Databehandleravtale

Mellom

**Behandlingsansvarlig**
Kunden

&

**Databehandler**
EasyPractice ApS
Strandlodsvej 44, 3. sal
2300 København S Denmark
CVR 35642536
Kontakt: support@easypractice.net

# Indhold

[**Indhold 2**](#_2et92p0)

[**1. Bakgrunn for Databehandleravtale 3**](#_3dy6vkm)

[**2. Den behandlingsansvarliges plikter og rettigheter 3**](#_1t3h5sf)

[**3. Databehandleren handler etter instrukser 4**](#_4d34og8)

[**4. Konfidensialitet 4**](#_2s8eyo1)

[**5. Sikkerhet ved behandling 4**](#_17dp8vu)

[**6. Bruk av underdatabehandlere 5**](#_3rdcrjn)

[**7. Overføring til tredjeland eller internasjonale organisasjoner 6**](#_26in1rg)

[**8. Bistand til den behandlingsansvarlig 6**](#_lnxbz9)

[**9. Brudd på Personopplysningssikkerheten 7**](#_35nkun2)

[**10. Sletting og returnering av opplysninger 7**](#_1ksv4uv)

[**11. Innsyn og revisjon 7**](#_44sinio)

[**12. Erstatningsansvar 8**](#_2jxsxqh)

[**13. Ikrafttredelse og opphør 8**](#_z337ya)

[**14. Meddelelser 8**](#_3j2qqm3)

[**15. Lovvalg og verneting 8**](#_1y810tw)

[**Vedlegg A - Informasjon om behandlingen 9**](#_4i7ojhp)

[**Vedlegg B - Underdatabehandlere 10**](#_2xcytpi)

[**Vedlegg C - Informasjonssikkerhet 11**](#_1ci93xb)

#

# Bakgrunn for Databehandleravtale

* 1. Denne databehandleravtalen ("**databehandleravtalen**") fastsetter de rettigheter og plikter som gjelder når databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige.
	2. Databehandleravtalen er utformet for at partene skal overholde Europaparlaments- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger og om oppheving av direktiv 95/46/EF ("**personvernforordningen**"), og gjeldende norsk lov som gjennomfører personvernforordningen (heretter samlet "**Personvernlovgivningen**").
	3. Databehandlerens behandling av personopplysninger gjøres for å oppfylle hovedavtalen mellom partene: "Terms and conditions” ("**hovedavtalen**"). Databehandlingen er nærmere beskrevet i vedlegg A (Informasjon om behandlingen).
	4. I denne Databehandleravtalen skal "personopplysning", "behandlingsansvarlig", "databehandler", den "registrerte", "behandling", "brudd på personopplysningssikkerheten", "tilsynsmyndighet" og "tredjestater" forstås på samme måte som etter Personvernlovgivningen.
	5. I tilfelle motstrid mellom denne databehandleravtalen og hovedavtalen, skal databehandleravtalen ha forrang for alle forhold som angår databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige.
	6. Denne databehandleravtalen består av denne generelle avtaleteksten, og følgende vedlegg: Vedlegg A (Informasjon om behandlingen), Vedlegg B (Underdatabehandlere) og Vedlegg C (Informasjonssikkerhet).
	7. Databehandleravtalen og tilhørende dokumenter oppbevares skriftlig, også elektronisk, av begge parter.
	8. Partene er enige om at den engelske versjonen av databehandleravtalen, tilgjengelig her, er den autoritative og offisielle versjonen av databehandleravtalen. Ved uoverensstemmelser eller inkonsistens skal den engelske versjonen ha forrang fremfor eventuelle oversatte versjoner. Du kan få tilgang til engelsk DPA her: https://system.easypractice.net/dpa-en
	9. Denne databehandleravtalen fritar ikke databehandleren for eventuelle forpliktelser som er direkte pålagt databehandleren i henhold til personvernlovgivningen.

# Den behandlingsansvarliges plikter og rettigheter

* 1. Den behandlingsansvarlige er ansvarlig for at behandlingen av personopplysninger skjer innenfor rammene av personvernlovgivningen.
	2. Den behandlingsansvarlige har rett og plikt til å bestemme formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes.
	3. Den behandlingsansvarlige er ansvarlig for, blant annet, å sikre at det foreligger et behandlingsgrunnlag for behandlingen av personopplysninger som databehandleren instrueres om.

# Databehandleren handler etter instrukser

* 1. Databehandleren kan bare behandle personopplysninger i henhold til dokumenterte instrukser fra den behandlingsansvarlige, med mindre databehandleren etter EU/EØS-retten eller medlemsstatenes nasjonale rett som databehandleren er underlagt, er forpliktet til å behandle personopplysninger på en annen måte. Dersom en slik forpliktelse oppstår skal databehandleren underrette den behandlingsansvarlige om dette rettslige kravet før behandlingen, med mindre denne rett forbyr slik underretning av hensyn til viktige samfunnsinteresser, jf. artikkel 28 nr. 3 bokstav a.
	2. Databehandleren skal omgående underrette den behandlingsansvarlige dersom databehandleren mener at en instruks fra den behandlingsansvarlige er i strid med personvernlovgivningen.

# Konfidensialitet

* 1. Databehandleren skal sørge for at det bare er de personene som er autorisert til det, som har tilgang til personopplysningene som behandles på vegne av den behandlingsansvarlige.
	2. Databehandleren skal sørge for at personene som er autorisert til å behandle personopplysninger på vegne av den behandlingsansvarlige, er underlagt enten lovpålagt eller avtalemessig taushetsplikt.
	3. På anmodning fra den behandlingsansvarlige skal databehandleren kunne påvise at de aktuelle ansatte er underlagt taushetsplikt.

# Sikkerhet ved behandling

* 1. Databehandleren skal iverksette alle tiltak som kreves i henhold til artikkel 32 i personvernforordningen. Dette innebærer at databehandleren, tatt i betraktning den tekniske utviklingen, gjennomføringskostnadene og behandlingens art, omfang, sammenhengen og formålet med den aktuelle behandlingen, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et tilstrekkelig sikkerhetsnivå ved behandlingen av personopplysningene.
	2. Ovennevnte forpliktelse innebærer at databehandleren må gjennomføre en risikovurdering og deretter treffe tiltak for å håndtere identifiserte risikoer. Slike tiltak kan blant annet omfatte følgende:
		1. Pseudonymisering og kryptering av personopplysninger;
		2. tiltak som sikrer evnen til å sikre vedvarende konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemene og -tjenestene;
		3. tiltak som sikrer evnen til å gjenopprette tilgjengeligheten og tilgangen til personopplysninger i rett tid dersom det oppstå en fysisk eller teknisk hendelse; og/eller
		4. en prosess for regelmessig testing, analysering og vurdering av hvor effektive behandlingens tekniske og organisatoriske sikkerhetstiltak er.
	3. Disse tiltakene er spesifisert i vedlegg C (Informasjonssikkerhet). For dette formål skal den behandlingsansvarlige gi databehandleren alle opplysninger som er nødvendige for å identifisere og vurdere slike risikoer.I forbindelse med den behandlingsansvarliges eller databehandlerens etterfølgende behov for etablering av ytterligere sikkerhetstiltak, vil dette fremgå av hovedavtalen eller av vedlegg C (Informasjonssikkerhet).

# Bruk av underdatabehandlere

* 1. Databehandleren må oppfylle vilkårene i personvernforordningen artikkel 28 nr. 2 og 4 for å bruke en annen databehandler ("**underdatabehandler**").
	2. Databehandleren kan ikke bruke en underdatabehandler til å behandle personopplysninger under denne databehandleravtalen uten forutgående skriftlig samtykke fra den behandlingsansvarlige.
	3. Den behandlingsansvarlige gir herved databehandleren sin generelle tillatelse til å benytte underdatabehandlere for å oppfylle Databehandleravtalen. Underdatabehandleravtalerne som benyttes ved inngåelsen av denne databehandleravtalen er inntatt i vedlegg B (Underdatabehandlere).
	4. Ved utskiftning av underdatabehandlere inntatt i vedlegg B (Underdatabehandlere), eller engasjering av nye underdatabehandlere, skal databehandleren varsle den behandlingsansvarlige i rimelig tid før underdatabehandleren tas i bruk. Behandlingsansvarlig kan motsette seg slike endringer dersom det er rimelig grunn til å anta at engasjementet vil svekke beskyttelsesnivået som garanteres for personopplysningene under denne databehandleravtalen. Dersom behandlingsansvarlig motsetter seg bruk av underdatabehandleren skal partene i god tro igangsette diskusjoner med mål om å finne en løsning som ivaretar den behandlingsansvarliges bekymringer.
	5. Når databehandleren engasjerer en underdatabehandler i samsvar med dette punkt 6, skal databehandleren sørge for å pålegge underdatabehandleren de samme forpliktelsene som databehandleren er pålagt i henhold til databehandleravtalen.
	6. Databehandlerens bruk av underdatabehandlere skal ikke redusere eller begrense databehandlerens ansvar og forpliktelser etter denne databehandleravtalen.

# Overføring til tredjeland eller internasjonale organisasjoner

* 1. Databehandleren skal ikke overføre eller på annen måte forårsake at personopplysningene blir overført ut av EU/EØS-området til tredjeland eller internasjonale organisasjoner som ikke er anerkjent som land med et tilstrekkelig beskyttelsesnivå for personopplysninger av EU-kommisjonen, uten den behandlingsansvarliges skriftlige forhåndssamtykke. Før et slikt samtykke gis, kan den behandlingsansvarlige kreve at Databehandleren treffer nødvendige beskyttelsestiltak, herunder (men ikke begrenset til) at overføringen skjer med grunnlag i EU-kommisjonens standardavtaler for overføringer av personopplysninger til tredjeland.

# Bistand til den behandlingsansvarlig

* 1. Databehandleren skal, ved hjelp av egnede tekniske og organisatoriske tiltak, bistå den behandlingsansvarlige med å svare på henvendelser fra registrerte vedrørende utøvelse av den registrertes rettigheter overfor behandlingsansvarlig etter kapittel III i personvernforordningen.
	2. Idet det tas hensyn til behandlingens art og den informasjonen som er tilgjengelig for databehandleren, skal databehandleren bistå den behandlingsansvarlige med å sikre overholdelse av den behandlingsansvarliges forpliktelser i henhold til personvernforordningen artikkel 32-36. Dette innebærer at databehandleren skal bistå den behandlingsansvarlige med å sikre overholdelse av:
		1. plikten til å gjennomføre en konsekvensanalyse for personvern dersom en type behandling sannsynligvis vil utgjøre en høy risiko for fysiske personers rettigheter og friheter ("data protection impact assessment" eller "DPIA").
		2. plikten til å rådføre seg med tilsynsmyndigheten (Datatilsynet) før behandling dersom en vurdering av personvernkonsekvenser viser at behandlingen vil føre til høy risiko dersom den behandlingsansvarlige ikke treffer tiltak for å begrense risikoen.
	3. Databehandleren har krav på kompensasjon for medgått tid for bistand til den behandlingsansvarlige dersom dette er avtalt i hovedavtalen eller i vedlegg C (Informasjonssikkerhet).

# Brudd på Personopplysningssikkerheten

* 1. Databehandleren skal underrette den behandlingsansvarlige uten ugrunnet opphold etter å ha blitt kjent med at det har forekommet et brudd på personopplysningssikkerheten hos databehandleren eller en underdatabehandler. Databehandleren skal gi nødvendig informasjon og bistand slik at den behandlingsansvarlige kan oppfylle sine rapporteringsplikter etter personvernlovgivningen. Databehandleren skal videre iverksette alle nødvendige tiltak for å begrense virkningen av sikkerhetsbruddet.

# Sletting og returnering av opplysninger

* 1. Ved opphør av databehandleravtalen kan den behandlingsansvarlige, dersom mulig, instruere databehandleren til å returnere alle personopplysninger som databehandleren har behandlet på vegne av den behandlingsansvarlige, til den behandlingsansvarlige eller til en tredjepart utpekt av den behandlingsansvarlige. Den behandlingsansvarlige kan i tillegg kreve at disse personopplysningene slettes. Databehandleren skal innen rimelig tid etter å ha mottatt en slik instruks, sende en skriftlig bekreftelse på at personopplysningene har blitt returnert og/eller slettet.

# Innsyn og revisjon

* 1. Databehandleren skal gjøre tilgjengelig for den behandlingsansvarlige all informasjon som er nødvendig for å påvise databehandlerens overholdelse av artikkel 28 i personvernforordningen og denne databehandleravtalen. Databehandleren skal muliggjøre og bidra til revisjoner, herunder inspeksjoner, som utføres av den behandlingsansvarlige eller en annen revisor autorisert av den behandlingsansvarlige for å kontrollere at Databehandleren overholder sine forpliktelser etter denne Databehandleravtalen.
	2. Den detaljerte prosedyren for den behandlingsansvarliges tilsyn med databehandleren finnes i vedlegg C (Informasjonssikkerhet).
	3. Den behandlingsansvarliges tilsyn med eventuelle underdatabehandlere er basert på databehandleren. Den detaljerte prosedyren for dette er angitt i vedlegg C (Informasjonssikkerhet).

# Erstatningsansvar

* 1. Ansvarsbegrensingen inntatt i hovedavtalen gjelder tilsvarende for partenes brudd på denne databehandleravtalen.
	2. Partenes ansvar for de registrertes eller andre fysiske personers tap som følge av brudd på personvernlovgivningen skal være regulert i henhold til artikkel 82 i personvernforordningen, uten ovennevnte begrensning.

# Ikrafttredelse og opphør

* 1. Denne avtalen trer i kraft på datoen for begge partenes underskrift av hovedavtalen.
	2. Begge partene kan kreve avtalen reforhandlet dersom lovendringer eller uhensiktsmessigheter i avtalen gir grunnlag til dette.
	3. Eventuell etterfølgende endringer knyttet til vederlag, betingelser eller lignende vil fremgå av hovedavtalen eller av vedlegg C (Informasjonssikkerhet).
	4. Oppsigelse av databehandleravtalen kan skje i samsvar med hovedavtalen.
	5. Databehandleravtalen gjelder så lenge Databehandleren behandler personopplysninger på vegne av den behandlingsansvarlige. Uavhengig av oppsigelsen av Hovedavtalen, vil databehandleravtalen forbli i kraft til behandlingen avsluttes og personopplysningene slettes av databehandleren og eventuelle underdatabehandlere.
	6. Avtalen inngås elektronisk, og aksept av avtalen gis ved å trykke på knappen "Godta" etter å ha lest og akseptert denne avtalen.

# Meddelelser

* 1. Meddelelser, varsler eller annen kommunikasjon mellom den Behandlingsansvarlige og databehandleren som i henhold til denne Databehandleravtalen skal gis skriftlig, skal sendes på e-post som angitt i vedlegg A (Informasjon om behandlingen).

# Lovvalg og verneting

* 1. Hovedavtalens bestemmelser om lovvalg og verneting gjelder tilsvarende for Databehandleravtalen.

# Vedlegg A - Informasjon om behandlingen

**Formålet med databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige er å:**

* Levere plattformen til den behandlingsansvarlige. Plattformen inneholder følgende funksjoner for sluttbrukerne:
	+ Klienthåndtering
	+ Journalføring
	+ Booking av avtaler/ online kurs/ arrangementer
	+ Kommunikasjon mellom terpaeuter og pasient
	+ Fakturering og betaling

**Databehandlerens behandling av personopplysninger på vegne av den behandlingsansvarlige dreier seg først og fremst om (behandlingens art):**

Behandlingen vil skje via plattformen ("**Systemet**") som stilles til rådighet for den enkelte terapeut. Plattformen fungerer som et system for registrering av medlemmer eller klienter for den enkelte terapeut. I tillegg brukes systemet for journalføring i tilfeller der det er klienter som går hos en terapeut.

Når det gjelder klienter, kan det også være nødvendig i henhold til helselovgivningen å registrere pasientens personnummer i forbindelse med stønadsberettiget behandling.

**Behandlingen omfatter følgende typer personopplysninger om de registrerte:**

* E-post
* Navn
* Personnummer
* Identifikasjon for nettbetaling
* Kontaktinformasjon (adresse, telefonnummer)
* Bruker ID nummer utdelt av Systemet

**Behandlingen omfatter følgende kategorier av registrerte:**

* Kunden og Kundens ansatte som har opprettet en profil og/eller bruker Systemet for registrering av klienter.
* Kundens klienter som har opprettet en profil i Online Booking direkte hos Systemet.

**Særlige kategorier av personopplysninger:**

* Helseopplysninger

# Vedlegg B - Underdatabehandlere

Ved inngåelsen av databehandleravtalen har den behandlingsansvarlige godkjent bruken av følgende underdatabehandlere: [Sub Data Processors](https://docs.google.com/spreadsheets/d/1QbAFma7w_KatGQPkE3p4WgSKZpSkOatfAiDfMecAMvc)

# Vedlegg C - Informasjonssikkerhet

**Informasjonssikkerhet**

Sikkerhetsnivået skal gjenspeile:

* Behandlingen av en stor mengde vanlige personopplysninger som omfattes av artikkel 6 i personvernforordningen om "alminnelige personopplysninger", og i noen tilfeller også sensitive personopplysninger som omfattes av artikkel 9 i personvernforordningen, og et "passende" sikkerhetsnivå bør fastsettes i samsvar med dette.

Databehandleren har da rett og plikt til å ta beslutninger om de tekniske og organisatoriske sikkerhetstiltakene som skal brukes for å skape det nødvendige (og avtalte) sikkerhetsnivået rundt opplysningene.

Databehandleren må imidlertid - i alle tilfeller og minst - gjennomføre følgende tiltak som er avtalt med den behandlingsansvarlige (basert på risikovurderingen utført av den behandlingsansvarlige):

Pseudonymisering brukes til statistikk.