GDPR – klubbens behandling av personopplysninger

1. Innledning
Personvernregelverket kan fremstå omfattende og vanskelig å håndtere. Nedenfor følger en kort innføring i hovedpunktene i regelverket og en oversikt over hva en klubb som minimum må/bør gjøre for å ivareta de viktigste kravene etter regelverket.

2. Kort om personvern og behandling av personopplysninger
Opplysninger og vurderinger som kan knyttes til en enkeltperson (personopplysninger) skal behandles i tråd med personopplysningsloven og GDPR-forordningen. Personopplysninger vil typisk være navn, adresse, e-postadresse, SoMe-adresser, aliaser/kallenavn, telefonnummer, foto og fødsels-/personnummer, men også vurderinger, kategoriseringer og karakteristikker av en person omfattes. Som sensitive personopplysninger regnes blant annet opplysninger om helse, seksuell orientering, etnisk opprinnelse, religiøs overbevisning samt genetiske og biometriske opplysninger. Det å «behandle» personopplysninger omfatter mye, herunder f.eks. å samle inn, registrere, vurdere, sammenstille, lagre, utlevere og slette personopplysninger.

Personopplysninger skal behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte, og samles inn for spesifikke, uttrykkelig angitte og berettigede formål. Den som bestemmer formålet med behandlingen av personopplysningene og hvilke midler som skal benyttes (klubben) er «behandlingsansvarlig», dvs ansvarlig for at kravene etter loven og forordningen er oppfylt. Klubben må derfor vurdere om det foreligger et behandlingsgrunnlag for alle personopplysninger som skal behandles. En klubb vil ikke bare behandle personopplysninger til egne medlemmer og ansatte, men også til andre klubbers medlemmer (f.eks. ifm avholdelse av konkurranser og arrangementer). De to vanligste behandlingsgrunnlagene innen idretten er a) at det er nødvendig for å oppfylle en avtale (typisk «medlemsavtalen» mellom klubben og hvert enkelt medlem) eller b) samtykke fra medlemmet/ansatte selv.

3. Klubbens håndtering av personopplysninger
Klubbene bør/må iverksette følgende:

1. Skaff dere en oversikt over hvilke personopplysninger klubben behandler, hvorfor klubben behandler dem og hvor de befinner seg (både hvor de er lagret elektronisk og (eventuelt) befinner seg i papirform. Lag en liste på dette.

2. Skaff dere en oversikt over hvordan personopplysningene innhentes/mottas og hva de brukes til. (Eksempler: Medlemsregistrering, betaling av kontingent/treningsavgift, trenings-/konkurransepåmelding, utbetaling av lønn, godtgjørelser/refusjoner, dommerhonorarer mv.) Lag en liste på dette og beskriv rutinene.

3. Avklar hva som er behandlingsgrunnlaget for personopplysningene (typisk at det er nødvendig for å oppfylle medlemsavtalen eller ved samtykke fra medlemmet selv). Lag en liste på dette og beskriv rutinene.

4. Sørg for at:

- Personopplysningene klubben behandler er sikret mot at utenforstående får tilgang (datasikkerhet), og bruk et anerkjent IT-/datasystem som ivaretar kravene til personvern (med såkalt «innebygd personvern»).
- Klubben ikke behandler personopplysningene til andre formål eller behandler personsensitive opplysninger uten særskilt grunnlag.
- Klubben sletter/minimerer personopplysninger det ikke lenger er saklig (lovlig) behov for å behandle, f.eks. når et medlem melder seg ut av klubben.
- Klubben inngår databehandleravtale med tjenesteleverandører og andre som behandler personopplysninger på klubbens vegne.

5. Lag en oversikt (protokoll) som angir hvordan klubben behandler personopplysninger. (Se mal på: https://www.idrettsforbundet.no/om-nif/personvern-i-idretten/maler/)

6. Lag en personvernerklæring som legges ut på klubbens hjemmeside der det lettfattelig og tydelig fremgår hvorfor, hvordan og hva personopplysningene klubben innhenter skal brukes til. Du finner for øvrig mye nyttig informasjon på Datatilsynets hjemmeside www.datatilsynet.no og på NIFs hjemmeside https://www.idrettsforbundet.no/om-nif/personvern-i-idretten/

****