Databehandlingspolitik for

Svømmeklubben Gigt og Bevægelse

Den 25. maj 2018 træder EU's persondataforordning GDPR og en ny dansk databeskyttelseslov i kraft.

I den anledning er alle foreninger forpligtet til at udarbejde en persondatapolitik og en databehandlingspolitik.

De skærpede krav indebærer særligt, at det skal være synligt for foreningens medlemmer, trænere, instruktører og frivillige, hvordan personoplysninger behandles. Det kan opfyldes ved en privatlivspolitik.

Et krav er også, at foreningen skal have beskrevet for sig selv, hvordan personoplysninger behandles, så det kan være dokumentation over for Datatilsynet (Databehandlingspolitik).

Nedenstående dokument er Svømmeklubben Gigt og Bevægelses databehandlingspolitik:

Politikken er vedtaget på et bestyrelsesmøde den 24.05.2018

---

1. Hvem har ansvaret for databeskyttelse i foreningen?	Kontaktoplysninger på navngivne personer.	Følgende bestyrelsesmedlemmer: Formand: Mail: formand@svklubgob.dk Kasserer: Mail: kasserer@svklubgob.dk
2. Hvad er formålene med behandlingen?	Der skal være en beskrivelse af behandlingsformålene. Formålet med behandlingerne i foreningen oplistes i overordnende kategorier.	a) Varetagelse af medlemsforhold og trænere og lederes forhold, herunder aktivitetsudøvelse, kommunikation, medlemsmøder, generalforsamlinger og kontingentopkrævning b) Administration af foreningens eksterne relationer, herunder indberetning til kommunen efter folkeoplysningsloven samt indberetning af medlemstal m.v. til idrætsorganisationer c) Udbetaling af løn, godtgørelser og føre foreningens bogholderi. d) Behandling knyttet til bekæmpelse af doping
3. Hvilke personoplysninger behandler vi?	Her oplistes de i foreningen behandlede personoplysninger.	Almindelige personoplysninger: a) Navn b) Mailadresse c) Telefon d) Adresse e) Fødselsår f) Mail Oplysninger, der er tillagt en højere grad af beskyttelse indsamles ikke: f.eks. CPR-nummer
4. Hvem behandler vi oplysninger om?	De forskellige typer af registrerede personer, hvorom der behandles personoplysninger.	Der behandles oplysninger om følgende kategorier af registrerede personer: a) Medlemmer b) Ledere og trænere

5. Hvem videregives oplysningerne til?	Oplistning af eventuelle modtagere af foreningens oplysninger, samt hvilke oplysninger der videregives og i hvilke tilfælde. Hvis oplysninger ikke videregives, angives dette.	a) Almindelige personoplysninger om medlemmer, ledere og trænere kan videregives til DGI når vi i foreningen har en berettiget interesse heri. b) Ved evt. indhentelse af børneattester videregives CPR-nummer til politiet. Herudover videregives personoplysninger i form af CPR-nummer, oplysninger om strafbare forhold til DGI, hvis en børneattest har anmærkninger
6. Hvornår sletter vi personoplysninger i foreningen?	Der bør være en angivelse af hvilke oplysninger, der skal slettes og hvornår.	a) Vi opbevarer almindelige personoplysninger på medlemmer i op til 3 år efter tilhørsforholdets ophør. Almindelige personoplysninger om ulønnede ledere og trænere opbevares i op til 1 – 5 år efter virket er ophørt. b) Oplysninger, der er tillagt en højere grad af beskyttelse, sletter vi i udgangspunktet straks efter, at behandlings-formålet er opfyldt. c) CPR-nummer indeholdt i bogføringsmateriale gemmes i 5 år fra regnskabsårets udløb som andet bogføringsmateriale. d) Børneattestoplysninger opbevares, så længe personen fungerer i sit virke.
7. Hvordan opbevarer vi personoplysninger i foreningen?	Her skal så vidt muligt laves en generel beskrivelse af de tekniske og organisa-toiske sikkerheds-foranstaltninger, herunder en beskrivelse af måden oplysningerne registreres.	Vi opbevarer alle personoplysninger i foreningen på vore foreningscomputere, som er beskyttet af password, og som kun formand og kasserer kender til. Computerne er stillet til rådighed for deres virke i foreningen og opbevares i hjemmet..

8. Hvad skal vi gøre, hvis der sker et brud på persondatasikkerheden?	Hvordan opdager, rapporterer og undersøger vi brud på persondatasikkerheden? F.eks. ved hackerangreb. Hvordan vurderer vi, hvor alvorligt bruddet er?	Hvis alle eller nogle af de registrerede oplysninger bliver stjålet, hacket eller på anden måde kompromitteret, kontakter vi vores hovedorganisation og drøfter eventuel anmeldelse til politiet og til Datatilsynet. Vi dokumenterer alle brud på følgende måde: Vi logger alle uregelmæssigheder.
9. Hvad kan vores IT-system	Her beskrives hvilke software vi benytter og til hvad.	Vi benytter standard-software og er underlagt databehandleraftaler med Google, Microsoft og One.com. Vi benytter Gmail, Google-Drev og cloud-løsninger til backup. Desuden Microsoft officepakken, word og excel, mail og samt onedrive. Vi har ikke et regnskabssystem, idet vores regnskab føres i excel udelukkende på baggrund af kontoudtog fra banken. Hjemmesiden hostes hos One.com
10. Har vi tænkt databeskyttelse ind i vores IT-systemer	Ved erhvervelse af et nyt IT-system eller ved ændringer på det nuværende, tænker vi databeskyttelse med ind. Vi er opmærksomme på, at systemet gerne må bidrage til: a) At vi ikke indsamler flere oplysninger end nødvendigt. b) At vi ikke opbevarer oplysningerne længere end nødvendigt. c) At vi ikke anvender oplysningerne til andre formål, end de formål, som oplysningerne oprindeligt blev indsamlet til.	Vores IT-system kan følgende: a) Systemet har ikke en automatisk slettefunktion, så vi gennemgår oplysningerne manuelt] b) Give notifikationer om databehandlingsopgaver, der skal udføres, herunder om kontrol og ajourføring af data c) Give notifikation om regelmæssig fornyelse af password