Sileo Idrætsmassage

Karina Rasmussen, Kildevangen 16, 4440 Mørkøv ☎ +45 28 10 33 84 sileo@outlook.dk

Den 27.05.2018

Behandling af personoplysninger

i virksomheden "Sileo Idrætsmassage" – CVR. 35980253

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

§§§

Hold fast i begreberne (se de officielle definitioner nedenfor):

Den data*<u>ansvarlige</u>*
- er den, der modtager de personlige oplysninger fra en kunde/klient og som har den personlige kontakt.

Data*<u>behandleren</u>*
- er den, der behandler/opbevarer/har adgang til de personlige oplysninger.

Det er *altid* den data*<u>ansvarlige</u>*, der har det juridiske ansvar overfor den person, hvis data man modtager.

§§§

De officielle GDPR definitioner:

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

Databehandler: *"En fysysk 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 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 forpligtigelse, der er gældende i forbindelse med behandlingen af personoplysninger og at dette kan dokumenteres overfor myndighederne.

---ooOoo---

2. Sådan gør vi – praksis i Sileo Idrætsmassage – CVR.35980253

2.1 Behandlingen af personoplysninger

Den registrerede har altid ret til indsigt i egne data.

2.1.1 Typer af personoplysninger

I virksomheden Sileo Idrætsmassage 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 eller digital 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

Klinikken er en enkeltmandsvirksomhed, der anvender virksomheden Mango Apps ApS(Terapeut Booking - https://terapeutbooking.dk) som udbyder elektronisk journal og faktureringssystem til behandling og arkivering af personoplysninger og bookingsystem til booking af tider i klinikken med tilhørende autogenereret bekræftelse til kunden. Databehandleren er derfor udbyderen, Mango Apps ApS.

Der foreligger en skriftlig databehandleraftale imellem den dataansvarlige og udbydervirksomheden. Aftalen med udbydervirksomheden findes som bilag 2.

2.3 Videregivelse af personlige oplysninger

Personlige oplysninger videregives aldrig til 3. part, uden kundens udtrykkelige skriftlige eller elektronisk 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

Klinikken er en enkeltmandsvirksomhed, der anvender virksomheden Mango Apps ApS(Terapeut Booking - https://terapeutbooking.dk) som udbyder elektronisk journal og faktureringssystem til behandling og arkivering af personoplysninger og bookingsystem.
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 "Sileo Idrætsmassage CVR nr. 35980253.

Den dataansvarlige er:

Sileo Idrætsmassage
Kildevangen 16
4440 Mørkøv
+45 28 10 33 84
Sileo@outlook.dk

2.5.2 Databehandleren
Databehandleren er:

Mango Apps ApS
Strandlodsvej 44, 3. sal
2300 København S
CVR: 35642536
Kontakt: kontakt@terapeutbooking.dk

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 manuel 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 CPR nr. (i få tilfælde) Helbredsoplysninger

2.5.5 Tidsfrister for sletning
Oplysninger, hvor sidste aktive dato er mere end 5 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 login	Lav
Opbevaring: Terapeut Booking	Lav
Sikret datalinje via 100 % krypteret kommunikation via SSL (RapidSSL)	Lav
Svar på henvendelser pr. e-mail og aftaler om konsultation	Lav
Korrespondance på "nettet" – der er password til pc'er	Lav
Kommunikation med databehandler (hvis aktuelt)	Lav

[*)] 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

Samtykke til håndtering af personoplysninger

Behandling af dine personoplysninger – samtykke

Jeg giver hermed mit samtykke til at Karina Rasmussen må indsamle og behandle mine personoplysninger. Personoplysninger omfatter følgende typer:

- Navn
- E-mail adresse
- Kontaktinformation
- CPR-nummer (Kun hvis det findes relevant i forbindelse med behandlingsforløbet)
- Helbredsoplysninger

Formålet med indsamling af ovenstående informationer er nødvendig for at udføre den rette behandling af klienten.

Procedure for behandling af data:

Jeg optager journal til brug for min behandling af dig på klinikken og dit forløb hos mig. Jeg har tavshedspligt og opbevarer dine data i et elektronisk journalsystem hos Terapeut Booking og opbevarer derfor ikke data på min arbejdscomputer. Data anvendes udelukkende til brug for din behandling. Hvis du ikke har fået behandling hos mig i 5 år, slettes de indsamlede informationer.

Du har pligt til at afgive korrekte informationer om sygdomme, medicinfirbrug, graviditet mv. i forbindelse med behandling.

Oplysningerne opbevares elektronisk hos Terapeut Booking (www.terapeutbooking.dk).

Dine rettigheder:

Du har ret til indsigt i de indsamlede data, og har ret til at bede om udlevering og sletning af disse. Du har ligeledes ret til at trække dit samtykke tilbage.

Dette kan du gøre ved at kontakte Karina Rasmussen på e-mail: sileo@outlook.dk.

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

Dato og underskrift

_____ _____

Bilag 2, indhold i databehandleraftalen

Databehandleraftale

Imellem:

Dataansvarlig

Karina Rasmussen
Gasværksvej 3
4300 Holbæk
CVR: 35980253
Kontaktperson: sileo@outlook.dk

og

Databehandler

Mango Apps ApS
Strandlodsvej 44, 3. sal
2300 København S
CVR: 35642536
Kontakt: kontakt@terapeutbooking.dk

Indhold

Baggrund for databehandleraftalen

- Denne aftale fastsætter de rettigheder og forpligtelser, som finder anvendelse, når databehandleren foretager behandling af personoplysninger på vegne af den dataansvarlige.

- Aftalen er udformet med henblik på parternes efterlevelse af artikel 28, stk. 3, i Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (Databeskyttelsesforordningen), som stiller specifikke krav til indholdet af en databehandleraftale.

- Databehandlerens behandling af personoplysninger sker med henblik på opfyldelse af parternes "hovedaftale": Den dataansvarliges brug af Terapeut Booking-systemet.

- Databehandleraftalen og "hovedaftalen" er indbyrdes afhængige, og kan ikke opsiges særskilt. Databehandleraftalen kan dog – uden at opsige "hovedaftalen" – erstattes af en anden gyldig databehandleraftale.

- Denne databehandleraftale har forrang i forhold til eventuelle tilsvarende bestemmelser i andre aftaler mellem parterne, herunder i "hovedaftalen".

- Til denne aftale hører fire bilag. Bilagene fungerer som en integreret del af databehandleraftalen.

- Databehandleraftalens Bilag A indeholder nærmere oplysninger om behandlingen, herunder om behandlingens formål og karakter, typen af personoplysninger, kategorierne af registrerede og varighed af behandlingen.

- Databehandleraftalens Bilag B indeholder den dataansvarliges betingelser for, at databehandleren kan gøre brug af eventuelle underdatabehandlere, samt en liste over de eventuelle underdatabehandlere, som den dataansvarlige har godkendt.

- Databehandleraftalens Bilag C indeholder en nærmere instruks om, hvilken behandling databehandleren skal foretage på vegne af den dataansvarlige (behandlingens genstand), hvilke sikkerhedsforanstaltninger, der som minimum skal iagttages, samt hvordan der føres tilsyn med databehandleren og eventuelle underdatabehandlere.

- Databehandleraftalens Bilag D indeholder parternes eventuelle regulering af forhold, som ikke ellers fremgår af databehandleraftalen eller parternes "hovedaftale".

- Databehandleraftalen med tilhørende bilag opbevares skriftligt, herunder elektronisk af begge parter.

- Denne databehandleraftale frigør ikke databehandleren for forpligtelser, som efter databeskyttelsesforordningen eller enhver anden lovgivning direkte er pålagt databehandleren.

Den dataansvarliges forpligtelser og rettigheder

- Den dataansvarlige har over for omverdenen (herunder den registrerede) som udgangspunkt ansvaret for, at behandlingen af personoplysninger sker indenfor rammerne af databeskyttelsesforordningen og databeskyttelsesloven.

- Den dataansvarlige har derfor både rettighederne og forpligtelserne til at træffe beslutninger om, til hvilke formål og med hvilke hjælpemidler der må foretages behandling.

- Den dataansvarlige er blandt andet ansvarlig for, at der foreligger hjemmel til den behandling, som databehandleren instrueres i at foretage.

Databehandleren handler efter instruks

- Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

- Databehandleren underretter omgående den dataansvarlige, hvis en instruks efter databehandlerens mening er i strid med databeskyttelsesforordningen eller databeskyttelsesbestemmelser i anden EU-ret eller medlemsstaternes nationale ret.

Fortrolighed

- Databehandleren sikrer, at kun de personer, der aktuelt er autoriseret hertil, har adgang til de personoplysninger, der behandles på vegne af den dataansvarlige. Adgangen til oplysningerne skal derfor straks lukkes ned, hvis autorisationen fratages eller udløber.

- Der må alene autoriseres personer, for hvem det er nødvendigt at have adgang til personoplysningerne for at kunne opfylde databehandlerens forpligtelser overfor den dataansvarlige.

- Databehandleren sikrer, at de personer, der er autoriseret til at behandle personoplysninger på vegne af den dataansvarlige, har forpligtet sig til fortrolighed eller er underlagt en passende lovbestemt tavshedspligt.

- Databehandleren skal efter anmodning fra den dataansvarlige kunne påvise, at de relevante medarbejdere er underlagt ovennævnte tavshedspligt.

Behandlingssikkerhed

- Databehandleren iværksætter alle foranstaltninger, som kræves i henhold til databeskyttelsesforordningens artikel 32, hvoraf det bl.a. fremgår, at der under hensyntagen til det aktuelle niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal gennemføres passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

- Ovenstående forpligtelse indebærer, at databehandleren skal foretage en risikovurdering, og herefter gennemføre foranstaltninger for at imødegå identificerede risici. Der kan herunder bl.a., alt efter hvad der er relevant, være tale om følgende foranstaltninger:
    - Pseudonymisering og kryptering af personoplysninger
    - Evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og – tjenester
    - Evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
    - En procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed

- Databehandleren skal i forbindelse med ovenstående – i alle tilfælde – som minimum iværksætte det sikkerhedsniveau og de foranstaltninger, som er specificeret nærmere i denne aftales Bilag C.

- Parternes eventuelle regulering/aftale om vederlæggelse eller lign. i forbindelse med den dataansvarliges eller databehandlerens efterfølgende krav om etablering af yderligere sikkerhedsforanstaltninger vil fremgå af parternes ”hovedaftale” eller af denne aftales bilag D.

Anvendelse af underdatabehandlere

- Databehandleren skal opfylde de betingelser, der er omhandlet i databeskyttelsesforordningens artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).

- Databehandleren må således ikke gøre brug af en anden databehandler (underdatabehandler) til opfyldelse af databehandleraftalen uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige.

- I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

- Den dataansvarliges nærmere betingelser for databehandlerens brug af eventuelle underdatabehandlere fremgår af denne aftales Bilag B.

- Den dataansvarliges eventuelle godkendelse af specifikke underdatabehandlere er anført i denne aftales Bilag B.

- Når databehandleren har den dataansvarliges godkendelse til at gøre brug af en underdatabehandler, sørger databehandleren for at pålægge underdatabehandleren de samme databeskyttelsesforpligtelser som dem, der er fastsat i denne databehandleraftale, gennem en kontrakt eller andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at underdatabehandleren vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i databeskyttelsesforordningen.

- Databehandleren er således ansvarlig, så vidt muligt, gennem indgåelsen af en underdatabehandleraftale – at pålægge en eventuel underdatabehandler mindst de forpligtelser, som databehandleren selv er underlagt efter databeskyttelsesreglerne og denne databehandleraftale med tilhørende bilag.

- Underdatabehandleraftalen og eventuelle senere ændringer hertil sendes – efter den dataansvarliges anmodning herom - i kopi til den dataansvarlige, som herigennem har mulighed for at sikre sig, at der er indgået en gyldig aftale mellem databehandleren og underdatabehandleren. Eventuelle kommercielle vilkår, eksempelvis priser, som ikke påvirker det databeskyttelsesretlige indhold af underdatabehandleraftalen, skal ikke sendes til den dataansvarlige.

- Databehandleren skal så vidt muligt i sin aftale med underdatabehandleren indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens

konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder og gøre dem gældende over for underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

- Hvis underdatabehandleren ikke opfylder sine databeskyttelsesforpligtelser, forbliver databehandleren fuldt ansvarlig over for den dataansvarlige for opfyldelsen af underdatabehandlerens forpligtelser.

Overførsel af oplysninger til tredjelande eller internationale organisationer

- Databehandleren må kun behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel (overladelse, videregivelse samt intern anvendelse) af personoplysninger til tredjelande eller internationale organisationer, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser, jf. art 28, stk. 3, litra a.

- Uden den dataansvarliges instruks eller godkendelse kan databehandleren – inden for rammerne af databehandleraftalen - derfor bl.a. ikke;
    - videregive personoplysningerne til en dataansvarlig i et tredjeland eller i en international organisation,
    - overlade behandlingen af personoplysninger til en underdatabehandler i et tredjeland,
    - lade oplysningerne behandle i en anden af databehandlerens afdelinger, som er placeret i et tredjeland.

- Den dataansvarliges eventuelle instruks eller godkendelse af, at der foretages overførsel af personoplysninger til et tredjeland, vil fremgå af denne aftales Bilag C.

Bistand til den dataansvarlige

- Databehandleren bistår, under hensyntagen til behandlingens karakter, så vidt muligt den dataansvarlige ved hjælp af passende tekniske og organisatoriske foranstaltninger, med opfyldelse af den dataansvarliges forpligtelse til at besvare anmodninger om udøvelsen af de registreredes rettigheder som fastlagt i databeskyttelsesforordningens kapitel 3.

- Dette indebærer, at databehandleren så vidt muligt skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:
    - oplysningspligten ved indsamling af personoplysninger hos den registrerede
    - oplysningspligten, hvis personoplysninger ikke er indsamlet hos den registrerede
    - den registreredes indsigtsret
    - retten til berigtigelse
    - retten til sletning (»retten til at blive glemt«)
    - retten til begrænsning af behandling
    - underretningspligt i forbindelse med berigtigelse eller sletning af personoplysninger eller begrænsning af behandling
    - retten til dataportabilitet
    - retten til indsigelse
    - retten til at gøre indsigelse mod resultatet af automatiske individuelle afgørelser, herunder profilering

- Databehandleren bistår den dataansvarlige med at sikre overholdelse af den dataansvarliges forpligtelser i medfør af databeskyttelsesforordningens artikel 32-36 under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for databehandleren, jf. art 28, stk. 3, litra f.

  Dette indebærer, at databehandleren, under hensyntagen til behandlingens karakter, skal bistå den dataansvarlige i forbindelse med, at den dataansvarlige skal sikre overholdelsen af:
    - forpligtelsen til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til de risici, der er forbundet med behandlingen
    - forpligtelsen til at anmelde brud på persondatasikkerheden til tilsynsmyndigheden (Datatilsynet) uden unødig forsinkelse og om muligt senest 72 timer, efter at den dataansvarlige er blevet bekendt med bruddet, medmindre at det er usandsynligt, at bruddet på persondatasikkerheden indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder.
    - forpligtelsen til – uden unødig forsinkelse – at underrette den/de registrerede om brud på persondatasikkerheden, når et sådant brud sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
    - forpligtelsen til at gennemføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder
    - forpligtelsen til at høre tilsynsmyndigheden (Datatilsynet) inden behandling, såfremt en konsekvensanalyse vedrørende databeskyttelse viser, at behandlingen vil føre til høj risiko i mangel af foranstaltninger truffet af den dataansvarlige for at begrænse risikoen

- Parternes eventuelle regulering/aftale om vederlæggelse eller lignende i forbindelse med databehandlerens bistand til den dataansvarlige vil fremgå af parternes ”hovedaftale” eller af denne aftales bilag D.

Underretning om brud på persondatasikkerheden

- Databehandleren underretter uden unødig forsinkelse den dataansvarlige efter at være blevet opmærksom på, at der er sket brud på persondatasikkerheden hos databehandleren eller en eventuel underdatabehandler. Databehandlerens underretning til den dataansvarlige skal om muligt ske senest 36 timer efter at denne er blevet bekendt med bruddet, sådan at den dataansvarlige har mulighed for at efterleve sin eventuelle forpligtelse til at anmelde bruddet til tilsynsmyndigheden inden for 72 timer.

- I overensstemmelse med denne aftales afsnit 10.2., litra b, skal databehandleren - under hensyntagen til behandlingens karakter og de oplysninger, der er tilgængelige for denne – bistå den dataansvarlige med at foretage anmeldelse af bruddet til tilsynsmyndigheden. Det kan betyde, at databehandleren bl.a. skal hjælpe med at tilvejebringe nedenstående oplysninger, som efter databeskyttelsesforordningens artikel 33, stk. 3, skal fremgå af den dataansvarliges anmeldelse til tilsynsmyndigheden:
    - Karakteren af bruddet på persondatasikkerheden, herunder, hvis det er muligt, kategorierne og det omtrentlige antal berørte registrerede samt kategorierne og det omtrentlige antal berørte registreringer af personoplysninger
    - Sandsynlige konsekvenser af bruddet på persondatasikkerheden
    - Foranstaltninger, som er truffet eller foreslås truffet for at håndtere bruddet på persondatasikkerheden, herunder hvis det er relevant, foranstaltninger for at begrænse dets mulige skadevirkninger

Sletning og tilbagelevering af oplysninger

- Ved ophør af tjenesterne vedrørende behandling forpligtes databehandleren til, efter den dataansvarliges valg, at slette eller tilbagelevere alle personoplysninger til den dataansvarlige, samt at slette eksisterende kopier, medmindre EU-retten eller national ret foreskriver opbevaring af personoplysningerne.

Tilsyn og revision

- Databehandleren stiller alle oplysninger, der er nødvendige for at påvise databehandlerens overholdelse af databeskyttelsesforordningens artikel 28 og denne aftale, til rådighed for den dataansvarlige og giver mulighed for og bidrager til revisioner, herunder inspektioner, der foretages af den dataansvarlige eller en anden revisor, som er bemyndiget af den dataansvarlige.

- Den nærmere procedure for den dataansvarliges tilsyn med databehandleren fremgår af denne aftales Bilag C.

- Den dataansvarliges tilsyn med eventuelle underdatabehandlere sker som udgangspunkt gennem databehandleren. Den nærmere procedure herfor fremgår af denne aftales Bilag C.

- Databehandleren er forpligtet til at give myndigheder, der efter den til enhver tid gældende lovgivning har adgang til den dataansvarliges og databehandlerens faciliteter, eller repræsentanter, der optræder på myndighedens vegne, adgang til databehandlerens fysiske faciliteter mod behørig legitimation.

Parternes aftaler om andre forhold

- En eventuel (særlig) regulering af konsekvenserne af parternes misligholdelse af databehandleraftalen vil fremgå af parternes ”hovedaftale” eller af denne aftales Bilag D.

- En eventuel regulering af andre forhold mellem parterne vil fremgå af parternes ”hovedaftale” eller af denne aftales Bilag D.

Ikrafttræden og ophør

- Denne aftale træder i kraft ved begge parters underskrift heraf.

- Aftalen kan af begge parter kræves genforhandlet, hvis lovændringer eller uhensigtsmæssigheder i aftalen giver anledning hertil.

- Parternes eventuelle regulering/aftale om vederlæggelse, betingelser eller lignende i forbindelse med ændringer af denne aftale vil fremgå af parternes ”hovedaftale” eller af denne aftales bilag D.

- Opsigelse af databehandleraftalen kan ske i henhold til de opsigelsesvilkår, inkl. opsigelsesvarsel, som fremgår af ”hovedaftalen”.

- Aftalen er gældende, så længe behandlingen består. Uanset ”hovedaftalens” og/eller databehandleraftalens opsigelse, vil databehandleraftalen forblive i kraft frem til behandlingens ophør og oplysningernes sletning hos databehandleren og eventuelle underdatabehandlere.

- Aftalen indgås elektronisk og accept af aftalen gives ved tryk på knappen ”Godkend” efter gennemlæsning og accept af denne aftale.

Kontaktpersoner/kontaktpunkter hos den dataansvarlige og databehandleren

- Parterne kan kontakte hinanden via de registrerede kontaktoplysninger, der opgives ved den elektroniske accept af denne databehandleraftale.

- Parterne er forpligtet til løbende at orientere hinanden om ændringer vedrørende kontaktpersonen/kontaktpunktet.

Bilag A - Oplysninger om behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er:

- Databehandleren stiller platform til rådighed for terapeuter til brug for:
    - Klient-registrering
    - Journalisering
    - Booking af tid/aftale
    - Kommunikation mellem behandler og klient

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige drejer sig primært om (karakteren af behandlingen):
Behandlingen vil ske via Mango Apps' Terapeut Booking-platform, som stilles til rådighed for den enkelte behandler. Platformen fungerer som et system til brug for registrering af medlemmer eller klienter for den enkelte terapeut. I tillæg hertil, benyttes systemet til journalisering i de tilfælde, hvor det er klienter, der går hos en behandler. I tilfældet med klienter kan det også i medfør af Sundhedsloven være nødvendigt at registrere patientens cpr-nummer i forhold til tilskudsberettiget behandling.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- E-mailadresse
- Navn
- Cpr.nr.
- Helbredsoplysninger
- Identifikation til online betaling
- Kontaktinformation (adresse, telefonnummer)

Behandlingen omfatter følgende kategorier af registrerede:

- Personer, som har oprettet en gratis Terapeut-profil og/eller benytter platformen Terapeut Booking til registrering af klienter
- Personer, der har oprettet en profil i Sikre beskeder direkte på Terapeut Booking

Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige kan påbegyndes efter denne aftales ikrafttræden. Behandlingen har følgende varighed:

- Behandlingen er ikke tidsbegrænset og varer indtil aftalen opsiges eller ophæves af en af parterne

Bilag B - Betingelser for databehandlerens brug af underdatabehandlere og liste over godkendte underdatabehandlere

Betingelser for databehandlerens brug af eventuelle underdatabehandlere
Databehandleren har den dataansvarliges generelle godkendelse til at gøre brug af underdatabehandlere. Databehandleren skal dog underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer. En sådan underretning skal være den dataansvarlige i hænde minimum 2 måneder før anvendelsen eller ændringen skal træde i kraft. Såfremt den dataansvarlige har indsigelser mod ændringerne, skal den dataansvarlige give meddelelse herom til databehandleren inden 1 måned efter modtagelsen af underretningen. Den dataansvarlige kan alene gøre indsigelse, såfremt den dataansvarlige har rimelige, konkrete årsager hertil.

Godkendte underdatabehandlere
Den dataansvarlige har ved databehandleraftalens ikrafttræden godkendt anvendelsen af følgende underdatabehandlere:

Navn	CVR-nr	Adresse	Beskrivelse af behandling
Dinero	34731543	Vesterbrogade 1 L, 6. sal 1620 København V	Terapeut Bookings brugere kan også forbinde til Dinero og fakturere deres klienter herigennem.
Mailgun			Udsendelse af e-mails
Sygeforsikringen Danmark	22656511	Palægade 5, 1261 København K	Indberetning af fakturaer til Sygeforsikringen “danmark”
E-conomic	29403473	Langebrogade 1 1411 København K.	Regnskabssystem som benyttes ifm. fakturering af abonnement af Terapeut Bookings brugere. Terapeut Bookings brugere kan også forbinde til e-conomic og fakturere deres klienter herigennem.
MailChimp			Terapeut Bookings brugere kan også forbinde til MailChimp og administrere nyhedsbreve til deres klienter.
Campaign Monitor			Vi udsender nyhedsbreve til Campaign Monitor til vores brugere.
ePay	28855060	Vandmanden 10 L DK-9200 Aalborg	Behandling af betalingsoplysninger.

Stripe			Behandling af betalingsoplysninger for terapeutens klienter.

Den dataansvarlige har ved databehandleraftalens ikrafttræden specifikt godkendt anvendelsen af ovennævnte underdatabehandlere til netop den behandling, som er beskrevet ud for parten. Databehandleren kan ikke – uden den dataansvarliges specifikke og skriftlige godkendelse – anvende den enkelte underdatabehandler til en "anden" behandling and aftalt eller lade en anden underdatabehandler foretage den beskrevne behandling.

Bilag C - Instruks vedrørende behandling af personoplysninger

Behandlingens genstand/ instruks
Databehandlerens behandling af personoplysninger på vegne af den dataansvarlige sker ved, at databehandleren udfører følgende:

- Terapeut Booking
    - Stiller et system til rådighed for den dataansvarlige til brug for oprettelse af klienter, booking af aftaler, journalisering mv.
- Dinero
    - Udveksling af regnskabsoplysninger efter konkret instruks fra den dataansvarlige
- Sygeforsikringen Danmark
    - Udbetaling af tilskud fra sygeforsikring efter instruks fra den dataansvarlige
- E-conomic
    - Udveksling af regnskabsoplysninger efter konkret instruks fra den dataansvarlige
- MailChimp
    - Udveksling af email-oplysninger efter konkret instruks fra den dataansvarlige
- Stripe
    - Modtagelse af online-betaling fra klienter efter konkret instruks fra den dataansvarlige

Behandlingssikkerhed
Sikkerhedsniveauet skal afspejle:

- At der er tale om behandling af en stor mængde almindelige personoplysninger omfattet af Databeskyttelsesforordningens artikel 6 om "almindelige personoplysninger" samt i nogle tilfælde tillige følsomme personoplysninger omfattet af Databeskyttelsesforordningens artikel 9, og der skal etableres et "passende" sikkerhedsniveau" i overensstemmelse hermed.

Databehandleren er herefter berettiget og forpligtet til at træffe beslutninger om, hvilke tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at skabe det nødvendige (og aftalte) sikkerhedsniveau omkring oplysningerne.

Databehandleren skal dog – i alle tilfælde og som minimum – gennemføre følgende foranstaltninger, som er aftalt med den dataansvarlige (på baggrund af den risikovurdering den dataansvarlige har foretaget):

Pseudonymisering anvendes ved statistik.

Mango Apps medarbejdere er underlagt krav om fortrolighed og integritet, og disse krav er også en del af Mango Apps persondatapolitik.

Mango Apps har indgået databehandleraftaler med underdatabehandlere herunder også i forhold til software og systemer.

I tilfælde af en fysisk eller teknisk hændelse, har Mango Apps mulighed for rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger via back-up.

Effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerheden testes og afprøves regelmæssigt i samarbejde med Mango Apps' underdatabehandlere.

Overførsel af personoplysninger til usikre tredjelande finder ikke sted og skulle det blive aktuelt vil det være under iagttagelse af de påkrævede sikkerhedsforanstaltninger for usikre tredjelande.

De almindelige personoplysninger opbevares på centraliseret og beskyttet vis og der er taget højde for dataminimering og begrænsning af adgang til både almindelige personoplysninger og følsomme personoplysninger.

Fysisk sikring af computere og sikring af adgang til lokaliteter, hvor der behandles personoplysninger.

Ved anvendelse af hjemme-/fjernarbejdsplads er computere sikret med personligt password.

Opbevaringsperiode/sletterutine
Personoplysningerne opbevares hos databehandleren, indtil den dataansvarlige anmoder om at få oplysningerne slettet eller tilbageleveret

Lokalitet for behandling
Behandling af de i aftalen omfattede personoplysninger kan ikke uden den dataansvarliges forudgående skriftlige godkendelse ske på andre lokaliteter end de følgende:

- Mango Apps, Strandlodsvej 44, 3. sal, 2300 København S

Instruks eller godkendelse vedrørende overførsel af personoplysninger til tredjelande
Overførsel af personoplysninger til et tredjeland vil i givet fald finde sted under iagttagelse af de fornødne sikkerhedsforanstaltninger efter databeskyttelsesforordningens kapital 5.

Nærmere procedurer for den dataansvarliges tilsyn med den behandling, som foretages hos databehandleren
Den dataansvarlige eller en repræsentant for den dataansvarlige har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos databehandleren, når der efter den dataansvarliges vurdering opstår et behov herfor.

Den dataansvarliges eventuelle udgifter i forbindelse med et fysisk tilsyn afholdes af den dataansvarlige selv. Databehandleren er dog forpligtet til at afsætte de ressourcer

(hovedsageligt den tid), der er nødvendig for, at den dataansvarlige kan gennemføre sit tilsyn.

Nærmere procedurer for tilsynet med den behandling, som foretages hos eventuelle underdatabehandlere

Databehandleren eller en repræsentant for databehandleren har herudover adgang til at føre tilsyn, herunder fysisk tilsyn, hos underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Udover det planlagte tilsyn, kan der føres tilsyn med underdatabehandleren, når der efter databehandlerens (eller den dataansvarliges) vurdering opstår et behov herfor.

Dokumentation for de afholdte tilsyn sendes snarest muligt til orientering hos den dataansvarlige.