Udkast 04. maj 2018

Vejledning om foreninger/klubbers behandling af Medlemsdata

I det følgende er en kort vejledning om, på hvilken måde man som forening/klub under en fagforening (klub) må behandle data om sine medlemmer i henhold til databeskyttelsesforordningen.

Databeskyttelsesforordningen træder i kraft i Danmark d. 25. maj 2018 og vil blive suppleret af databeskyttelsesloven, der endnu kun ligger som lovforslag. I forhold til de bestemmelser, der er relevant for denne vejledning, vil lovforslaget ikke ændre i reguleringen efter forordningen. I denne vejledning skal enhver reference til "GDPR" forstås som en reference til såvel forordningen som loven.

De fleste forhold om personoplysninger anført i denne vejledning har gjaldt siden juli 2000, da persondataloven trådte i kraft. GDPR skærper og udvider dog ansvaret. Det er derfor vigtigt, at klubberne får strammet op på den måde, som man behandler sine medlemsdata og eventuelt andre personoplysninger på. Persondataloven vil blive erstattet af GDPR.

Særligt relevante begreber

Persondataloven og GDPR har sin egen begrebsverden. I forhold til denne vejledning er følgende begreber af særlig betydning:

Personoplysninger: enhver form for information om en identificeret eller identificerbar fysisk person, nærmest uanset hvorledes personen kan identificeres.

Følsomme personoplysninger: en særlig kategori af personoplysninger, der blandt andet omfatter race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold, helbredsoplysninger mv.

Behandling: stort set enhver aktivitet relateret til personoplysninger, f.eks. indsamling, registrering, organisering, systematisering, ændring, opbevaring, videregivelse mv.

Dataansvarlig: den fysiske eller juridiske person m.m., der alene eller sammen med andre afgør til hvilket formål og med hvilke hjælpemidler personoplysningerne skal behandles.

Databehandler: den fysiske eller juridiske person m.m., som behandler personoplysninger på vegne af en dataansvarlig.

Klubben

Personoplysninger

Klubbernes medlemsdata er per definition personoplysninger, da de angår en identificeret person. Medlemsdataene formodes at bestå af følgende: navn, adresse, mail-adresse/telefonnummer og fødselsdag/alder, og personens tilhørsforhold til den fagforening, som klubben hører ind under. Den sidstnævnte oplysning om personens medlemskab af en fagforening er en følsom personoplysning. Selvom de resterende oplysninger er ikke-følsomme gør det forhold, at oplysningen om medlemskabet afslører et fagforeningsmæssigt tilhørsforhold, at alle oplysninger vil skulle behandles som følsomme oplysninger.

Dataansvarlig eller databehandler?

Som en selvstændighed enhed, der selv bestemmer hvordan personoplysninger behandles og bruges (i modsætning til hvis klubben efter aftale med fagforbundet kun behandlede oplysningerne efter fagforbundets instruks), er klubben dataansvarlig, og har de pligter under persondataloven/GDPR, som gælder for dataansvarlige.

Behandlinger

Alle de aktiviteter, som en klub udfører i forhold til sine medlemsdata, er behandlinger, og derfor omfattet af persondataloven/GDPR.

Grundlæggende principper for behandling af personoplysninger

Lovlighed, rimelighed og gennemsigtighed

Behandlingen skal være lovlig, rimelig og gennemsigtig i forhold til den registrerede. Dette er den helt grundlæggende og overordnede regel.

Klubben

Klubbens skal sikre, at klubben har lov til at behandle personoplysningerne i henhold til GDPR, at behandlingen står i rimeligt mål med formålet med behandlingen, og der for den registrerede er gennemsigtighed i hvilke oplysninger, der behandles om vedkommende.

Formålsbestemt behandling

Personoplysningerne skal indsamles til udtrykkeligt angivne og legitime mål og må ikke efterfølgende behandles til formål, der er uforenelig med de oprindelige.

Klubben

Klubbens formål med indsamling af oplysninger om medlemmerne skal for at være legitime være berettiget af Klubbens virksomhed. Typisk vil indsamling af navn, adresse, email/telefonnr. være saglig, og da klubben desuden er en seniorklub med aldersbegrænsning vil også

registrering af fødselsdato/alder være saglig. Tilsvarende vil registreringen af medlemmets fagforening være saglig, da det er grundlaget for medlemsskabet.

Såfremt andre oplysninger ønskes registreret skal klubben gøre sig sit formål dermed klart, og vurdere om det er sagligt.

Den efterfølgende behandling af de indsamlede personoplysninger må ikke være uforenelig med det formål, som oplysningerne blev indsamlet til (kriterierne relevant for vurderingen er opregnet i lovens § 5, stk. 2).

En klub der kun indsamler medlemsdata (som nævnt ovenfor) for at kunne sikre at personen kan være medlem, sende information ud til medlemmer om arrangementer og evt. foretage indberetning til kommune o.lign. for at modtage støtte, vil kravet om formålsbestemthed være umiddelbart opfyldt, da formålet med behandlingen, herunder indsamlingen og den efterfølgende behandling, er det samme.

Eksempel: Det kunne være interessant at registrere til hvilke og hvor meget et medlem deltager i klubbens arrangementer. I lyset af klubbernes eget formål vil den registrering savne et sagligt formål, og derfor være i strid med formålsprincippet.

Dataminimering

Personoplysningerne registreret af den dataansvarlige skal være tilstrækkelige, relevante og begrænset til det nødvendige i forhold til behandlingens formål.

Klubben

Klubben skal registrere de tilstrækkelige og relevante oplysningerne til dets formål, men må ikke gå ud over det nødvendige i forhold til det formål, de behandles til.

Eksempel: Klubbens registrering af et medlems tidligere adresser, om vedkommende er gift/skilt/registreret partner, antallet af børn o.lign. er ikke relevante for formålet med registreringen, og derfor ikke tilladt.

Rigtighed

Personoplysningerne skal være korrekte og ajourførte, og der skal tages de rimelige skridt til at sikre, at personoplysninger, der er urigtige i forhold til de formål til hvilket de behandles, slettes eller berigtiges.

Klubben

Klubben har en pligt til at sikre sig, at medlemsdataene er korrekte og ajourførte til enhver tid.

Eksempel: Klubben skal sørge for opdatering af medlemsoplysningerne, og dvs. navn, adresse, telefon/mobilnr., email-adresse og alder (hvis ikke det er fødselsår, der er registreret), efterhånden som de måtte ændre sig og klubben får besked herom.

Opbevaringsbegrænsning

Personoplysninger skal opbevares på en måde så det ikke er muligt at identificere de registrerede i længere tid end det nødvendige til det formål, som oplysningerne behandles for.

Klubben

Klubben bør som udgangspunkt slette data for tidligere medlemmer og personer, der ikke er medlemmer. Undtagelse kan gøres, hvis det af bogholderi- eller tilskudsmæssige årsager er nødvendigt at holde på oplysningerne i længere tid.

Integritet og fortrolighed

Personoplysningerne skal behandles på en måde, der sikrer en tilstrækkelig sikkerhed, herunder mod uautoriseret eller ulovlig behandling, hændeligt tab m.v., og ved brug af passende tekniske eller organisatoriske foranstaltninger. Forordningens art. 32 uddyber kravet yderligere.

Klubben

Klubben skal sikre sig, at medlemsdataene alene deles mellem et fåtal af personer i klubben, og at selve formatet, hvori oplysningerne opbevares, også er rimeligt sikkert i forhold til omstændighederne.

Eksempel: Hvis det er en formand og kasserer der håndterer alle forhold omkring medlemmerne, bør medlemsdataene alene deles mellem de to. Begge skal sikre sig, at medlemsdataene opbevares fortroligt. For en organisation som klubben vil det blive anset for tilstrækkeligt, at medlemsdataene opbevares på en almindelig computer, der er password-beskyttet, opdateret med en gængs sikkerhedspakke og hvis flere har adgang til computeren eller filen med oplysningerne sendes over email, bør filen (f.eks. Word eller Excel) password-beskyttes, sådan at man kun kan læse dem ved at indtaste et password.

Ved ændringer i personkredsen, der varetager administrationen, bør klubben sikre sig, at de afgående personer over for klubben erklærer, at de ikke længere er i besiddelse af eller selv har adgang til medlemsoplysningerne.

Ansvarlighed

Den dataansvarlige er ansvarlig for og skal kunne påvise overholdelsen af ovenstående principper.

Klubben

Klubben skal sikre sig, at overholdelsen af de ovenstående principper kan dokumenteres til enhver tid. Den ene del af dokumentationen er, at have en nedskrevet politik for, hvilke personoplysninger der indsamles og behandles, hvorledes de opbevares, hvem der har adgang til dem, mv., mens den anden del selvsagt handler om at overholde politikken og regelmæssigt at følge op på om politikken overholdes (se yderligere nedenfor om dokumentationskravene).

Eksempel: I forhold til klubben kan politikken holdes på 1-2 sider, der specificerer klubbens konkrete behandling af data, f.eks. at alene de ovennævnte persondata registreres, at de skal opbevares i en password-beskyttet excel-fil på en almindelig sikker password-beskyttet PC, alene må deles mellem de personer, der har med administrationen af medlemskabet og evt. tilskud at gøre.

Ledelsen i klubben skal desuden på regelmæssig vis, mindst årligt, undersøge om politikken og derved GDPR overholdes af i klubben.

Retsgrundlaget for behandling af personoplysninger

Grundlaget for behandling af personoplysninger afhænger af hvilken type oplysninger, der behandles, dvs. følsomme eller ikke-følsomme oplysninger. For begge typer af oplysninger gælder det dog, at den dataansvarlige altid kan behandle oplysningerne på grundlag af et samtykke fra den registrerede.

Reglerne om grundlaget for behandling af ikke-følsomme personoplysninger fremgår af GDPR forordningens art. 6 og lovens § 6, mens reglerne for grundlaget for behandlingen af følsomme oplysninger fremgår af henholdsvis art. 9 og § 7.

Klubben

Da klubbens medlemsdata er følsomme personoplysninger, jf. ovenfor, skal klubbens grundlag for at behandle oplysningerne findes i reglerne for behandling af følsomme personoplysninger (forordningens art. 9 og lovens § 7).

Af de regler følger, at en organisation, der ikke arbejder med gevinst for øje, og hvis sigte er af fagforeningsmæssig art, kan foretage behandling af personoplysninger som led i organisationens legitime aktiviteter og forudsat overholdelsen af de ovenstående grundlæggende principper.

Behandlingen af følsomme oplysninger må alene angå organisationens medlemmer, tidligere medlemmer og personer der er i regelmæssig kontakt med organisationen pga. dets formål, og ingen af de følsomme personoplysninger må videregives uden samtykke til nogen uden for organisationen.

Da klubbens formål med indsamling af oplysninger kan være indberetning til kommune, fagforening o.lign, vil et samtykke hertil skulle indhentes fra den registrerede.

Af samme årsag må det anbefales, at klubben får samtykke fra den registrerede allerede på tidspunktet for indsamlingen, såvel til klubbens almindelige behandling af personoplysningerne som en eventuel videregivelse heraf.

Samtykke

GDPR stiller krav til indholdet og udformingen af et samtykke fra den registrerede til den dataansvarliges behandling af personoplysninger.

Samtykket skal være en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, om at den dataansvarlige må behandle personoplysninger om vedkommende til et givent formål. Det følger heraf, at samtykket ikke kan være stiltiende.

Derudover følger det af GDPR art. 7, at den dataansvarlige skal kunne påvise samtykket, at hvis samtykket er skriftligt skal det være letforståeligt og tilgængeligt, og at den registrerede kan trække samtykket tilbage på samme lette måde til enhver tid, som da samtykket blev givet.

Klubben

Hvis klubben indberetter medlemsoplysninger til udenforstående, er det tvingende nødvendigt at indhente samtykke fra de registrerede til denne videregivelse. Det er ikke nødvendigt, at klubben beder om et samtykke til overhovedet at kunne behandle medlemmernes personoplysningerne.

Hvorledes samtykket indhentes er underordnet, det vigtigste er at samtykket efterfølgende kan påvises af klubben. Samtykket kan således indhentes via email (”klik ”ja””), via hjemmeside (”kryds af i feltet”) eller pr. brev (underskriv nederst). Hvis der indhentes elektronisk samtykke (altså vi email/hjemmeside), skal klubben sikre sig så vidt muligt, at det er medlemmet selv, der giver samtykket.

Det skal gøres klart for medlemmet, hvad konsekvensen er for ikke at give sit samtykke. Hvis klubben ikke kan køre rundt uden medlemmernes samtykke til indberetning vil det være acceptabelt, at konsekvensen er, at man ikke kan være medlem, men hvis der ikke er en sådan kobling, så vil det være i strid med GDPR at kræve samtykket.

Klubben kan med fordel koble opnåelsen af samtykket sammen med den oplysningspligt, som klubben har (se nedenfor).

Eksempel: Klubben kan udsende et brev/email til sine medlemmer, give dem oplysningerne påkrævet efter sin oplysningspligt, og bede dem svare tilbage med et ja eller nej tilbage pr. email i forhold til indberetningen. Alternativt kan medlemmerne på et arrangement blive bedt om, at underskrive en fysisk samtykkeblanket.

Den dataansvarliges særlige pligter

Det er lagt til grund i denne vejledning, at klubben alene modtager personoplysninger om et medlem direkte fra medlemmet selv. Der indsamles altså ikke oplysninger om vedkommende fra nogen anden kilde.

Oplysningspligten ved indsamling af oplysninger hos den registrerede

Den dataansvarlige har en oplysningspligt over for de registrerede om behandlingen af deres data. Oplysningspligten behøves ikke opfyldt, hvis medlemmerne allerede er bekendt med de oplysninger, som den dataansvarlige skal give dem. Oplysningspligtens indhold er beskrevet i forordningens art. 13.

Klubben

For klubben omfatter oplysningspligten, at de nedenstående oplysninger gives til de registrerede på tidspunktet for indsamlingen:

(i) Identitet og kontaktoplysninger på klubben.
(ii) Formålene med den klubbens behandling, og retsgrundlaget for behandlingen (jf. ovenfor).
(iii) Eventuelle modtagere eller kategorier af modtagere af oplysningerne.

Desuden skal der gives følgende oplysninger, som har til formål at sikre den dataansvarliges rimelige og gennemsigtige behandling af personoplysningerne:

(iv) Efter hvilke kriterier oplysningerne vil blive opbevaret af klubben (højst sandsynligt så længe personen er medlem af klubben og i en periode derefter afhængig for at kunne dokumentere medlemskabet over for myndigheder o.lign).
(v) Retten til at bede om indsigt i og berigtigelse eller sletning af personoplysniner om den registrerede, samt en eventuel ret til at modtage oplysningerne i et maskinlæsbart format (gælder, hvis behandlingen er baseret på et samtykke, jf. art. 20).
(vi) Retten til at trække et samtykke til en behandling tilbage.
(vii) Retten til at indgive en klage til Datatilsynet.
(viii) Konsekvenserne af ikke at give personoplysningerne til klubben

Det bemærkes, at i det omfang klubben måtte ønske at behandle oplysningerne til andre formål end dem de er indsamlet til, skal den registrerede opdateres herom forud for en sådan behandling.

Underetningspligt til modtagerne

Den dataansvarlige har pligt til at underrette modtagerne af personoplysningerne om enhver berigtigelse, sletning eller begrænsning af behandling, der er udført af den dataansvarlige efter anmodning fra den registrerede (i henhold til den registreredes rettigheder hertil, se nedenfor).

Klubben

Hvis klubben videregiver medlemsdata til kommunen, fagforening o.lign. har klubben også pligt til at berigtige, få slette eller få begrænset modtagerens behandling af medlemsdatene i samme omfang, som klubben selv måtte være blevet pålagt under GDPR.

Pligt til at føre fortegnelse over behandlingen af personoplysninger

Hvis den dataansvarlige behandler følsomme oplysninger, som i tilfældet med fagforeningsklubber, har den dataansvarlige pligt til at føre en skriftlig og elektronisk fortegnelse over behandlingen som nærmere beskrevet i forordningens art. 30. Fortegnelsen er et internt dokument, der skal sikre at den dataansvarlige har opfyldt sine forpligtelser efter GDPR, og som skal stilles til rådighed for Datatilsynet ved modtagelse af anmodning herom.

Klubben

For klubben skal fortegnelsen indeholde følgende oplysninger

i) Navn og kontaktoplysninger på den dataansvarlige og den dataansvarliges repræsentant (navn og adresse på klubben og de personer, der står for behandlingen af oplysningerne)
ii) Formålene med behandlingen af medlemmernes personoplysninger (typisk ”medlemsadministration” og ”opnåelse af støtte i forhold til medlemmer over x år”)
iii) En beskrivelse af kategorierne af registrerede (f.eks. ”medlemmer af fagforening X over 60 år”) og kategorierne af personoplysninger (dvs. typisk blot ”navn”, ”adresse”, ”fødselsdato”, ”email-adresse”, ”telefonnummer” og ”fagforeningsmæssigt tilhørsforhold”)
iv) Kategorierne af modtagere som vil personoplysningerne vil blive videregivet til (typisk kommune X, fagforening Y, o.lign.)
v) Hvis muligt, de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger.
vi) Hvis muligt, en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger truffet til beskyttelse af oplysningerne i henhold til forordningens art. 32 (typisk: organisatorisk: ”begrænsning af deling af oplysningerne mellem person x og person y”, og teknisk: ”kodet fil med medlemsoplysningerne” og ”brug af sikret email ved fremsendelse til andre” (eller lignende).

En skabelon til en fortegnelse er vedlagt som bilag 1 til dette notat.

Andre pligter

Den dataansvarlige har også andre pligter under GDPR, der angår den dataansvarliges adfærd og reaktion. Disse omfatter samarbejde med myndigheder, anmeldelse til Datatilsynet ved brud på datasikkerheden og i alvorlige tilfælde til den registrerede, og opfyldelse af den registrerede rettigheder i relation til personoplysningerne. Sådanne pligter gennemgås ikke nærmere i denne vejledning.

Den registreredes særlige rettigheder

Den registrerede har en række rettigheder over for dataansvarlige, som den registrerede kan anmode om opfyldes. Rettighederne af relevans for en klub, og som ikke gennemgås yderligere, omfatter blandt andet retten til:

(i) berigtigelse af oplysninger,
(ii) sletning af oplysninger (retten til at blive glemt),
(iii) begrænsning af behandlingen af oplysninger,
(iv) underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
(v) ret til dataportabilitet (modtage en struktureret maskinlæsbar udskrift af sine personoplysninger hos den dataansvarlige)

Konsekvenserne af manglende overholdelse af GDPR

Manglende overholdelse af GDPR vil efter loven medføre erstatningsansvar over for den registrerede og strafansvar med bøde eller fængsel op til 6 måneder. Strafansvaret kan også ifaldes af de konkrete personer, der får adgang til personoplysningerne og ikke behandler dem i henhold til lovgivningen.

Datatilsynet har i offentlige høringer nævnt, at man har forståelse for, at der vil være en indkøringsperiode for den nye lovgivning efter ikrafttrædelsen d. 25. maj 2018, og at fokus vil være på de organisationer og virksomheder, der helt tilsidesætter deres pligter, og ingen indsats forsøger at gøre for at overholde lovgivningen.

København, 4. maj 2018

Mandeep Singh Rathour

BILAG 1

SKABELON TIL FORTEGNELSE OVER BEHANDLINGSAKTIVITER

Dataansvarlig	**Klubbens navn CVR-nr. og kontaktoplysninger** *(adresse, hjemmeside, telefonnummer og e-mail)*	*Indsæt klubbens oplysninger*
	Den dataansvarliges repræsentant samt dennes kontaktoplysninger *(adresse, hjemmeside, telefonnummer og e-mail)*	*Indsæt kontaktoplysninger på personerne, som er ansvarlige for klubbens behandling af personoplysingerne.*
Formål(-ene)	**Behandlingens eller behandlingernes formål** *(et samlet, logisk sammenhængende formål med en behandling eller en række af behandlinger, som hermed angives som ét formål ud af alle samlede formål hos den dataansvarlige)*	Medlemsadministration
Kategorierne af registrerede og kategorierne af personoplysningerne	**Kategori af registrerede personer** *(medlemmer) (hvis andre personkategorier også registreres skal dette indsættes her og formålet dermed skal indføjes ovenfor)*	Der behandles oplysninger om følgende kategorier af registrerede personer: a) medlemmer af klubben *b) [andre]*
	Oplysninger, som behandles om de registrerede personer *(beskriv de typer af oplysninger, som er omfattet af behandlingsaktiviteterne)*	Der behandles følgende oplysninger: a) navn b) adresse, telefon-/mobilnr. og email-adresse(r) c) fagforeningsmæssige tilhørsforhold d) eventuelle besvarelser af relevante forhold relateret til personoplysninger (samtykker mv.)
Modtagerne af personoplysningerne	**Kategorier af modtagere som oplysninger er eller vil blive videregivet til herunder modtagere i** **tredjelande og internationale organisationer** *(eksempelvis andre myndigheder, virksomheder, borger/kunder mv.)*	Oplysningerne vil blive videregivet til følgende: *a) [navn på offentlige myndighed(-er)]* *b) [fagforeningen, hvis den skal have noget at vide om medlemsskabet]* *c) [andre?]*

Sletning	**Tidspunkt for sletning af oplysninger** *(de forventede tidsfrister for sletning af de forskellige kategorier af oplysninger)*	Oplysninger om tidligere medlemmer slettes senest *X* år efter medlemskabets ophør.
Tekniske og organisatoriske sikkerhedsforanstaltninger	**Generel beskrivelse af tekniske og organisatoriske sikkerheds- foranstaltninger** *(hvis muligt skal der gives* *en generel beskrivelse af de tekniske og organisatoriske sikkerhedsforanstaltninger, jf. artikel 32, stk. 1)*	Medlemslisten opbevares i MS Excel-format, der er passwordbeskyttet. Excel-filen er lagret på formandens og kassererens laptops, der begge er passwordbeskyttede [*og meget gerne krypteret med Windows Bitlocker henholdsvis Apple's Filevault]* Transmittering af den passwordbe-

		Der anvendes følgende sikker-

BACH | ADVOKATER