

Fortegnelse over behandling af personoplysninger i FDF Buddinge.

Fortegnelsen er til opfyldelse af den dokumentationspligt, der påhviler en forening i medfør af persondataforordningen. Foreninger er omfattet af pligten i fuldt omfang, hvorfor der skal føres fortegnelse over almindelige personoplysninger såvel som personoplysninger tillagt en højere grad af beskyttelse (følsomme oplysninger, oplysninger om strafbare forhold og CPR-nummer).

Den sidste kolonne skal udfyldes og ajourføres løbende af foreningen.

Fortegnelse over behandlingsaktiviteter i: FDF Buddinge.

Data for seneste ajourføring af dokumentet: 23/05/2018

1. Hvem har ansvaret for databeskyttelse i foreningen?	Kontaktoplysninger på navngivne personer.	Følgende bestyrelsesmedlemmer: - Randi Mørck, randi.boyemorck@gmail.com. - Daniel Handler, dthandler@gmail.com.
2. Hvad er formålene med behandlingen?	Der skal være en beskrivelse af behandlingsformålene. Formålet med behandlingerne i foreningen oplyses i overordnede 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 til landsforbundet FDF. c) Indhentelse af børneattester d) Hensyntagen til skader og helbredsforhold e) Udbetaling af udlæg og lign
3. Hvilke personoplysninger behandler vi?	Her oplyses de i foreningen behandlede personoplysninger.	Almindelige personoplysninger: a) Navn b) Mailadresse c) Telefon d) Adresse e) Email-adresse f) Køn g) Indmeldelsesdato h) Deltagelse i aktiviteter Oplysninger, der er tillagt en højere grad af beskyttelse: a) CPR-nummer b) Helbredsoplysninger c) Oplysninger om strafbare forhold
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 c) Bestyrelsesmedlemmer

<p>5. Hvem videregives oplysningerne til?</p>	<p>Oplisting af eventuelle modtagere af foreningens oplysninger, samt hvilke oplysninger der videregives og i hvilke tilfælde.</p> <p>Hvis oplysninger ikke videregives, angives dette.</p>	<p>a) Almindelige personoplysninger om medlemmer, ledere og bestyrelsesmedlemmer videregives til landsforbundet FDF</p> <p>b) Almindelige personoplysninger om medlemmer, ledere og bestyrelsesmedlemmer videregives til Gladsaxe Kommune i forbindelse med udbetaling af tilskud.</p> <p>c) Ved indhentelse af børneattester videregives CPR-nummer til politiet. Herudover videregives personoplysninger i form af CPR-nummer, oplysninger om strafbare forhold til FDF, hvis en børneattest har anmærkninger</p>
<p>6. Hvornår sletter vi personoplysninger i foreningen?</p>	<p>Der være en angivelse af hvilke oplysninger, der skal slettes og hvornår.</p>	<p>a) Vi opbevarer almindelige personoplysninger på medlemmer og ledere i op til 5 år efter tilhørsforholdets ophør. Almindelige personoplysninger om bestyrelsesmedlemmer opbevares i op til 1 år efter virket er ophørt.</p> <p>b) Oplysninger, der er tillagt en højere grad af beskyttelse, sletter vi i udgangspunktet straks efter, at behandlingsformålet er opfyldt.</p> <p>c) Aktivitetsdeltagelse opbevares i indeværende sæson, hvorefter det slettes.</p> <p>d) Børneattestoplysninger opbevares, så længe personen fungerer i sit virke</p>
<p>7. Hvordan opbevarer vi personoplysninger i foreningen?</p>	<p>Her laves en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, herunder en beskrivelse af måden oplysningerne registreres.</p>	<p>Medlemsoplysninger opbevares krypteret i FDFs medlemskartotek Carla.</p> <p>Derudover har hver klasseleder en fortegnelse over børnene i klassen i indeværende sæson. Disse udleveres på papir og opbevares forsvarligt i indeværende sæson, hvorefter de makuleres eller på lignende måde destrueres.</p> <p>Oplysninger om medlemmers aktivitetsdeltagelse behandles på mail og SMS og slettes når dataen ikke</p>

		længere er relevant, senest ved afslutning af indeværende sæson.
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: Adgangskontrol til Carla og mailbokse.
9. Hvad kan vores IT-system, og 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) Krypterer al data b) Håndtere total sletning af data. c) Manuel igangsætning af sletning er dog nødvendigt. Klasselederne opretholder et højt sikkerhedsniveau i deres mailbokse f.eks. med stærke, unikke passwords, to-faktor autentificering mm.