

Politik for beskyttelse og behandling af personoplysninger



Marts 2018

1. Indledning

Denne politik om beskyttelse og behandling af personoplysninger beskriver, hvordan vi i brancheforeningen ICF Danmark

- Behandler personoplysninger om foreningens medlemmer
- Anbefaler foreningens medlemmer at behandle personoplysninger i deres coaching-virksomhed

Grundlæggende behandler ICF Danmark og medlemmerne personoplysninger i overensstemmelse med ICFs etiske grundlag og gældende dansk lovgivning.

Politikken indarbejder persondataforordningens regler som er gældende med virkning fra 25. maj 2018.

Begreber



Figur 1: Datatilsynets definition af dataansvarlig og databehandler.

1. Hvad er personoplysninger?

Personoplysninger er enhver form for information, der kan identificere personer, som f.eks. navn, adresse, telefonnummer, personnummer, registreringsnummer eller lignende. Oplysninger i form af f.eks. et billede eller et fingeraftryk er også personoplysninger.

Persondataforordningen skiller mellem "personfølsomme oplysninger" og "almindelige personoplysninger" som det fremgår af nedenstående figur 1.

| | |
|--------------------------------------|--|
| Personfølsomme oplysninger | Race, Etnisk oprindelse, Politisk, religiøs eller filosofisk overbevisning, Fagforeningsmæssige tilhørsforhold, Genetiske data, Biometriske data mhp. entydig identifikation, Helbredsoplysninger, Seksuelle forhold eller orientering. |
| Straffedomme og lovovertrædelser | |
| Almindelige personoplysninger | Navn, Adresse, Fødselsdato, Væsentlige sociale problemer, Andre rent private forhold, Økonomi, Skat, Gæld, Sygedage, Tjenstlige forhold, Familieforhold, Bolig, Bil, Eksamen, Ansøgning, CV, Ansættelsesdato, Stilling, Arbejdsområde, Arbejdstelefon. |

Figur 1: Personfølsomme oplysninger og almindelige personoplysninger

Det er kun de personfølsomme oplysninger, som er nævnt i skemaet, persondataforordningen anser for at være personfølsomme. Personoplysninger som ikke falder ind under kategorien "følsomme personoplysninger", kan kaldes "almindelige personoplysninger" – som for eksempel identifikationsoplysninger som navn og adresse.

Regler om behandling af oplysninger om strafbare forhold samt CPR-numre fremgår ikke direkte af forordningen, men reguleringen heraf er i stedet overladt til de enkelte medlemslande. I lovudkastet, der skal implementere forordningen i Danmark, fremgår hjemlerne til at behandle strafbare forhold af § 8 og hjemlerne til at behandle CPR-numre af § 11.

1.1. Behandling af personoplysninger

Begrebet "behandling" omfatter enhver form for håndtering af personoplysninger. Det er først og fremmest elektronisk behandling af oplysninger, der er omfattet af reglerne. Det kan for eksempel være indsamling, registrering, systematisering, opbevaring, søgning, brug, videregivelse eller sletning af oplysninger.

Det betyder, at en virksomhed, som stiller en server til rådighed, som oplysningerne opbevares på, også foretager en behandling af oplysningerne ved at opbevare dem. Behandling kan også være offentliggørelse af oplysninger på en hjemmeside eller registrering af oplysninger i en elektronisk database.

1.2. Principper for behandling af personoplysninger

Brancheforeningen ICF Danmark og foreningens medlemmer forpligter sig til at behandle personoplysninger ud fra følgende seks grundlæggende principper:

1. **Lovlighed, rimelig og gennemsigtighed.** Den dataansvarlige skal overholde reglerne for behandling af oplysninger og skal give let tilgængelig information om behandlingen af oplysninger. Det indebærer bl.a., at den person, der behandles oplysninger om, som udgangspunkt skal have oplyst, hvem der er ansvarlig for behandlingen af oplysninger, og hvad der er formålet med behandlingen.
2. **Formålsbestemthed.** Databehandlingen skal være formålsbestemt og saglig. Data må ikke indsamles med den begrundelse, at det måske senere kan vise sig nyttigt at være i besiddelse af oplysningerne. Der skal være et legitimt formål med at registrere oplysningerne, og senere behandling ikke må stride mod det oprindelige formål.
3. **Dataminimering og proportionalitet.** Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet. En god tommelfingerregel er at behandle de oplysninger, som er *need to know* og ikke oplysninger som er *nice to know*, det vil sige så få oplysninger som muligt.
4. **Datakvalitet.** Oplysningerne skal være rigtige og ajourførte, og hvis oplysningerne viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges.
5. **Opbevaringsbegrænsning.** Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne. Det er i første omgang op til den enkelte dataansvarlige at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra det formål, som oplysningerne oprindeligt blev indsamlet til. Ved sletning af elektroniske data skal oplysningerne også slettes fra backup systemerne.
6. **Integritet og fortrolighed.** Den dataansvarlige er forpligtet til at sørge for de nødvendige sikkerhedsforanstaltninger, så oplysninger ikke kommer i de forkerte hænder, behandles ulovligt, går tabt, tilintetgøres eller beskadiges.

Disse seks principper er kernen af god databehandling. Principperne har været gældende hidtil, og med persondataforordningen suppleres de med et nyt princip:

7. **Ansvarlighed.** Den dataansvarlige er ansvarlig for, at de seks grundlæggende principper efterleves og skal kunne påvise, at det sker.

Det nye er, at den dataansvarlige fremover skal kunne *påvise*, det vil sige dokumentere at det sker, imod tidligere at skulle *sikre*.

1.2.1. Medlemsoplysninger

Brancheforeningen ICF Danmarks tjenester kræver registrering af personlige oplysninger. Medlemmer kan besøge foreningens webside og hente information centralt på ICF Danmarks webside uden aktivt at opgive identitet. Foreningen benytter dog cookies på hjemmesiden, hvilket vil sige, at IP-adressen registreres.

Foreningens registrering af oplysninger om medlemmerne omfatter almindelige oplysninger som indmeldelsesdato, id-oplysninger, evt. tillidshvervsposter m.m. Brancheforening vil som udgangspunkt også kunne registrere oplysninger af mere speciel karakter, f.eks. oplysninger om et medlems udmærkelser, certificerings niveau m.m.

Ved registrering som medlem af foreningen udsendes en persondatameddelelse til medlemmet, som opfylder forordningens krav til oplysningspligten.

1.2.2. Kundeoplysninger

Brancheforeningen ICF Danmark anbefaler, at medlemmernes egen registrering af oplysninger om kunder begrænser sig til almindelige personoplysninger som opstartsdato og kontaktoplysninger.

Coachen vil også kunne registrere oplysninger af mere speciel og personfølsom karakter, men medmindre registrering af personfølsomme oplysninger har et klart formål, anbefaler ICF Danmark af hensyn til den registreredes rettigheder og coachens forpligtigelse til at kunne påvise nødvendigheden, at der konsekvent registreres et minimum af oplysninger, herunder kontaktoplysninger og tidspunkt for coaching.

1.2.3. Sikkerhed

Brug og håndtering af personoplysninger skal foregå betryggende og med et passende niveau af sikkerhed og privatlivsbeskyttelse. Sikkerhedsniveauet¹ skal afspejle den konkrete risiko for, at oplysningerne stjæles, mistes, skades, eller behandles ulovligt.

Virksomheder skal foretage en konsekvensanalyse forud for databehandlinger, som sandsynligvis vil indebære en høj risiko.

ICF Danmark vurderer, at karakteren af databehandlingen, som finder sted i regi af brancheforeningen og medlemmernes coachingvirksomhed under normale omstændigheder ikke indebærer en høj risiko.

¹ For nærmere oplysninger om reglerne om persondatasikkerhed mv. henvises til Datatilsynets hjemmeside og de vejledninger, der vil blive udarbejdet om disse emner. Ved tvivl kan man endvidere altid rette henvendelse til Datatilsynet.

2.0. Procedure for registrering og oplysningspligt

De registreredes vigtigste rettigheder efter persondataforordningen er:

- Retten til at modtage oplysning om behandling af sine personoplysninger (oplysningspligt)
- Retten til at få indsigt i sine personoplysninger – gratis
- Retten til at få eventuelt urigtige personoplysninger berigtiget
- Retten til at få sine personoplysninger slettet
- Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
- Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering
- Retten til at flytte sine personoplysninger (dataportabilitet).

Medlemmerne har pligt til at oplyse de registrerede om deres rettigheder og skal være rede til at håndtere de registreredes krav om for eksempel at blive slettet fra kartoteket.

Den enkelte virksomhed, som er medlem af foreningen, har selv dataansvaret overfor sine kunder. ICF Danmark deler ikke et ansvar over for det enkelte medlems kunder.

2.1. Persondatameddelelse

Den enkelte coach, som kunden henvender sig til, er dataansvarlig. Det enkelte medlem af ICF Danmark, som driver coaching virksomhed, har en oplysningspligt over for den enkelte kunde (den registrerede). Den såkaldte persondatameddelelse oplyser den registrerede om, at der indsamles oplysninger om vedkommende.

Brancheforeningen ICF Danmark fremsender persondatameddelelsen til medlemmer ved registrering og anbefaler medlemmerne at sende en **konkret** og **tilpasset** persondatameddelelse til deres egne kunder i forbindelse med registrering. Det er vigtigt, at meddelelsen indeholder oplysning om **medlemmets** behandling af kundens personoplysninger.

Persondatameddelelsen fra den dataansvarlige skal bl.a. indeholde oplysning om:

- Hvem den dataansvarlige er (foreningens eller virksomhedens navn og adresse),
- Formålet med indsamlingen, registreringen m.v. (f.eks. at kunne etablere coachingaftale, fakturere for ydelser, tilbyde den registrerede nyheder eller tilbud fremover),
- Kategorier af modtagere, hvis oplysningerne skal videregives (dvs. dem der regelmæssigt sker videregivelse til),
- Retsgrundlaget for behandlingen (fx samtykke eller kontrakt),
- Videregivelse af personoplysninger,
- Hvor længe oplysningerne opbevares,
- Den registreredes rettigheder (indsigt, sletning, ændring af personoplysning),
- Tilbagetrækning af samtykke (hvis hjemlen er samtykke),

- Muligheden for at klage til tilsynsmyndigheden (som i Danmark er Datatilsynet), såfremt den registrerede mener, at du behandler oplysningerne i strid med persondataforordningen, og
- Retten til at ændre i persondatameddelelsen

Den registrerede skal modtage disse oplysninger snarest muligt og senest inden for 10 dage efter, at behandlingen af personoplysningerne påbegyndes.

Se ICF Danmarks **Persondatameddelelse i BILAG 1**.

3.0. Modtager af personoplysninger

Ansvar for at personoplysninger om medlemmer eller kunder ikke kommer til uvedkommendes kendskab ligger hos den dataansvarlige. Den dataansvarlige har det overordnede ansvar, også for behandling af data, som foretages af tredjepart på vegne af den dataansvarlige.

ICF Danmark er dataansvarlig for de oplysninger, ICF Danmark behandler om medlemmerne af foreningen.

De enkelte medlemmer er dataansvarlig for de oplysninger, medlemmerne behandler om de kunder, som de indgår aftale med.

3.1. Videregivelse og overladelse af medlemsoplysninger

For så vidt angår videregivelse af medlemsoplysninger skelner ICF Danmark mellem to situationer:

- Videregivelse af deltagerlister til medlemmer i forbindelse med deltagelse i interne arrangementer – som for eksempel medlemsmøde – kan som udgangspunkt ske uden det enkelte medlems samtykke under forudsætning af, at oplysningerne kun videredistribueres til medlemmer
- Videregivelse i form af offentliggørelse på det åbne internet – dette kræver det enkelte medlems samtykke

Medlemskab af en forening er en privat sag, og der vil være en risiko for, at medlemsoplysningerne kan blive brugt til uvedkommende formål, f.eks. markedsføring. Offentliggørelse af en oplysning om persons medlemskab kræver derfor det enkelte medlems samtykke.

Lukkede sider på internettet ligestilles med et foreningsblad m.v. under forudsætning af, at det for eksempel ved hjælp af password eller lignende sikres, at kun medlemmer har adgang til den pågældende side.

3.2. Videregivelse og overladelse af kundeoplysninger

At følge et coachingforløb er en privat sag, og offentliggørelse af oplysninger om kunderelationer kræver den enkelte kundes samtykke.

Videregivelse af personoplysninger om kunder til en 3. part kræver, at coachen oplyser kunden om at oplysninger videregives. Det kræver ikke kundens skriftlige samtykke. Når coachen for eksempel løbende skal dokumentere antal timer i sin coachingpraksis over for ICFs globale hovedorganisation for at opretholde sin ICF-certificering, skal den enkelte kunde *oplyses* om videregivelsen.

Det er således tilstrækkeligt, at den enkelte coach beskriver forholdet omkring videregivelsen af personoplysninger (navn, mail og telefonnummer). Dette gøres mest effektivt via coachens generelle persondatameddelelse til kunden.

Alternativt kan det gøres i forbindelse med den første coaching session, hvor coachen introducerer den registrerede til ICFs etiske standarder m.v. Her anbefaler brancheforeningen, at coachen oplyser det i persondatameddelelsen for at kunne dokumentere at der er oplyst derom.

Til gengæld er det nødvendigt at indhente samtykke fra de medlemmer, som der fremsendes markedsføringsmateriale til.

Et samtykke behøver ikke nødvendigvis være skriftligt, men da coachen som dataansvarlig skal kunne dokumentere et samtykke, benytter ICF Danmark en skriftlig samtykkeerklæring.

Ved behov for overførsel af personoplysninger lande uden for EU, dvs. såkaldte tredjelande, henvises til forordningens kapitel 5.

4. Brud på persondatasikkerheden

I databeskyttelsesforordningen defineres et brud på persondatasikkerheden således:

“Et brud på sikkerheden, der fører til hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger der er transmitteret, opbevaret eller anden på anden måde behandlet”

Som eksempler på brud på persondatasikkerheden kan nævnes:

1. Andre personer end de personer hos dataansvarlige, der er autoriseret til det, får (uautoriseret) adgang til personoplysninger
2. Den dataansvarliges medarbejdere ændrer eller sletter personoplysninger ved et uheld
3. Brud på den dataansvarliges server, hvor uvedkommende får indsigt i personoplysninger
4. Den dataansvarliges medarbejdere videregiver bevidst eller ubevidst personoplysninger om en kunde til en anden kunde – eller til andre uvedkommende personer
5. Når manglede kryptering af den dataansvarliges hjemmeside resulterer i, at en eller flere uvedkommende får direkte adgang til kundens personoplysninger.

De fleste brud på persondatasikkerheden sker ved uagtsom håndtering af papir.

4.1. Indberetning af datasikkerhedsbrud

Ved brud på persondatasikkerheden er den dataansvarlige forpligtet til at indberette bruddet inden for 72 timer. Indberetningen skal ske til Datatilsynet, og den forurettede skal samtidig informeres om bruddet.

Som udgangspunkt skal alle brud på persondatasikkerheden anmeldes til Datatilsynet. Der skal dog ikke ske anmeldelse, hvis det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.

Indtil Datatilsynets fælles digitale indberetningsløsning er klar og tilgængelig på virk.dk fra den 25. maj 2018 vil det være muligt at finde et link til den digitale indberetningsløsning via Datatilsynets hjemmeside: www.datatilsynet.dk.²

² Datatilsynets vejledning om brud på persondatasikkerheden kan læses i sin fulde længde via dette link: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/Vejledning_sikkerhedsbrud.pdf