Hypnoseguiden

Merethe S. Erbs, Mich. Berings Vang 8, 2-2, 2650 Hvidovre ☎ +45 2685 8578 kontakt@hypnoseguiden.dk

Den 27.05.2018

Behandling af personoplysninger

i virksomheden Hypnoseguiden v/Merethe S. Erbs CVR-nr. 32 03 93 24

Indholdsfortegnelse

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 Adresse Telefonnummer Fødselsdato e-mailadresse Familieforhold Sociale problemer Stilling	Helbredsmæssige eller seksuelle forhold Fagforeningsoplysninger CPR nr. (DK) Politisk/religiøs overbevisning Genestiske eller biomestriske data

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 kontaktinformation 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.

---ooOoo---

2. Sådan gør jeg – praksis hos Hypnoseguiden

2.1 Behandlingen af personoplysninger

Den registrerede har altid ret til indsigt i egne data.

2.1.1 Typer af personoplysninger

I virksomheden Hypnoseguiden 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 klinikkens indehaver.

2.2.2 Databehandler

Databehandling af personfølsomme oplysninger gennem hele behandlingskæden foretages af klinikkens indehaver.

Hjemmeside, webmail og mailadresse-kartotek til udsendelse af nyhedsbreve er hos One.com

Der foreligger en skriftlig databehandleraftale imellem klinikkens indehaver og One.com. Aftalen med udbydervirksomheden findes som bilag 2.

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

Der tages noter ifb. med konsultationer i klinikken. Noterne opbevares i et aflåst metalskab i klinikken. Samtykkeerklæringen opbevares i en mappe i et skab. Der er ikke navn på noterne, men en kode, der er registreret i en bog, som ligger i et andet skab. Koden findes kun i bogen og på noterne og navnet findes kun i bogen og på samtykkeerklæringen. Dvs. får at kunne finde ejeren af noterne skal man både have noterne, bogen og samtykkeerklæringen, som befinder sig 3 forskellige steder i klinikken i indehaverens hjem.

2.5 Dokumentation

2.5.1 Den dataansvarlige

Hypnoseguiden v/Merethe S. Erbs, CVR nr. 32 03 93 24.

Den dataansvarlige er:

Hypnoseguiden v/Merethe S. Erbs
Mich. Berings Vang 8, 2-2
2650 Hvidovre
Mobil: +45 2685 8578

Mail: kontakt@hypnoseguiden.dk

2.5.2 Databehandleren
Databehandlere er:

Hypnoseguiden v/Merethe S. Erbs
&
One.com Cvr. Nr. 28 67 71 38
Kalvebod Brygge 24
1560 København V
Tlf.: +45 7020 5872
Mail: support@dk.one.com

2.5.3 Formålet med behandlingen af personlige oplysninger
Formålet er – ud fra kundens egne oplysninger og andre konkrete personoplysninger - at kunne identificere, diagnosticere og behandle kunden med hypnosepsykoterapi mm. og kunne dokumentere den gennemførte behandling.

2.5.4 Beskrivelse af kategorier af anvendte personoplysninger
Følgende personlige oplysninger efterspørges:

Almindelige oplysninger	**Følsomme oplysninger**
Navn Adresse Telefonnummer e-mailadresse	Journaloptegnelser: Jeg tager noter ifb. med konsultationer bl.a. årsag til henvendelse

2.5.5 Tidsfrister for sletning
Personfølsomme oplysninger, hvor sidste aktive dato er mere end 2 år gammel, destrueres på betryggende måde.

Almindelige oplysninger, der er anvendt til fakturering af ydelser destrueres efter 5 år i henhold til bogføringsloven.

Navn og e-mailadresse, som opbevares hos One.com, der er afgivet i forbindelse med ønsket om at modtage nyhedsbreve bliver gemt så længe der ikke er trukket et afgivet samtykke tilbage. Samtykket kan altid trækkes tilbage ved at sende mig en e-mail med "afmeld" i emnerubrikken.

Er der verserende sager af juridisk karakter, kan oplysningerne opbevares i længere tid.

2.5.6 Tekniske og organisatoriske sikkerhedsforanstaltninger (risikovurdering)

Sikkerhedsforanstaltning	**Risikovurdering**[*)]
Opbevaring: Metalskab og 2 forskellige skabe. Oplysningerne er fordelt 3 steder.	Lav
Svar på henvendelser pr. e-mail og aftaler om konsultation: PC har kode, antivirus, firewall og antimalware programmer. Mails slettes løbende, så der ikke ligger for mange. Mails med personfølsomme oplysninger slettes med det samme.	måske middel

[*)] 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

Navn: _____

Adresse: _____ Tlf.: _____

Postnr: _____ By: _____

E-mailadresse: _____

Hvordan fandt du frem til mig? anbefaling: ____ annonce: ____ internet: ____

Andet/uddyb: _____

Må jeg evt. kontakte dig 3-4 uger efter sidste behandling for at høre hvordan det går?
Ja: __ Nej: __

Er du interesseret i at modtage informationer om nye tiltag, tilbud og lign. på mail?
Ja: _____ Nej: _____

Jeg tager noter til brug for min behandling af dig i klinikken. Det er kun mig, der ser oplysningerne, jeg har tavshedspligt og jeg opbevarer dine data på følgende måde:

Mine noter opbevares i aflåst metalskab. Der er ikke navn på noterne, men en kode, der er registreret i en bog, som ligger i et andet skab. Koden findes kun i bogen og på noterne og dit navn findes kun i bogen og på samtykkeerklæringen. Samtykkeerklæringen opbevares i en mappe i et skab. Dit navn og adresse anvendes til fakturering i mit regnskab til Skat. Fakturaerne gemmes på min computers harddisk og på en ekstern harddisk (backup). Jeg anvender udelukkende de indsamlede oplysninger til din behandling. Hvis du ikke har været hos mig i 2 år, makuleres noterne, mens dit navn og adresse slettes efter 5 år i henhold til bogføringsloven.

Du har ret til indsigt i de indsamlede data og har ret til at bede om sletning og kan trække dit samtykke tilbage.

Behandling i klinikken kan ikke stå i stedet for lægelig behandling og du har pligt til at afgive korrekte informationer om sygdomme, medicinforbrug, graviditet mv. i forbindelse med behandling i klinikken.

Jeg skriver hermed under på, at jeg har læst ovenstående og giver hermed samtykke til indsamling og opbevaring af data

Dato og underskrift

_____ _____

Hypnoseguiden v/Merethe S. Erbs – Mich. Berings Vang 8, 2. th., 2650 Hvidovre - tlf. 2685 8578

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 underdatabehandleres 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*