Vejledning om GDPR til jer, der driver en mindre forening

7 trin, der hjælper jer med at overholde GDPR

DATATILSYNET

Overblik

Grundlæggende om GDPR

Hvad er GDPR?

Når I som forening i Danmark bruger personoplysninger, skal I overholde GDPR.

GDPR står for ”General Data Protection Regulation” og er på dansk også kendt som databeskyttelsesforordningen. GDPR er EU-reglerne for databeskyttelse og gælder bl.a., når foreninger behandler oplysninger om personer (personoplysninger).

Alle danskere har som EU-borgere en række rettigheder i GDPR. Det betyder konkret, at når I som en forening ”behandler personoplysninger” om andre – dvs. indsamler, registrerer, videregiver eller sletter personoplysninger om f.eks. dine medlemmer, frivillige eller ansatte – skal I overholde GDPR.

Hvorfor GDPR?

Reglerne har skabt et øget fokus på den enkelte borgers ret til at have kontrol over sine egne data – det gælder også dine oplysninger, når du som privatperson bliver medlem af en forening. Med GDPR har vi som EU-borgere de samme databeskyttelsesrettigheder inden for EU – uanset hvilket EU-land, vores data bruges i.

Når det gælder foreninger, skal GDPR skabe nogle klarere regler for brug af personoplysninger som interesseorganisation. Som en fælles EU-lov gør GDPR de forskellige EU-landes håndtering af databeskyttelsesreglerne ensartet og fjerner unødvendig administration på tværs af landene.

GDPR er fleksible regler

I kender bedst jeres forening, og det er derfor også jer, der er de bedste til at vurdere, hvilke personoplysninger, I har behov for at behandle for at holde jeres forening kørende. Derfor er det også jer, der skal vurdere, til hvilke formål I behandler personoplysninger, og hvor længe det er nødvendigt at gemme oplysningerne.

Formålet med at udforme databeskyttelsesreglerne som fleksible regler, hvor I selv skal vurdere og sikre, at I lever op til reglerne er ikke at skabe usikkerhed eller bekymring for jer som forening, men derimod at sikre, at reglerne har den nødvendige fleksibilitet til at favne de mange forskellige typer af foreninger.

Heldigvis har I altid mulighed for at få vejledning af Datatilsynet, og typisk vil jeres brancheforening også kunne være behjælpelig med at besvare konkrete spørgsmål til netop jeres forenings håndtering af GDPR.

1 Skab overblik

Reglerne om databeskyttelse gælder også for jer som en lille forening, hvis I bruger eller opbevarer oplysninger om andre personer.

For at I kan overholde reglerne, er det vigtigt, at I får skabt et overblik over:

- hvor I har personoplysninger
- hvem I håndterer personoplysninger om
- hvilke personoplysninger I håndterer

Find ud af, hvor I har personoplysninger

I vil sandsynligvis have personoplysninger gemt på jeres telefon, tablet, computer eller it-systemer, f.eks. i e-mails og SMS'er. Det kan også være, at I har printede dokumenter med personoplysninger på. Det kunne være navne og kontaktoplysninger på medlemmer eller ansatte, men også information om kommende bookinger, aftaler, ordrebøger eller andre bestillinger. Husk, at hvis I kan identificere en person ud fra noget, I har gemt, så er der tale om personoplysninger.

Find ud af, hvem I håndterer oplysninger om

Når I har fundet ud af, hvor I opbevarer personoplysninger, bør I notere jer, hvem oplysningerne handler om. I kan med fordel inddele disse personer i samlede grupper, herunder:

- Personer, som foreningen kommer i kontakt med i forlængelse af foreningens drift - f.eks. medlemmer, beboere eller grundejere
- Personer, der yder ulønnet frivilligt arbejde
- Personer, der er ansat i foreningen.

Find ud af, hvilke oplysninger I håndterer

Når I har fundet ud af, hvor der kan være personoplysninger, og hvem I håndterer oplysninger om, bør I starte med at lave en oversigt over, hvilke typer af oplysninger I har om de forskellige grupper, f.eks. "medlemmers telefonnumre".

Håndterer andre personoplysninger på jeres vegne?

Det ovenstående overblik, som I skal skabe, gælder også, hvis I har fået andre til at håndtere oplysningerne på vegne af jer.

Fortegnelse

En fortegnelse er et andet ord for en ordnet oversigt. Begrebet bruges i GDPR til at beskrive den oversigt, man skal lave, når man håndterer personoplysninger om andre.

På Datatilsynets hjemmeside, kan I hente en skabelon til en fortegnelse over oplysninger om et idrætsforeningsmedlem.

2 Spørg jer selv "hvorfor"

Når I har oplysninger om andre, f.eks. medlemmer, beboere eller frivillige, skal I først og fremmest finde ud af, om I har en god grund til at have personoplysningerne.

Her kan foreningen med fordel spørge sig selv "Hvorfor har vi oplysningerne?". Hvis I kan besvare dette spørgsmål på en fornuftig måde, har I som udgangspunkt en god grund til at have oplysningerne. En god grund kan f.eks. være, at I har personoplysninger på et medlem, som har meldt sig ind i jeres forening eller en beboer, som er blevet valgt ind i bestyrelsen.

Lovlige grundlag
Selvom I har en god grund til at have oplysninger om andre, er det også nødvendigt, at I opfylder en eller flere betingelser i loven for at have oplysningerne. I må håndtere personoplysninger, hvis én af følgende betingelser er opfyldt:

- I forfølger jeres gode grund, samtidig med at jeres brug af oplysningerne ikke medfører gener eller konsekvenser for den, som I håndterer oplysninger om
- I har behov for personoplysninger, for at opfylde en aftale, som I har indgået med den, som I håndterer oplysninger om
- I er forpligtet af en anden lovgivning til at håndtere oplysningerne
- I har samtykke fra den, som I håndterer oplysninger om.

Foreningen skal altid vælge det lovlige grundlag, som passer bedst til den enkelte situation.

I nogle tilfælde vil det være foreningens aftale med eksempelvis et medlem, som udgør det lovlige grundlag. Det kan f.eks. være, hvis I har betalingsoplysninger om jeres medlemmer, fordi I skal opkræve kontingent. Det skyldes, at I skal bruge oplysningerne, for at kunne opfylde jeres aftale med medlemmet.

I mange andre tilfælde kan foreninger behandle personoplysninger, som er nødvendige i forlængelse af foreningens drift, fordi foreningen har en god grund til det, samtidig med at brugen af oplysningerne ikke medfører særlige gener eller konsekvenser for de personer, som foreningen håndterer oplysninger om.

Der skal derfor kun indhentes samtykke, hvis der ikke findes et andet lovligt grundlag. Det kan være i tilfælde af, at jeres behandling af oplysningerne medfører gener eller konsekvenser for den person, som I håndterer oplysninger om.

Er der tale om følsomme personoplysninger, som f.eks. er oplysninger om race, politisk overbevisning, religiøs overbevisning, helbredsoplysninger og seksuel orientering, gælder der som udgangspunkt et forbud mod at behandle oplysningerne. Der findes dog en række undtagelser til dette forbud, f.eks. vil en forening typisk kunne håndtere sådanne oplysninger, hvis det er nødvendigt for, at I kan fastlægge et retskrav, eller I har den pågældendes samtykke.

Husk
I skal i øvrigt altid være opmærksomme på, at I ikke må håndtere flere oplysninger end dem, I skal bruge.

3 Husk at slette

Selvom ingen personer har rettet henvendelse med et ønske om sletning, skal I stadig helt generelt overveje, hvor længe I opbevarer oplysninger. Hvis en person retter henvendelse om sletning, skal I tage stilling til, om hensynet til den, som retter henvendelse, vejer tungere end hensynet til at opbevare.

I skal slette personoplysninger, når foreningen ikke længere har behov for at have personoplysningerne. Det betyder, at personoplysningerne skal slettes, når det ikke længere er nødvendigt at håndtere oplysningerne for at opfylde den gode grund (se trin 2: Spørg dig selv hvorfor).

Hvis det følger af andre regler, at I skal gemme personoplysninger, hvilket f.eks. er tilfældet i bogføringsloven, skal I ikke slette personoplysningerne, så længe I er forpligtet til at opbevare oplysningerne. Bogføringsloven siger nemlig, at visse foreninger skal opbevare regnskabsmateriale i fem år beregnet fra udgangen af det regnskabsår, som materialet vedrører.

Hvis foreningen ikke er forpligtiget til at gemme personoplysninger i henhold til anden lovgivning, er det databeskyttelsesreglerne, der bestemmer, hvor længe oplysningerne må opbevares. I sådanne tilfælde kan det være vanskeligt at fastsætte en præcis opbevaringsperiode, da beskyttelsesreglerne ikke angiver faste tidsgrænser for opbevaring af personoplysninger.

I ved bedst, hvornår det er nødvendigt at slette

Når databeskyttelsesreglerne ikke specifikt angiver, hvor længe foreningen må håndtere personoplysninger, skyldes det, at det er foreningen, der bedst kan vurdere, hvor længe foreningen har brug for personoplysningerne.

Det betyder, at I har et vist råderum til at vurdere, hvor længe det er nødvendigt for jer at opbevare personoplysninger, for at opfylde formålet/formålene. I praksis kan I som forening spørge jer selv, ”hvorfor har vi stadig brug for oplysningerne?”. Så længe I kan besvare dette spørgsmål på en fornuftig måde, kan foreningen opbevare personoplysningerne.

Så længe I har rutiner, der sikrer, at I løbende sletter personoplysninger, har I ikke pligt til løbende at gennemgå samtlige dokumenter mv. for at overveje, om enkeltstående oplysninger er nødvendige at gemme (se trin 5: Sørg for at have gode procedurer).

At det er foreningen, der bedst kan vurdere, hvor længe I har brug for personoplysningerne, indebærer derfor også, at I som forening i langt de fleste tilfælde ikke skal være nervøse for, at Datatilsynet vil være uenig i en slettefrist, I har fastsat.

4 Oplys om, at I behandler personoplysninger

Foreningen har pligt til at oplyse medlemmer, frivillige og ansatte om, at I har oplysninger om dem. Udover at oplyse dem om, at I har oplysninger om dem, skal I give dem en række andre informationer, f.eks. om hvad I skal bruge oplysningerne til, og hvor længe I gemmer dem. Hvis I får oplysningerne fra personen selv, skal I give informationen på det tidspunkt, I modtager dem. Hvis I får oplysningerne fra andre end personen selv, skal I give oplysningerne hurtigst muligt - og senest inden 1 måned efter at I har modtaget oplysningerne.

I skal informere på en måde, der er let for folk at forstå. I kan med fordel give informationen i en privatlivspolitik, som ligger lettilgængeligt på foreningens hjemmeside, og som I kan linke til, f.eks. når et nyt medlem melder sig ind i foreningen.

Foreningen skal oplyse om følgende:

Identitet og kontaktoplysninger
Dette er foreningens navn og kontaktoplysninger.

Hvilke personoplysninger
De typer af oplysninger, som I har fundet i forbindelse med trin 1: Skab overblik.

Hvorfor
Her skriver I jeres gode grund og jeres lovlige grundlag fra trin 2: Spørg jer selv hvorfor.

Hvor længe gemmes oplysninger
Her skrives jeres overvejelser fra trin 3: Husk at slette.

Hvem oplysningerne evt. deles med
Hvis I giver folks oplysninger til nogen uden for jeres forening, skal I oplyse om, at I gør dette, og om hvem der modtager oplysningerne. Det kan f.eks. være, hvis nogen håndterer oplysningerne på foreningens vegne.

Rettigheder
Her kan I med fordel skrive følgende:

”Du har efter databeskyttelsesforordningen en række rettigheder i forhold til vores behandling af oplysninger om dig.

Ret til at se oplysninger (indsigtsret)
Ret til berigtigelse (rettelse)
Ret til sletning
Ret til begrænsning af behandling
Ret til indsigelse
Ret til at transmittere oplysninger (dataportabilitet)

Hvis du vil gøre brug af dine rettigheder, skal du kontakte os.

Du har i øvrigt ret til at indgive en klage til Datatilsynet, hvis du er utilfreds med den måde, vi behandler dine personoplysninger på. Du finder Datatilsynets kontaktoplysninger på www.datatilsynet.dk”

5 Sørg for at have gode procedurer

De personer, hvis oplysninger I bruger eller gemmer, har en række rettigheder. De har bl.a. ret til at anmode om at få en kopi af deres oplysninger (ret til indsigt), at få forkerte oplysninger rettet (ret til berigtielse) og at få deres oplysninger slettet (ret til sletning).

Hvis en person anmoder om at gøre brug af en af disse rettigheder, skal foreningen svare inden for en måned, også selvom I afviser deres anmodning. For at sikre, at foreningen kan svare inden for denne frist, er det en god idé at have gode procedurer for, hvordan I håndterer disse anmodninger.

Tjekliste
Her kan I finde en tjekliste, som I kan bruge, når I modtager en anmodning fra en person, som ønsker at gøre brug af sine rettigheder.

- ✓ **1. Vælg en ansvarlig**
  Vælg en person til at være tovholder på alle opgaver, som handler om databeskyttelse.
- ✓ **2. Vær sikker på, hvem personen er**
  I skal tjekke, hvem der anmoder om at gøre brug af sine rettigheder. I må gerne bede om mere information, men bed kun om at se ID, hvis det er absolut nødvendigt.
- ✓ **3. Tjek, at de har ret til det, som de beder om**
  Læs mere om de registreredes rettigheder på Datatilsynets hjemmeside.
- ✓ **4. Find ud af, hvad personen vil have**
  Spørg gerne ind til, hvad det præcist er, personen gerne vil have oplyst, slettet, rettet mv.
- ✓ **5. Sæt deadlines**
  I skal svare inden for en måned. Sæt derfor gerne en for deadline for jer selv, som er kortere end en måned, så I er sikre på at nå det. Hvis I modtager en kompliceret anmodning, kan I forlænge fristen med to måneder. I skal dog gøre personen opmærksom på, at det kommer til at tage længere tid.
- ✓ **6. Søg efter information om personen de relevante steder**
  I skal overveje, hvor I kan have oplysninger liggende, og vær grundig når I leder. Husk også at tænke på eksterne harddiske, USB-stik, opslag på sociale medier mv. Det kan også være hos andre, som håndterer oplysningerne på vegne af foreningen.
- ✓ **7. Tjek om materialet, I udleverer, indeholder oplysninger om andre**
  I må ikke udlevere oplysninger om andre personer end personen selv. Hvis det materiale, som I vil udlevere, indeholder oplysninger om andre, skal I fjerne oplysningerne om disse andre personer. Det kan I f.eks. gøre ved at overstrege oplysningerne eller sløre et billede eller videomateriale. Hvis I bruger en computer til dette, skal I fjerne oplysningerne på en måde, så modtageren ikke kan genskabe informationen.
- ✓ **8. Forbered de supplerende oplysninger og jeres svar**
  Udover selve oplysningerne skal personen også have at vide, hvorfor I bruger deres oplysninger, hvordan I har fået dem, hvor længe I planlægger at gemme dem, hvem I deler dem med, og hvordan de kan få deres oplysninger slettet eller forkerte oplysninger rettet. Link eventuelt til jeres privatlivspolitik, som I har udarbejdet i forbindelse med trin 4: Oplys om at du behandler personoplysninger.

6 Husk sikkerheden

Hvorfor IT-sikkerhed?
Cyberangreb rammer både små og store foreninger. Derfor spiller IT-sikkerhed en vigtig rolle, når foreningens systemer og personoplysninger skal beskyttes.

Hvis I ikke har tænkt over IT-sikkerhed før, så start med de elektroniske enheder, hvor I håndterer personoplysninger, der kræver særlig beskyttelse - fx helbredsoplysninger, CPR-numre og børneattester. Elektroniske enheder er fx PC, tablets, mobil, USB-stik og ekstern harddisk.

Praktiske råd til bedre behandlingssikkerhed
SikkerDigital har samlet 7 gode råd om it-sikkerhed, som kan hjælpe små og mellemstore foreninger med at styrke deres basale digitale sikkerhed:

1. Få overblik over vigtige data og systemer
2. Opdater programmer, herunder applikationer, løbende
3. Køb antivirus og firewall
4. Tag backup af data
5. Lær at spotte mistænkelige e-mails
6. Lav stærke adgangskoder
7. Stil sikkerhedskrav til IT-leverandører

Har I outsourcet?
Hvis I har outsourcet IT-driften og IT-sikkerheden, er det jeres ansvar at stille de rigtige krav til jeres leverandør. SikkerDigital har udarbejdet en værktøjskasse med vejledning og et spørgeskema, som kan hjælpe jer med at stille de rigtige spørgsmål og krav til jeres IT-leverandør.

Tænk sikkerhed ind i dine arbejdsprocesser

Nedenunder finder I en række lavpraktiske råd, der giver god sikkerhed i de daglige arbejdsprocesser – også når man arbejder hjemmefra.

Brug sikker WiFi
Så risikerer I ikke, at andre uberettiget får adgang til oplysninger om jeres frivillige, medlemmer, ansatte eller foreningens forhold.

Lås skærmen, når I forlader jeres plads – uanset hvor længe I er væk
Så risikerer I ikke uberettiget adgang til oplysninger om jeres frivillige, medlemmer eller ansatte via jeres elektroniske enheder med personoplysninger.

Lås skærmen, når I forlader jeres plads – uanset hvor længe I er væk
Så risikerer I ikke uberettiget adgang til oplysninger om jeres frivillige, medlemmer eller ansatte via jeres elektroniske enheder med personoplysninger.

6

Lås skærmen, når I forlader jeres plads – uanset hvor længe I er væk
Så risikerer I ikke uberettiget adgang til oplysninger om jeres frivillige, medlemmer eller ansatte via jeres elektroniske enheder med personoplysninger.

Husk sikkerheden, når I arbejder på distancen
Når I arbejder på distancen, skal I huske at beskytte jeres elektroniske enheder, som hvis I var på arbejdspladsen. I skal også være opmærksom på jeres omgivelser, fx hvis I arbejder i toget eller i bussen, hvor andre personer potentielt kan følge med på jeres skærm eller lytte til jeres samtale.

Afskaf elektroniske enheder på en forsvarlig måde
Inden I afskaffer jeres elektroniske enheder fx mobil, tv, pc og tablet, skal I sikre jer, at enhederne ikke indeholder personoplysninger. Det kan I gøre ved at nulstille enheden. Alternativt kan I sikre jer, at oplysningerne på ingen måde kan tilgås af andre, f.eks. ved kryptering.

Efterlad ikke fysiske dokumenter og elektroniske enheder uden opsyn
Brud på persondatasikkerheden kan opstå, når fysiske dokumenter eller elektroniske udstyr med personoplysninger efterlades uden opsyn på steder, hvor uvedkommende har adgang. Det kan typisk være på hotellet, i bilen eller i toget. Sørg for altid for at opbevare jeres dokumenter og enheder et sikkert sted, når de ikke er i brug.

Hav styr på, hvem der har adgang til hvad
I skal altid have styr på, hvem der har adgang til hvilke systemer og bygninger, samt hvorfor de har adgang. I kan ikke lade enhver have adgang til jeres systemer og bygninger, da sikkerheden forringes og risikoen for brud på persondatasikkerheden øges. I skal derfor begrænse adgangen, så det kun er personer med et arbejdsbetinget behov, der har adgang. Når en frivillig eller ansat stopper, skal I sørge for, at den pågældende ikke længere har adgang til systemer og bygninger.

Gem ikke personoplysninger i længere tid end nødvendigt
I kan begrænse jeres ansvar og jeres risiko ved ikke at opbevare flere personoplysninger end nødvendigt og ved ikke at opbevare dem længere end nødvendigt. Jo færre oplysninger I har, jo mindre risiko er der også for at miste data, f.eks. i forbindelse med et cyberangreb.

Send og modtag sikkert
I skal være særligt opmærksomme på, hvordan I sender/modtager personoplysninger, der kræver særlig beskyttelse, som f.eks. helbredsoplysninger, CPR-numre og børneattester.

Når I vælger at sende/modtage personoplysninger, er det vigtigste, at I vælger en sikker måde at kommunikere på, så personoplysninger ikke ender i de forkerte hænder.

I kan som regel godt kommunikere sikkert via e-mail.

Digital Post som f.eks. e-boks er også en sikker måde at kommunikere på. Forsendelse af fysisk brev eller pakke med posten betragtes ligeledes som en sikker kommunikation.

Husk, at hvis I sender elektroniske enheder, f.eks. USB-stik, PC eller ekstern harddisk, som indeholder fortrolige eller følsomme personoplysninger, skal enhederne være krypteret.

7 I er også ansvarlige, når I deler

I vil næsten altid have behov for at dele data med andre, enten fordi I gemmer personoplysninger i et IT-system, eller fordi I er forpligtet til at videregive personoplysninger til andre, f.eks. myndigheder. I GDPR skelner man mellem at være 'dataansvarlig' og 'databehandler', da det har en betydning for jeres ansvar, når I behandler personoplysninger.

Jeres forening er dataansvarlige for de personoplysninger, I behandler om jeres frivillige, medlemmer og ansatte. Det betyder, at det er jeres ansvar at sikre, at personoplysninger om jeres frivillige, medlemmer og ansatte bliver behandlet lovligt.

Når I anvender et IT-system
Leverandører af de IT-systemer, I bruger, vil typisk være databehandlere. Det kan være leverandører af software til udsendelse af nyhedsbreve (f.eks. Mailchimp), lønadministrationsprogrammer (f.eks. Bluegarden eller Visma), medlemssystemer (f.eks. Holdsport eller Membercare) og mailprogrammer (f.eks. Outlook i MS365, hotmail eller gmail).

Når I anvender en databehandler, skal I have en databehandleraftale. Det er vigtigt, at I har et overblik over de databehandleraftaler, I har med jeres leverandører. I kan med fordel gemme aftalerne i en mappe på jeres computere.

Når I videregiver personoplysninger til andre dataansvarlige
Nogle gange har I behov for at give personoplysninger om jeres frivillige, medlemmer eller ansatte videre til andre. Det kunne være til et bookingssystem, der skal bruge jeres medlemmers oplysninger, så de kan booke foreningens faciliteter, eller en samarbejdspartner der skal invitere jeres medlemmer til et fælles arrangement.

I skal tænke over, hvem I giver oplysningerne til, og I skal huske at informere jeres frivillige, medlemmer eller ansatte om, at deres oplysninger bliver delt. Det kan I passende gøre i jeres persondatapolitik, trin 4: Oplys om, at I behandler personoplysninger.

Har I spørgsmål til GDPR i jeres forening?
Skriv eller ring til os.

33 19 32 00
dt@datatilsynet.dk
www.datatilsynet.dk/gdprunivers-foreninger

GDPR-universet for små foreninger er lavet i samarbejde med

abf DGI Fonden for Socialt Ansvar

DATATILSYNET