# GDPR i båtlivet

ett material från Svenska Båtunionen

v. 1.1

# Vad är GDPR?

General Data Protection Regulation
Allmänna dataskyddsförordningen

I Sverige ersätter den (bl a) Personuppgiftslagen (PUL) som är en nationell lagstiftning som bygger på ett EU-direktiv från 1995.

Dataskyddsförordningen (GDPR) gäller i hela EU och har också till syfte att skapa en enhetlig och likvärdig nivå för skyddet av personuppgifter så att det fria flödet av uppgifter inom Europa inte hindras. Förordningen gäller när organisationer behandlar personuppgifter. Samma regler gäller inom hela EU.

Mycket i dataskyddsförordningen liknar de regler som fanns i personuppgiftslagen. På samma sätt som enligt PUL får man till exempel behandla personuppgifter med stöd av samtycke från de registrerade, för att uppfylla ett avtal eller efter en intresseavvägning. De registrerade kommer även i fortsättningen att ha rätt att få information om den personuppgiftsbehandling som sker – och den som behandlar personuppgifter måste ha tillräckliga säkerhetsåtgärder för att uppgifterna skyddas på rätt sätt. Om det är fråga om uppgifter om hälsa, etniskt ursprung, sexuell läggning, politisk uppfattning eller religiös tro ställs särskilda krav (känsliga personuppgifter).

## GDPR i sju punkter

1. **Rätt till tillgång av din data.**
   Som EU-medborgare har du rätt att veta vilken data en organisation har om dig och hur den används.

2. **Rätten att bli glömd**
   Organisation ska sluta använda och/eller radera din persondata om du ber om det.

3. **Dataportablitet**
   Du har rätt att flytta din data från en organisation till en annan, ungefär som du i dag kan flytta ditt mobiltelefonnummer från en operatör till en annan.

4. **Inbyggt dataskydd**
   Om ett system är designat för att leva upp till GDPR-standard har man vad som brukar kallas inbyggd dataskydd, eller "privacy by design".

5. **Lämpliga säkerhetsåtgärder**
   Organisation ska löpande vidta åtgärder för att skydda persondata.

6. **Rapporteringsplikt**
   Organisation måste rapportera incidenter som rör persondata till tillsynsmyndighet (i Sverige är det Datainspektionen) inom 72 timmar. I vissa fall ska även berörda EU-medborgare informeras. Exempel på incidenter är: dataintrång, dataförlust eller annan felaktig behandling av personuppgifter.

7. **Utökat dataskydd**
   Även organisation utanför EU omfattas av GDPR så länge den hanterar EU-medborgares data.

## Varför ny lagstiftning?

Digitaliseringen i samhället är orsaken till GDPR. Idag kan enorma och detaljerade mängder uppgifter om oss samlas in, bearbetas och utnyttjas. Och så sker redan.

I stor utsträckning har vi nytta av det och dagens ekonomi och samhällsliv bygger i allt större utsträckning på dessa möjligheter. Digital profilering av oss

- gör att vi får användbara träffar när vi googlar
- gör att vi slipper ta del av en hel del för oss irrelevanta uppgifter och reklam
- gör att vårt umgänge med företag, myndigheter, ideella organisationer – och vänner och bekanta – blir smidigt
- och kan till och med bidra till effektivare hälsovård

Men det kan också medföra risker av olika slag

- oönskad reklam eller bearbetning från olika organisationer
- exponering av uppgifter om oss som vi inte vill se spridda, kanske till och med säkerhetsrisker. T ex om andra vet precis var jag är (och inte är) kan jag bli utsatt för hot, våld och andra brott.

Data om individer är alltså värdefulla på olika sätt och GDPR ska ge individen ökad kontroll över data om sig. Det personligt aktiva medgivandet ska normalt krävas för att någon organisation ska få samla och använda uppgifter om dig.

## Skillnad mot PUL?

Skillnaden mot PUL är, i praktiken, inte särskilt stor. Kort sammanfattning:

- I GDPR finns lite mer krav på transparens och “ordning och reda”.
- “Missbruksregeln” är borttagen - den innebar lättnader för att använda personuppgifter i ostrukturerat material (e-post, hemsidor och liknande).
- Straff! - Det blir betydligt mer kännbart om man döms för brott mot GDPR. Höga viten kan bli påföljd.

# Förstå GDPR - begrepp och förklaringar

I det här kapitlet förklaras viktiga termer inom området “behandling av personuppgifter”.

## Behandla personuppgift

Exempel på när båtklubben behandlar registrerades personuppgifter kan vara vid:

- Insamling - t ex när personen söker medlemskap.
- Registrering - t ex när personen antas som medlem.
- Lagring - t ex i en databas, i en kortlåda, i en dokumentsamling.
- Bearbetning - t ex vid urval till exempelvis listningar (lista alla personer som har båtplats vid en viss brygga).
- Spridning - t ex föreningsmatrikel.
- Samkörning - t ex om ni jämför en extern lista med ert eget medlemsregister (för att se vilka som även är (eller inte är) medlemmar i föreningen.
- Radering - t ex när någon lämnar föreningen och inte längre ska vara registrerad.

## Code of conduct

Uppförandekoder inom varje bransch som kommer sätta standarden för tillämpningen av GDPR. Att ta del av utfall av domstolsbeslut kan vara ett sätt att sätta standarden.

## Integritetspolicy

Ett dokument som beskriver hur båtklubben behandlar personuppgifter. Vilka personuppgifter behandlas och för vilka ändamål? I vilken utsträckning får andra tillgång till personuppgifter? T ex finns listor anslagna publikt (bryggplatslista vid landgången, tryckt matrikel…).

## Kvasiidentifierare

Något som kan hänföras till en enskild person utan att det är direkta personuppgifter t.ex. en unik båt, ovanligt yrke kombinerat med bostadsort…

## Känslig personuppgift

- Biometriska och genetiska uppgifter (t.ex. storlek på kläder)
- Etniskt ursprung
- Hälsa
- Medlemskap i fackförening
- Politiska åsikter
- Religiös/filosofisk övertygelse

- Sexuell läggning

## Personuppgift

Varje uppgift som kan identifiera en fysisk nu levande person, direkt eller indirekt. Namn, personnummer, adress, e-postadress och fotografi är exempel på personuppgifter.

## Personuppgiftsansvarig

Det är den organisation som behandlar personuppgifter (som inte sker i rent privat användning). Det är varje enskild klubb som är personuppgiftsansvarig för den behandling av personuppgifter som görs inom just er klubb.

## Personuppgiftsbiträde

Personuppgiftsbiträde är den organisation som behandlar personuppgifter för den personuppgiftsansvariges räkning. Det är exempelvis samarbetspartners, myndigheter eller utomstående personer som tar del av era personuppgifter inom klubben. Ett skriftligt avtal måste upprättas (personuppgiftsbiträdesavtal). Det är den personuppgiftsansvarige som ansvarar för att avtalet finns.

## Personuppgiftsbiträdesavtal

Ett avtal som upprättas mellan den personuppgiftsansvarige och personuppgiftsbiträdet. I avtalet ska det särskilt föreskrivas att personuppgiftsbiträdet får behandla personuppgifterna bara i enlighet med instruktionerna och att personuppgiftsbiträdet måste vidta de säkerhetsåtgärder som man avtalat.

## Personuppgiftsincident

Om det inträffar en säkerhetsincident som rör personuppgifter, till exempel ett dataintrång eller en oavsiktlig förlust av personuppgifter.

## Personuppgiftsregister (personregister)

Ett register som innehåller personuppgifter. Register med kombination av minst två personuppgifter om samma person, som kan identifiera personen ifråga anses som ett personuppgiftsregister. T ex namn och adress.

## Privacy by design

“Sekretess genom utformning” Begrepp för att beskriva hur system utformas för att uppfylla sekretesskrav. T ex utformning för att minimera risken att användare gör fel av misstag.

## Rapporteringsskyldighet

När man upptäcker en personuppgiftsincident måste man dokumentera incidenten och anmäla den till Datainspektionen inom 72 timmar. Man kan också behöva informera de registrerade, till exempel om det finns risk för id-stöld eller bedrägeri.

## Vite

Datainspektionen är tillsynsmyndighet för GDPR. Det är alltså den myndighet som ska se till att GDPR efterföljs. Företag, organisationer och myndigheter som inte uppfyller kraven i GDPR riskerar ett stort vite på upp till 20 miljoner euro alternativt 4 procent av den globala årsomsättningen.

# Principer för behandling av personuppgifter

a) Uppgifterna ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade (laglighet, korrekthet och öppenhet).

b) De ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål. Ytterligare behandling för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1 ska inte anses vara oförenlig med de ursprungliga ändamålen (ändamålsbegränsning).

c) De ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas (uppgiftsminimering).

d) De ska vara korrekta och om nödvändigt uppdaterade. Alla rimliga åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga i förhållande till de ändamål för vilka de behandlas raderas eller rättas utan dröjsmål (korrekthet).

e) De får inte förvaras i en form som möjliggör identifiering av den registrerade under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Personuppgifter får lagras under längre perioder i den mån som personuppgifterna enbart behandlas för arkivändamål av allmänt intresse, vetenskapliga eller historiska forskningsändamål eller statistiska ändamål i enlighet med artikel 89.1, under förutsättning att de lämpliga tekniska och organisatoriska åtgärder som krävs enligt denna förordning genomförs för att säkerställa den registrerades rättigheter och friheter (lagringsminimering).

f) De ska behandlas på ett sätt som säkerställer lämplig säkerhet för personuppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder (integritet och konfidentialitet).

## Laglig grund för behandling av personuppgifter

### Samtycke

En person ska frivilligt kunna samtycka till hur personuppgifterna behandlas efter att den registrerade har fått information om personuppgiftsbehandlingen. Samtycket ska, otvetydigt, genom en aktiv handling, lämnas av personen för att organisationen ska få använda uppgifterna för specifika ändamål. Den som behandlar personuppgifter med stöd av ett samtycke måste kunna visa att ett giltigt samtycke har lämnats av den registrerade. **Ett samtycke ska närsomhelst kunna återkallas av den registrerade lika lätt som det lämnades.**

### Avtal

T ex den överenskommelse som båtklubb och personen ingår när personen blir medlem i båtklubben. Den behandling av personuppgifter som är nödvändig för att fullgöra avtalet ska tydligt definieras i medlemsvillkoren och finnas lättillgängligt för personen att ta del av. I avtalet ingår behandling av personuppgifter som är nödvändiga för att avtalet ska kunna efterföljas. **Personuppgiftsbehandling i enlighet med avtalet kan inte personen avsäga sig utan att samtidigt bryta avtalet (dvs gå ur båtklubben)**.

### Rättslig förpliktelse

Personuppgifter får behandlas om det är nödvändigt för att uppfylla en rättslig förpliktelse. Som exempel på en rättslig förpliktelse kan nämnas bokföringsskyldigheten som anges i bokföringslagen.

### Berättigat intresse/intresseavvägning

Är behandling av personuppgifter där organisationens intresse väger tyngre än den registrerades intresse av skydd för sina personuppgifter. Barn anses vara särskilt skyddsvärda. T.ex. när organisationen lämnar ut uppgifter till samarbetspartners i syfte att informera medlemmen om dess förmåner eller erbjudanden.

Om den registrerade personen invänder mot en pågående behandling måste organisationen göra en ny intresseavvägning och upphöra med behandlingen om det inte finns tillräckliga belägg för att fortsätta behandlingen. Om personen invänder mot behandling som sker för direktmarknadsföring måste behandlingen upphöra.

# Registrerade personers rättigheter

## Rätt till information

Registrerad person har rätt att få information när dennes personuppgifter behandlas. Bland annat ska information lämnas om kontaktuppgifter till den personuppgiftsansvarige, den rättsliga grunden för behandlingen och ändamålet med behandlingen.

Information ska lämnas av den personuppgiftsansvarige både när uppgifterna samlas in och när den registrerade annars begär det. Därutöver finns det vissa tillfällen när särskild information ska ges till den registrerade, till exempel om det inträffar ett dataintrång eller liknande (en personuppgiftsincident) och det finns risk för till exempel identitetsstöld eller bedrägeri.

## Rätten att bli glömd

En registrerad person har rätt att få sina uppgifter borttagna. Om det finns annan lagstiftning som kräver att uppgifterna sparas kan de dock inte raderas. Det kan även förekomma en intresseavvägning då organisationen ändå kan spara uppgifter utan personens samtycke. Det kan också hända att organisationens intresse för att spara uppgifterna väger tyngre än den registrerades önskan att få desamma raderade. Till exempel om någon som är utesluten vill bli raderad/glömd. Då kan organisationens intresse av att ha kvar uppgifterna väga tyngre, d.v.s. organisationen måste ha kvar informationen om att personen är utesluten, för att denne inte ska kunna bli medlem igen. Detta kan även appliceras på protokoll från möten och sammanträden vilka är en förutsättning för demokratiska organisationer. Då skulle man kunna göra bedömningen att organisationen har berättigat intresse. På samma sätt som man kan anse att registrerade, och även publicerade, tävlingsresultat är en förutsättning för tävlingar.

Det är viktigt att organisationen endast lagrar/publicerar relevanta personuppgifter för ändamålet samt att till exempel protokoll skrivs sakligt och utan onödiga personuppgifter eller utlämnande information.

## Rätt till korrigering

Organisation måste korrigera felaktiga uppgifter på begäran av den registrerade.

## Rätt till dataportabilitet

Den registrerade personen har rätt att få sina uppgifter flyttade. Uppgifterna ska då göras tillgängliga i en fil i digitalt format som kan läsas av vanliga system, t.ex. xml.

## Rätt att få ut sina uppgifter som behandlats

Registrerad person har rätt att kostnadsfritt en gång om året få ett utdrag på all behandling av dennes personuppgifter. Detta gäller såväl digitala som analoga register. Informationen ska tillhandahållas i en lättillgänglig, skriftlig form och med ett tydligt och enkelt språk.

## Rätt att begränsa direktmarknadsföring

Registrerad person har rätt att begränsa vilka personuppgifter som behandlas av företag med syfte till riktad, personifierad marknadsföring.

# Vad bör klubben göra?

## Projekt GDPR

Det är bra att formalisera arbetet i ett tydligt projekt. Det är då lätt att besluta, genomföra och följa upp. Här följer en “checklista” med förslag till tillvägagångssätt.

### 1. Skapa en GDPR-organisation

Alla i båtklubbens styrelse måste vara med på och förstå att GDPR-arbetet är viktigt. Det är i första hand ett verksamhetsprojekt och inte ett IT-projekt. En person bör utses som ansvarig och leda arbetet.

### 2. Informera er

Ni bör ta reda på vad GDPR innebär och vilket arbete det kan innebära för er som båtklubb. Ni hittar information om GDPR på datainspektionens hemsida, www.datainspektionen.se.

### 3. Börja med att göra en nulägesanalys

Det här är en viktig del av arbetet, och troligen det mest tidskrävande. För att kunna gå vidare med att ta reda på vad ni bör göra för att uppfylla GDPR så måste ni göra en inventering och kartlägga hur ni hanterar personuppgifter idag. Exempelvis bör följande frågor besvaras:

Vilka arbetsuppgifter har vi där vi behandlar personuppgifter?

Hur behandlas våra medlemmar gällande personuppgifter?

Vilka system har vi där personuppgifter behandlas?

Har vi några leverantörer som behandlar personuppgifter för vår räkning? Exempelvis Svenska Båtunionen, tryckeriet som trycker medlemsmatrikeln...

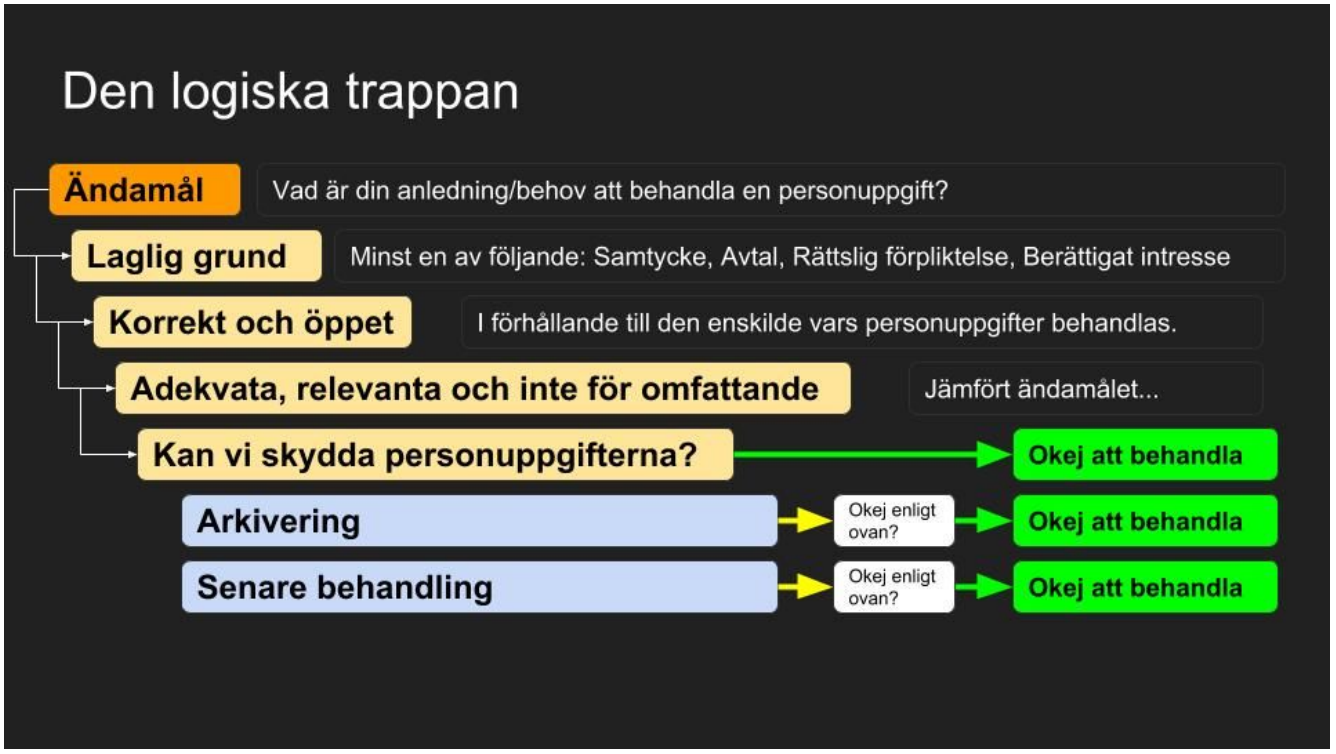
Hur informerar vi våra medlemmar idag om personuppgiftsbehandlingar och om deras rättigheter?

Inventeringen förenklas om ni delar upp klubbens verksamheter i lämpliga delar, för att ni ska kunna inventera de olika personuppgiftsbehandlingar som görs inom varje del. Ett exempel på en sådan uppdelning kan vara: ekonomi, medlemsservice, arrangemang, hamn och varv.

### 4. Gör en GAP- och riskanalys

GAP-analys är skillnaden (gapet) mellan nuläget och det läge ni måste nå för att följa GDPR. Ni får då fram vad ni behöver göra för att kunna efterleva lagen. Det kan handla om dokumentation, nya rutiner och att ta fram tekniska lösningar där det behövs. Dessutom kommer ni antagligen att behöva gallra och radera information.

En riskanalys är ett sätt att titta på personuppgiftsbehandlingarna och försöka avgöra dels vilket ingrepp i den personliga integriteten behandlingen gör, men även risken för en personuppgiftsincident (t ex om personuppgifter kommit orätta händer). Det är alltså en process för att identifiera och minimera riskerna med personuppgiftshanteringen.




### 5. Prioritera det fortsatta arbetet

Efter att GAP- och riskanalysen är gjord så är det dags att prioritera arbetet.

Viktiga saker att ta hänsyn till är riskerna med era behandlingar, de med hög risk eller med känsliga personuppgifter bör ni ta tag i först. Uppgifter med stort gap (nuläge - önskat läge) bör man också ta i ett tidigt skede då dessa kan ta tid.

### 6. Dokumentera alla behandlingar

För att bland annat kunna visa att ni uppfyller kraven enligt GDPR bör ni dokumentera alla personuppgiftsbehandlingar. I dokumentationen ska ändamålet med behandlingen, lagringstiden för uppgifterna samt den lagliga grund ni använder för att behandla uppgifterna ingå.

#mall att använda för inventering av personuppgiftsbehandlingar och personregister

### 7. Ta fram dokument/processer/rutiner som krävs

Enligt GDPR har den personuppgiftsansvarige (båtklubben) en skyldighet att informera registrerade om hur ni hanterar personuppgifter. Detta ska framgå av integritetspolicyn (även kallad personuppgiftspolicy eller privacy policy). Där talar ni om vilka personuppgifter ni samlar in, för vilket syfte, lagringstid mm. Ni ska också informera om den registrerades rättigheter (t ex rätten till registerutdrag och rätten att få felaktiga uppgifter korrigerade). GDPR ställer krav på att informationen som lämnas ska vara kortfattad, lättbegriplig och utformad med ett tydligt och enkelt språk. Informationen ska också vara lättillgänglig. Många har integritetspolicyn publicerad på en egen sida på sin hemsida. Självklart kan man lämna informationen på andra sätt än på hemsidan. Huvudsaken är att den är enkelt formulerad, omfattar alla formella krav och är enkel att ta till sig (läs mer om detta under punkten 9).

#exempel på integritetspolicy

Om båtklubben har egen IT-utrustning, t ex en kanslilokal med utrustad arbetsplats, och kanske också anställd personal så bör man även ta fram en IT-säkerhetspolicy. Den ska beskriva vilka IT- och

informationsåtgärder som klubben tillämpar för att skydda personuppgifter. Det kan t ex vara att det krävs inloggning för att komma åt system, att inloggning ska vara krypterad, att man inte ska lämna datorn olåst och gå på lunch mm.

Utöver dessa dokument ska ni ta fram tydliga processer och rutiner vid personuppgiftshantering. Om ni behandlar personuppgifter med stöd av samtycke bör det t ex finnas en rutin vid hantering av samtycke för att ni ska kunna visa att ett samtycke har lämnats. Det bör också finnas rutiner för hur man inom klubben ska agera om en personuppgiftsincident sker. Har personuppgifter kommit i orätta händer ska detta rapporteras till Datainspektionen inom 72 timmar och i vissa fall (om man misstänker att läckan kan skada personerna, t ex ID-kapning) även till de registrerade personerna.

### 8. Se över befintliga avtal (inklusive stadgar, direktiv och andra ordningar)

Behöver era avtal skrivas om eller behöver det bifogas en bilaga utifrån de krav som GDPR ställer? Se i så fall till att genomföra dessa förändringar. Detta gäller både interna och externa avtal, såsom avtal med medlemmar och leverantörer.

### 9. Hur informerar ni era medlemmar?

Integritetspolicyn ska vara enkelt tillgänglig för medlemmarna och eventuellt andra registrerade. Ni bör se över och ta fram en plan på hur ni ska informera och genomföra de förändringar som krävs.

Information lämnas lämpligen till nya medlemmar i samband med ansökan om medlemskap. Befintliga medlemmar kan t ex informeras i samband med att man aviserar att medlemsavgiften skall betalas, i kallelse till årsmöte eller liknande.

Det är vanligt att båtklubb publicerar sin integritetspolicy på sin hemsida. Då kan man hänvisa dit i t ex avtal, e-post (via en länk) eller telefonsvarare när personuppgifterna samlas in via telefon.

### 10. Skriv personuppgiftsbiträdesavtal

Personuppgiftsbiträde är den som behandlar personuppgifter för den personuppgiftsansvariges räkning, dvs i många fall en leverantör av IT-tjänster. Det kan också t ex vara en byrå som sköter medlemsregister, fakturering och bokföring.

Den personuppgiftsansvarige kan inte delegera sitt ansvar och är alltid ytterst ansvarig för att behandlingen sker i enlighet med kraven i GDPR. Ett personuppgiftsbiträde kan bli skadeståndsansvarigt om denne har brutit mot de bestämmelser som specifikt riktar sig till biträden eller har behandlat uppgifter i strid med den personuppgiftsansvariges instruktioner. Personuppgiftsbiträdet kan även, precis vad som gäller för personuppgiftsansvariga, drabbas av sanktionsavgifter om denne inte uppfyller de skyldigheter som finns i GDPR.

När den personuppgiftsansvarige anlitar ett personuppgiftsbiträde ska det finnas ett skriftligt avtal, ett så kallat personuppgiftsbiträdesavtal. Det är den personuppgiftsansvarige som ansvarar för att avtalet finns.

### 11. Behöver systemen åtgärdas eller bytas ut?

Grundläggande principer enligt GDPR är att inte samla in mer information än vad som behövs, inte ha kvar informationen längre än nödvändigt och inte använda uppgifterna till något annat än vad som var syftet när de samlades in.

Behandlingen av personuppgifter måste ske med rimlig säkerhet. Personuppgifterna ska skyddas från dataintrång och läckor när de t ex skickas eller lagras. Vilka åtgärder som behövs beror bland annat

på uppgifternas art, omfattning och syfte med behandlingen liksom vilka risker för enskildas rättigheter och friheter som behandlingen kan innebära.

Den registrerade har även vissa rättigheter enligt GDPR. Den registrerade ska kunna få ta del av sina uppgifter, korrigera felaktiga uppgifter och kunna få sina personuppgifter borttagna i vissa fall. Denne har även rätt att få sina personuppgifter flyttade (dataportabilitet).

För att tillgodose alla krav enligt GDPR behöver ni se över era system och undersöka om de behöver uppdateras, åtgärdas eller bytas ut. Om det är på det sättet så måste ni planera för att kunna genomföra detta när det kommer till resurser och utbildning.

### 12. Ta fram rutiner för att säkra individens rättigheter

För att kunna tillgodose de registrerades rättigheter att t ex få sina personuppgifter raderade, rättade eller flyttade (dataportabilitet) bör ni se till att skapa rutiner. Dessa rutiner måste också vara kända av samtliga som jobbar med medlemsadministration i klubben, och det är bra om dessa rutiner finns enkelt tillgängliga för samtliga att följa.

### 13. Utbilda berörda i GDPR samt rutiner

Rekommendationen är att utbilda samtliga som jobbar med medlemsadministration i klubben och styrelsen (då de är ansvariga för klubbens verksamhet, även behandling av personuppgifter) i grunderna i GDPR. Dessa personer måste även få utbildning gällande de policys, processer och rutiner som tagits fram eller justerats under GDPR-arbetet.

Resurser

DI föreningsinformation - “Det här behöver ni göra”

DI föreningsinformation - “Det här behöver ni veta”

DI föreningsinformation - “Frågor och svar”