

Graafland | Behandling af personoplysninger

Graafland behandling af persondata: den forenklede version:

Her får du den korte version af, hvad du i praksis kan forvente vedr. behandling af persondata hos Graafland:

Ved indledende kontakt/ første session besvarer du dels en klientformular med relevante baggrundsoplysninger, som er nødvendige for at du kan modtage en sikker, sammenhængende og individuel behandling hos Graafland. Desuden udfyldes en samtykkeerklæring med dine oplysninger: (navn/ fødselsdato/ kontaktdata), hvor du underskriver vedr. vilkår for persondata (jfl. GDPR), samt vilkår for behandling i øvrigt.

Jeg udfører løbende journal over sessioner, så min behandling af dig i klinikken og dit forløb hos mig bliver så kvalitativt og sammenhængende som muligt. Det er kun mig, der ser oplysningerne, og jeg har tavshedspligt.

Jeg opbevarer data på følgende måde:

Identifikationsoplysninger/ samtykkeerklæring opbevares separat, i aflåst arkiv i aflåst stålskab i klinikken, adskilt fra følsomme oplysninger.

Personfølsomme oplysninger/ Klientformular og Journaloptegnelser: Fysisk data opbevares i aflåst arkiv i aflåst stålskab i klinikken, adskilt fra identifikationsoplysninger.

Digital data opbevares sikkert på kodet USB-stick på separat lokation. Digital back-up opbevares på kodet USB-stick i aflåst pengeskab på separat lokation.

Jeg kommunikerer med dig via SSL krypteret mailsystem. Jeg har tavshedspligt og anvender udelukkende de indsamlede oplysninger til behandlingen. Hvis du ikke har været hos mig i 5 år, slettes/ destrueres/ anonymiseres de indsamlede informationer.

Jeg samarbejder med Optimeo, som står for hjemmesiden og mailboksen. Optimeo har ligeledes dokumenterede sikkerhedsforanstaltninger for at beskytte dine data.

Personlige oplysninger videregives ikke.

Ved referenceudtalelser til brug på hjemmeside/ Facebook-side indhentes udtrykkelig tilladelse og evt. ønsket anonymitet garanteres.

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

Se mere/ mere detaljerede informationer på de følgende sider/ Graafland persondatabehandling.

© **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 hos Graafland

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

Forklaring på begreberne: (se de officielle definitioner nedenfor):

Dataansvarlig: den, der modtager de personlige oplysninger fra en klient/kunde og som har den personlige kontakt.

Databehandler: den, der behandler/ opbevarer/ har adgang til de personlige oplysninger.

Det er *altid* den dataansvarlige, der har det juridiske ansvar overfor den person, hvis data man modtager.

De officielle GDPR definitioner:

Dataansvarlig: "En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger; hvis formålene og hjælpemidlerne til en sådan behandling fastsat i EU-retten eller medlemsstaternes nationale ret, kan den dataansvarlige eller de specifikke kriterier for udpegelse af denne fastsættes i EU-retten eller medlemsstaternes nationale ret."

Databehandler: "En fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne."

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	Helbredsmaessige 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 *forskul på anvendelsen af oplysningerne* og at den dataansvarlige ved, at "ejereren" 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 databehandlersaftale 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 forpligtigelse, der er gældende i forbindelse med behandlingen af personoplysninger og at dette kan dokumenteres overfor myndighederne.

2. Sådan gør vi – praksis i Graafland

2.1 Behandlingen af personoplysninger

Den registrerede har altid ret til indsigt i egne data.

2.1.1 Typer af personoplysninger

I **Graafland** indhentes ifbm. indledende kontakt/ første session via en klientformular de nødvendige personlige oplysninger til at identificere personen og til at jeg kan udføre en sammenhængende og individuel behandling.

2.1.2 Samtykkeerklæring

Der indhentes *altid* en skriftlig samtykkeerklæring med identifikationsdata. Denne findes vedlagt 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

Klinikken er en enkeltmandsvirksomhed, der anvender virksomheden Optimeo, som udbyder Wordpress system til hjemmeside hosting og kontaktformular fra hjemmeside til behandler.

Der foreligger en skriftlig aftale imellem den dataansvarlige og udbydervirksomheden, hvoraf opbevaringsfrister mm. fremgår. Aftalen med udbydervirksomheden findes vedlagt som bilag 2.

2.3 Videregivelse af personlige oplysninger

Personlige oplysninger videregives ikke.

Ved referenceudtalelser til brug på hjemmeside/ Facebook-side indhentes udtrykkelig tilladelse og evt. ønsket anonymitet garanteres.

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

Identifikationsoplysninger opbevares aflåst og adskilt fra personfølsomme oplysninger:

Identifikationsoplysninger/ samtykkeerklæring opbevares separat, i aflåst arkiv i aflåst stålskab i klinikken, adskilt fra følsomme oplysninger.

Personfølsomme oplysninger/ Klientformular og Journaloptegnelser: Fysisk data opbevares i aflåst arkiv i aflåst stålskab i klinikken, adskilt fra identifikationsoplysninger.

Digital data opbevares sikkert på kodet USB-stick på separat lokation. Digital back-up opbevares på kodet USB-stick i aflåst pengeskab på separat lokation.

Klinikken er en enkeltmandsvirksomhed, der anvender virksomheden Optimeo, som udbyder Wordpress system til Graafland hjemmeside hosting, mailboks samt kontaktformular fra hjemmeside til behandler. Der foreligger en skriftlig aftale imellem den dataansvarlige og udbydervirksomheden, hvoraf opbevaringsfrister mm. fremgår. Aftalen med udbydervirksomheden findes som bilag 2.

2.5 Dokumentation

2.5.1 Den dataansvarlige

Virksomheden er Graafland, CVR nr. 3257 3738

Den dataansvarlige er:

Ghita Lauth Graafland, Svenstrupvej 113, 4400 Kalundborg
+45 4128 4528 - info@graafland.dk

2.5.2 Databehandleren

Databehandleren er: Optimeo ApS, CVR nr: 3548 1605

Robert Jacobsens vej 60, 2.sal, 2300 Kbh S
+45 7199 0889 - INFO@OPTIMEO.DK

2.5.3 Formålet med behandlingen af personlige oplysninger

Formålet er – ud fra kundens egne personlige oplysninger og andre konkrete personoplysninger - at kunne identificere, kommunikere med og behandle kunden sammenhængende og individuelt i forbindelse med Personlig udvikling og terapeutisk behandling via Coaching, Kognitiv terapi, NLP, Hypnoterapi og Mentaltræning 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 Adresse Fødselsdato Telefonnummer e-mailadresse	Årsag til henvendelse Relevante psykiske og fysiske helbredsforhold*

* Data, som håndteres af databehandleren, indeholder almindelige personoplysninger (navn/ telefon-nummer/ e-mail) samt årsag til henvendelse, herunder kun de følsomme personoplysninger, som evt. anses for relevante og valgfrit er oplyst af klienten selv i kontaktformular/ mail.

2.5.5 Tidsfrister for sletning

Oplysninger, hvor sidste aktive dato er mere end 5 år gammel, slettes/ 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 ¹⁾
Adgangsforhold: Klinik under opsyn eller aflåst.	lav
Opbevaring: Adskilte data i aflåst arkiv i aflåste stålskabe	lav
Sikret datalinje: Norton antivirus, firewall og malware beskyttelse	lav - middel
Svar på henvendelser pr. e-mail og aftaler om konsultation: Kodeord på programmer	lav - middel
Korrespondance på "nettet": Password til pc'er/ mobil samt anvendte programmer	lav - middel
Kommunikation med databehandler: Sikret linje (se bilag)	lav - middel

¹⁾ Risikovurderingen kan være Lav, Middel eller Høj

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

Det tilstræbes endvidere at underrette berørte personer hurtigst muligt.

Bilag 1, samtykkeerklæring

Graafland | samtykkeerklæring**Undertegnede:**

Navn:

(v. barn i behandling: forælder til/ værge for):

Adresse:

Post nr. / by:

Født dato:

Telefon/ mobil:

E-mail:

giver hermed mit udtrykkelige samtykke til, at

Graafland | bedre nu
v. Ghita Lauth Graafland
Svenstrupvej 4400 Kalundborg

opbevarer nødvendige personlige oplysninger om mig/ mit barn, for at jeg/ mit barn kan modtage en sammenhængende og individuel behandling 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/ destrueres/ anonymiseres senest 5 år efter sidste anvendelse
- jeg kan tilbagekalde samtykkeerklæringen og at mine personlige oplysninger derefter slettes eller anonymiseres.

Vilkår i øvrigt:

Jeg indestår for, at behandling hos certificeret og godkendt registreret behandler Ghita Graafland finder sted frivilligt og på eget ansvar, og at oplysninger afgivet i klientformular og samtykkeerklæring er rigtige.

Jeg er bekendt med og accepterer følgende vilkår for behandling:

- Afbud skal ske med min. 24 t. varsel, ellers betales fuld sessionspris.
- Klienter, der møder op påvirket af alkohol/ euforiserende stoffer afvises, og der betales fuld sessionspris.
- Jeg er blevet oplyst om, at der ved fysiske symptomer og diagnoser, herunder spiseforstyrrelser, er krav om sideløbende behandling/ tilsyn ved læge/ specialist, således at sessioner hos Registreret Behandler Ghita Graafland er komplementerende behandling i form af terapeutisk arbejde.

Dato/ underskrift:

Strandgården, d. _____

Bilag 2, indhold i databehandleraftalen

Følgende specifikke krav gælder til en databehandler aftale:

- databehandleren må kun behandle personoplysninger, efter 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:

Leverandørens og eventuelle underdatabehandlers niveau for behandlingssikkerhed afspejler oplysningernes følsomhed.

Data, som håndteres af databehandleren, indeholder almindelige personoplysninger (navn/ telefon-nummer/ e-mail) samt årsag til henvendelse, herunder kun de følsomme personoplysninger, som evt. af klienten selv anses for relevante og valgfrit er oplyst i kontaktformular/ mail.

Behandlingerne på klinikken kan evt. indeholde personoplysninger i de nedenfor afkrydsede kategorier. Data, som håndteres af databehandleren, kan dermed evt. afspejle dette.

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 evt. diagnoser og brug/ misbrug af medicin, narkotika, alkohol m.v.
- ☒ Psykiske forhold, herunder evt. psykiske diagnoser, medicinering m.v.

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:
Private forhold, som angår behandling og oplyses frivilligt i forbindelse hermed

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

☐ CPR-numre
