Hvordan bliver man compliant?

Det kan ofte være svært at vurdere, hvad der skal til for, at man som dataansvarlig overholder kravene i persondataforordningen.

Nogle krav er hårde og kan ikke gradbøjes, mens andre dele af arbejdet med GDPR er baseret på skøn og vurderinger, hvor det vigtigste er, at I kan argumentere for jeres valg.

Denne liste indeholder de politikker, aftaler og dokumentationsgrundlag, I **skal** have. Vi har tilføjet en kort beskrivelse til hvert punkt, link til yderligere viden samt skabeloner, som I kan tage udgangspunkt i. Listen er ikke udtømmende, men den giver jer et godt indblik i, hvordan I kommer godt i gang med dit arbejde.

- Dokumenter til opfyldelse af oplysningspligten (datapolitikker)
    - Som dataansvarlig har I en ubetinget forpligtelse til at orientere de registrerede om jeres behandling af deres personoplysninger. Forpligtelsen findes i Persondataforordningens artikel 13 og 14.
    - Læs mere om de registreredes rettigheder i Datatilsynets vejledning.
    - I kan tage udgangspunkt i disse forslag til en datapolitik for frivillige og for deltagere, eller I kan benytte Datatilsynets skabelon.

- Dokumentation for de organisatoriske og tekniske foranstaltninger, I har vedtaget (intern datapolitik)
    - Som dataansvarlig har I pligt til at indføre passende organisatoriske og tekniske tiltag med henblik på beskyttelse af persondata. Forpligtelsen findes i Persondataforordningens artikel 32.

- Læs mere om de registreredes rettigheder i Datatilsynets vejledning.
- I kan også tage udgangspunkt i dette forslag.

- **En fortegnelse over foreningens behandlingsaktiviteter**
  - I har pligt til at føre en fortegnelse over jeres behandling af personoplysninger i henhold til Persondataforordningens artikel 30.
  - I kan læse mere om fortegnelser i Datatilsynets vejledning.
  - I kan tage udgangspunkt i Datatilsynets skabelon.

- **Kontrollister, der viser, hvordan foreningen vil kontrollere compliance og de vedtagne tiltag**
  - I har pligt til at undersøge og følge op på, hvorvidt jeres tiltag bliver overholdt, samt om I kan blive bedre til at beskytte personoplysningerne.
  - Kravet følger af Persondataforordningens artikel 32, stk. 1, litra d.

- **Risikovurdering af foreningens IT og datasikkerhed**
  - Kravet udspringer af Persondataforordningens artikel 32, stk. 2.
  - I kan læse mere om, hvordan I laver en risikovurdering i Datatilsynets vejledning.

- **Databehandleraftaler med alle foreningens databehandlere**
  - Før I lader andre behandle personoplysninger på jeres vegne, skal I indgå en databehandleraftale. Husk, at en modtager ikke bliver jeres databehandler, blot fordi I sender personoplysninger til vedkommende. Det er kun i de tilfælde, hvor modtagerens opgave består i at behandle personoplysningerne for jer – altså ikke til egne formål – at der kan blive tale om en databehandlerkonstruktion.
  - Reglerne om databehandlere findes i Persondataforordningens artikel 28.
  - Vurdering af dataansvar er en svær disciplin, hvorfor det er en god idé at læse Datatilsynets vejledning.
  - Skal I indgå en databehandleraftale, kan I med fordel benyttes Datatilsynets skabelon.
  - Husk, at I også skal føre tilsyn med jeres databehandlere, så I kan dokumentere, at de gør, som I har aftalt. I kan læse mere om tilsyn i Datatilsynets vejledning.

- Proces for databrud
    - [Organisation], de ansatte og de frivillige skal vide, hvad I skal gøre, hvis noget går galt i forbindelse med jeres databehandling. Derfor skal I have en procedure for, hvad I gør ved databrud.
    - Anmeldelse af databrud er lovpligtigt i henhold til Persondataforordningens artikel 33.
    - Datatilsynet har skrevet en vejledning til, hvordan I kan bære jer ad.

- Proces for henvendelse fra de registrerede
    - Alle de personer, som I behandler personoplysninger om, har nogle bestemte rettigheder i henhold til Persondataforordningen. Derfor skal I sikre jer, at jeres organisation er parat til at imødekommende den registreredes rettigheder jf. Persondataforordningens artikel 12.
    - Dette sikres typisk ved, at I udarbejder en procedure for, hvordan I håndterer henvendelser fra de registrerede.
    - I kan læse mere om disse rettigheder, samt hvordan I overholder dem, I Datatilsynets vejledning.

- Eventuelle aftaler om fælles dataansvar
    - Hvis I har et fælles dataansvar med andre organisationer, skal I indgå aftaler om, hvordan I behandler personoplysningerne sammen jf. Persondataforordningens artikel 28.
    - Datatilsynet har forklaret lidt om konceptet i denne vejledning, og I kan tilsvarende benytte Datatilsynets standardaftale.

- Standardkontrakter ved overførsel af data til usikre tredjelande (kun hvis relevant - kontrakten er en EU-standard)
    - Hvis I skal sende persondata ud af EU/EØS, kan det være nødvendigt at lave en "Transfer Impact Agreement" (TIA), der er et dokument, som tager stilling til risikoen ved at overføre persondata til et usikkert tredjeland.
    - Reglerne herom kan I finde i Persondataforordningens artikel 46, stk. 2, litra c.
    - I kan læse mere om konceptet og problematikkerne i Datatilsynets vejledning.

- Dokumentation for hvorfor/hvorfor ikke, foreningen skal have en DPO
    - Kravene til en ”Data Protection Officer” (DPO) eller en ”Databeskyttelsesrådgiver” kan I finde i Persondataforordningens artikel 37.
    - I kan læse mere om DPO-rollen i Datatilsynets vejledning.

- Dokumentation for, hvordan foreningen udfører kontrol med og underviser frivillige
    - For at overholde de vedtagne tiltag i Persondataforordningens artikel 32.

- Undervisningsmateriale
    - For at overholde de vedtagne tiltag i Persondataforordningens artikel 32.

- Årshjul, der dokumenterer, hvordan foreningen løbende udvikler GDPR-compliance
    - For at overholde de vedtagne tiltag i Persondataforordningens artikel 32.

- Dokumentation for vedtagne hjemmelsgrundlag, formål og slettepolitikker
    - For at kunne dokumentere beslutningsgrundlagene.

Husk, at ovenstående dokumenter alene er facit på jeres overvejelser, og reelt kun giver et overfladisk billede af jeres databehandling. En linje om, at I har besluttet at slette data efter 5 år, giver ikke megen indsigt i overvejelserne bag beslutningen. Derfor kan det være nødvendigt at lave yderligere dokumentation ud over ovenstående. Der kan derfor være behov for ekstra dokumentationsarbejde, men det kan afhænge af situationen og af jeres forening eller organisation.

GDPR er en "blød" lovgivning, hvor mange af reglerne er bundet op på et skøn. Det giver jer stor handlefrihed, men medfører også et større behov for dokumentation, da I skal kunne dokumentere, hvorfor I har foretaget et skøn, og hvorfor det er rimeligt. Alternativt kan I ende i situationer, hvor I skal dokumentere eller forklare på bagkant, hvilket ikke er hensigtsmæssigt.

Der findes masser af litteratur og gode vejledninger på nettet, som I med fordel kan grave frem. Særligt anbefaler vi, at I læser Justitsministeriets vejledning i persondata i frivillige foreninger, da denne vejledning giver et rigtig god indblik i de krav, I skal leve op til.

God arbejdslyst!