vissa föreningar behöver utse ett dataskyddsombud. Dataskyddsombudets roll är att kontrollera att ni följer dataskyddsförordningen inom organisationen, genom att till exempel utföra kontroller och informationsinsatser.

Exempel på föreningar som kan behöva utse ett dataskyddsombud:

- religiösa och politiska föreningar
- föreningar som riktar sig mot människor med funktionsnedsättningar
- hbtq-föreningar.

Personuppgiftsbiträde - teckna ett biträdesavtal om ni lämnar ut personuppgifter

Om ni lämnar ut personuppgifter till någon utanför er förening som ska behandla uppgifterna för er räkning, till exempel för att göra ett utskick till era medlemmar, behöver ni upprätta ett avtal med den ni lämnar uppgifterna till – till det så kallade personuppgiftsbiträdet. Avtalet som ska upprättas kallas biträdesavtal och ska bland annat innehålla instruktioner för hur personuppgiftsbiträdet får behandla personuppgifterna.

E-post - Datainspektionens rekommendation

- När ni mottagit och läst e-posten, bedöm om uppgifterna ska bevaras och var det i så fall ska ske (överförs till andra IT-system, pärmar mm) för att uppfylla de krav som gäller för just dessa uppgifter.
- Skicka inte känsliga personuppgifter i oskyddad e-post.
- Informera på er webb i samband med e-postadressen hur ni behandlar personuppgifter eller länka därifrån till er integritetspolicy.
- Om ni skickar svarsmejl eller autosvar, bifoga en standardtext där ni informerar den som skickat e-post om hur ni behandlar personuppgifter eller länka till en integritetspolicy på er webbplats.
- Informera alla i er organisation om reglerna och rutinerna för hur ni behandlar personuppgifter i er organisation. Se också till att rutinerna hålls levande.