

Den 21.05.2018

Behandling af personoplysninger

i virksomheden Klassisk Kinesisk Medicin"



© **Olejann Malchau**

Udarbejdet på baggrund af skriftligt materiale vedrørende Persondataforordningen, samt efter seminar forestået af Thorsten Kranz fra advokatfirmaet Bech-Bruun.

Stilles til rådighed for medlemmerne i RABforum og SundhedsRådet.

Uden ansvar.

Indholdsfortegnelse

1. Lovgivningens rammer - teori

1.1 Baggrund	side 5
1.1.1 Persondataforordning.....	side 5
1.1.2 Tilsluttende dansk lovgivning.....	side 5
1.2 Krav	side 5
1.3 Ansvar	side 5
1.3.1 Ansvar for data.....	side 5
1.3.2 Ansvar for databehandlingen.....	side 5
1.3.3 Samtykkeerklæring.....	side 5
1.4 Videregivelse	side 6
1.4.1 Aftale om databehandlingen.....	side 6
1.4.2 Lovreguleret videregivelse.....	side 6
1.4.3 Back-up og "cloud".....	side 6
1.5 Opbevaring af personlige oplysninger	side 6
1.6 Dokumentationskrav	side 6
1.6.1 Behandlingen af personoplysninger skal dokumenteres.....	side 6
1.6.2 Risikoanalyse.....	side 6

2. Sådan gør vi – praksis i/hos "Klassisk Kinesisk Medicin"

2.1 Behandling af personoplysninger	side 7
2.1.1 Typer af personoplysninger.....	side 7
2.1.2 Samtykkeerklæring.....	side 7
2.2 Ansvar for personoplysningerne	side 7
2.2.1 Dataansvarlig.....	side 8
2.2.2 Databehandler.....	side 7
2.3 Videregivelse af personoplysninger	side 7
2.4 Opbevaring af personoplysninger	side 7
2.5 Dokumentation	side 8
2.5.1 Den dataansvarlige.....	side 8
2.5.2 Databehandleren.....	side 8
2.5.3 Formålet med behandlingen af personoplysninger.....	side 8
2.5.4 Beskrivelse af kategorier af anvendte personoplysninger.....	side 8
2.5.5 Tidsfrister for sletning.....	side 8
2.5.6 Tekniske og organisatoriske sikkerhedsforanstaltninger.....	side 8
Samtykkeerklæring	side 9
Krav til Databehandleraftale	side 10

1. Lovgivningens rammer - teorien

Fortalen til **Jyske Lov** fra år 1241, som kong Valdemar gav, og Danerne vedtog, lyder således: "*Med lov skal land bygges*".

Og denne sætning gælder fortsat, således at vi som borgere i Danmark, har pligt til at følge landets lovgivning. Derfor skal personlige oplysninger behandles og anvendes på en lovlig, rimelig og gennemsigtig måde.

1.1 Baggrund

Baggrunden for dette resume af lovgivningens rammer for behandling af personoplysninger tager udgangspunkt i

- EU's Persondataforordning (GDPR)
- Tilsluttende dansk lovgivning.

Formålet med lovgivningen er at sikre samtlige borgere i såvel EU som i Danmark en privatlivsbeskyttelse, således at der sikres arbejdsgange, der beskytter oplysningerne om den enkelte person.

1.2 Krav til behandling af personoplysninger

Forudsætningen for indhentning og opbevaring af personoplysninger er, at

- de er nødvendige
- de er rigtige og ajourførte
- de er tilgængelige for den person, de vedrører
- de kan slettes
- der foreligger en samtykkeerklæring, kontrakt eller juridisk forpligtigelse.

Enhver håndtering af personlige oplysninger er *behandling*.

Der er to typer af personoplysninger, som angivet i eksemplerne nedenfor:

Almindelige oplysninger	Følsomme oplysninger
Navn	Helbredsmæssige eller seksuelle forhold
Adresse	Fagforeningsoplysninger
Telefonnummer	CPR nr. (DK)
Fødselsdato	Politisk/religiøs overbevisning
e-mailadresse	Genetiske eller biometriske data
Familieforhold	
Sociale problemer	
Stilling	

For at sikre, at en person ved, at behandleren opbevarer personlige data om den pågældende, skal der foreligge en *samtykkeerklæring* vedrørende den konkrete behandling. Denne kan ifølge dansk lovgivning være enten mundtlig eller skriftlig.

Afgivelse af en samtykkeerklæring skal være *frivillig* (uden pres eller tvang), *specifik* (knyttet til en konkret anvendelse) og *informeret* (hvad samtykket gives til) og i særlige tilfælde *utvetydigt*.

Formålet er at sikre, at de oplysninger, den dataansvarlige ønsker at få oplyst, kun er *de nødvendige*, at den dataansvarlige ved, at der er *forskel på anvendelsen af oplysningerne* og at den dataansvarlige ved, at "ejeren" til konkrete personoplysninger alene er den person, som oplysningerne vedrører.

1.3 Ansvar

Der skelnes i Persondataforordningen imellem i hvert fald disse følgende hovedtyper af interessenter

- den dataansvarlige
 - databehandleren, og
-

- tredjemand

Alle udover den dataansvarlige og databehandleren er tredjemand.

Databehandleren er en fysisk eller juridisk person, der behandler personoplysninger på den dataansvarliges vegne. Der må udelukkende anvendes databehandlere, som kan stille garantier i form af ekspertise, pålidelighed og ressourcer.

Man kan outsource opgaven, men ikke ansvaret. Derfor skal der være en skriftlig databehandleraftale imellem den dataansvarlige og databehandleren.

Formålet er at fastlægge ansvaret for håndteringen af personlige oplysninger, således at den *dataansvarlige* er den, der indsamler og bruger de personlige data og *databehandleren*, der både kan være den dataansvarlige selv, eller f.eks. en ekstern udbyder af bookingsystemer, systemer til journalføring eller udbydere af hjemmesider o.l.

1.4 Videregivelse af data

1.4.1 aftale om databehandling

Videregivelsen skal principielt

- være i en legitim ("berettiget") interesse
- være baseret på en skriftlig aftale om ansvarsfordeling mm.
- udvise varsomhed i forbindelse med sociale medier
- være godkendt i en samtykkeerklæring

1.4.2 lovreguleret videregivelse

For lovgivningsmæssige krav om videregivelse af personlige oplysninger, kan der foreligge andre krav.

1.4.3 Back-up og "cloud"

Her skal udbyderen dokumentere en sikker adgang og opbevaring.

Formålet er at sikre, at personlige data ikke "slippes fri" eller "lækkes" overfor tredjemand.

1.5 Opbevaring af personlige oplysninger

Der stilles krav til opbevaring af personlige oplysninger, såvel vedrørende

- en fysisk opbevaring, som
- en elektronisk opbevaring

Formålet er, som nævnt under 1.1 at sikre en privatlivsbeskyttelse. Opbevaringen skal beskrives, jf. punkt 1.6.

1.6 Dokumentationskrav

Den dataansvarlige er ansvarlig for *og skal kunne påvise*, at principperne for behandlingen af personoplysninger overholdes. Der er bl.a. følgende krav til dokumentationen, der skal foreligge skriftligt

- Navn og kontaklinformation på den dataansvarlige
- Formål med anvendelsen af personlige oplysninger
- Beskrivelse af kategorier af personoplysninger
- Evt. en generel angivelse af tidsfrister for sletning
- En beskrivelse af tekniske og organisatoriske sikkerhedsforanstaltninger (risikovurdering)

Formålet er at kunne bevise at virksomheden har forstået og lever op til de retslige forpligtigelser, der er gældende i forbindelse med behandlingen af personoplysninger og at dette kan dokumenteres overfor myndighederne.

2. Sådan gør vi – praksis i "Klassisk Kinesisk Medicin"

2.1 Behandlingen af personoplysninger

Den registrerede har altid ret til indsigt i egne data.

2.1.1 Typer af personoplysninger

I virksomheden Klassisk Kinesisk Medicin indhentes de nødvendige personlige oplysninger til at kunne identificere personen og til at kunne stille en diagnose forud for iværksættelse af en behandling.

2.1.2 Samtykkeerklæring

Der indhentes *altid* en skriftlig samtykkeerklæring. Samtykkeerklæringen findes som bilag 1.

Behandlingen af "*Almindelige personoplysninger*" kræver informeret samtykke ("*mundtligt eller skriftligt indforstået*"), mens behandlingen af "*Følsomme personoplysninger*" kræver et udtrykkeligt samtykke ("*frivilligt, specifikt og informeret viljestilkendegivelse*"). "*Stiltiende*" eller "*indirekte*" samtykke er ikke gældende.

Personen har ret til at trække sit samtykke tilbage. I så fald slettes eller anonymiseres personens data.

2.2 Ansvar

2.2.1 Dataansvarlig

Den *dataansvarlige* er klinikens indehaver.

2.2.2 Databehandler

Mette Heinz

2.3 Videregivelse af personlige oplysninger

Personlige oplysninger videregives aldrig til 3. part, uden kundens udtrykkelige skriftlige samtykke, medmindre særlovgivning siger noget andet.

Personen har ret til at få udleveret de oplysninger, som personen selv har tilvejebragt, eller at få dem videresendt til en anden dataansvarlig i et almindeligt anvendt og maskinlæsbart format.

2.4 Opbevaring af personlige oplysninger

Alle personlige oplysninger opbevares i et aflåst stålskab i klinikken.

2.5 Dokumentation

2.5.1 Den dataansvarlige

Virksomheden er Klassisk Kinesisk Medicin. CVR nr. 36 78 24 63.

Den dataansvarlige er:

Mette Heinz

Kastagervej 5

2730 Herlev

Telefonnr. 53544229

Email: metteheinz@outlook.com

2.5.2 Databehandleren

Databehandleren er:

Mette Heinz

Kastagervej 5

2730 Herlev

Telefonnr. 53544229

Email: metteheinz@outlook.com

2.5.3 Formålet med behandlingen af personlige oplysninger

Formålet er – ud fra kundens egne helbredsoplysninger og andre konkrete personoplysninger - at kunne identificere, diagnosticere og behandle kunden med akupunktur, tuina massage og kinesisk urte terapi mm. samt at kunne dokumentere den gennemførte behandling.

2.5.4 Beskrivelse af kategorier af anvendte personoplysninger

Følgende personlige oplysninger efterspørges:

Almindelige oplysninger	Følsomme oplysninger
Navn Stilling/arbejdsvilkår Adresse Telefonnummer e-mailadresse	Årsag til henvendelse Medlemskab af sygeforsikringen CPR nr.

2.5.5 Tidsfrister for sletning

Oplysninger, hvor sidste aktive dato er mere end fem år gammel, destrueres på betryggende måde.

Er der forskningsmæssige hensyn, hvor oplysningerne indgår i anonymiseret form, eller er der verserende sager af juridisk karakter, kan oplysningerne opbevares i længere tid.

2.5.6 Tekniske og organisatoriske sikkerhedsforanstaltninger (risikovurdering)

Sikkerhedsforanstaltning	Risikovurdering ^{*)}
Adgangsforhold: via aflåst dør	lav
Opbevaring: patient papirnoter opbevares i aflåst metal arkiv i klinik.	lav
Sikret datalinje (udbyder forsikrer firewall)	middel
Svar på henvendelser pr. e-mail og aftaler om konsultation	middel
Korrespondance på "nettet" – der er password til pc'er og telefon	middel
Kommunikation med databehandler (ikke relevant)	

^{*)} Risikovurderingen kan være Lav, Middel eller Høj

Ved brud på sikkerheden anmeldes dette til Datatilsynet senest 72 timer efter bruddet.

Her oplyses det, hvad konsekvenserne af sikkerhedsbruddet er samt oplyses, hvad der er gjort for at stoppe sikkerhedsbruddet, og – hvor det er muligt – underrettes de berørte personer.

---ooOoo---

Bilag 1, samtykkeerklæring

Samtykkeerklæring

Undertegnede

Navn _____

Adresse _____

Postnr. _____ By _____

Telefon _____

Email _____

giver hermed mit udtrykkelige samtykke til, at:
Klassisk Kinesisk Medicin
Mette Heinz
Kastagervej 5
2730 Herlev

opbevarer *nødvendige* personlige oplysninger om mig, for at jeg kan modtage den behandling, som diagnosticeres til at være nødvendig i forbindelse med min henvendelse.

Jeg bekræfter samtidig, at jeg er blevet informeret om, at

- samtykkeerklæringen kun er gyldig, fordi jeg har afgivet den *frivilligt*
- oplysningerne *udelukkende anvendes i forbindelse med det, min henvendelse vedrører*
- oplysningerne udelukkende anvendes *i forbindelse med den behandling, der iværksættes*
- jeg til enhver tid har *ret til indsigt* i de opbevarede oplysninger
- mine personlige oplysninger *slettes senest 5 år efter sidste anvendelse*
- *jeg kan tilbagekalde samtykkeerklæringen* og at mine personlige oplysninger derefter slettes eller anonymiseres.

Herlev den _____

Underskrift

Bilag 2, indhold i databehandleraftalen

Følgende specifikke krav gælder til en databehandler aftale:

- databehandleren må kun behandle personoplysninger, efter en dokumenteret instruks fra den *dataansvarlige*
- den *dataansvarlige* skal sikre, at databehandlerens medarbejdere er underlagt fortrolighed/tavshedspligt
- databehandleren skal have passende tekniske og organisatoriske sikkerhedsforanstaltninger
- databehandleren skal indhente godkendelse fra den *dataansvarlige* ved brug af underdatabehandlere
- databehandleren skal bistå den *dataansvarlige* i forhold til bl.a. at
 - a. sikre de registreredes rettigheder
 - b. sikre overholdelse af kravene til dataenes behandlingssikkerhed, notifikation og konsekvensanalyse
- databehandleren skal slette eller tilbagelevere personoplysninger ved aftalens ophør
- databehandleren stiller oplysninger/dokumentation til rådighed for den *dataansvarlige* og bidrager til revision og inspektioner

Det er den *dataansvarlige*, der skriftligt skal definere, hvilke personlige oplysninger, der overlades til databehandleren.

De øvrige punkter er de krav, som den *dataansvarlige* stiller til, at databehandleren beskriver og leverer skriftligt.

Typen af personoplysninger der behandles (forslag til indhold):

Behandlingerne indeholder personoplysninger i de nedenfor afkrydsede kategorier. Leverandørens og eventuelle underdatabehandlers niveau for behandlingssikkerhed bør afspejle oplysningernes følsomhed.

Almindelige personoplysninger (jf. Databeskyttelsesforordningens artikel 6)

Almindelige personoplysninger

Følsomme personoplysninger (jf. Databeskyttelsesforordningens artikel 9):

- Racemæssig eller etnisk baggrund
- Politisk overbevisning
- Religiøs overbevisning
- Filosofisk overbevisning
- Fagforeningsmæssige tilhørsforhold
- Helbredsforhold, herunder misbrug af medicin, narkotika, alkohol m.v.
- Seksuelle forhold

Oplysninger om enkeltpersoners rent private forhold (jf. Databeskyttelsesforordningens artikel 6 og 9):

- Strafbare forhold
- Væsentlige sociale problemer
- Andre rent private forhold, som ikke er nævnt ovenfor:

Oplysninger om CPR-nummer (jf. Databeskyttelsesforordningens artikel 87)

CPR-numre
