

Databehandleraftale

Imellem:

Dataansvarlig

Rick Scott Consulting, ApS
Ny Boder 8 (SundhedsCenter Børkop)
7080 Børkop
CVR: 38918931
Kontaktperson: info@rickscott.dk

og

Databehandler

EasyPractice ApS
Dampfærgevej 27, 5.
2100 København Ø
Denmark
CVR: 35642536
Kontakt: kontakt@terapeutbooking.dk

Indhold

Indhold	2
1. Baggrund for databehandleraftalen	3
2. Den Dataansvarliges rettigheder og forpligtelser	4
3. Databehandleren handler efter instruktioner	4
4. Fortrolighed	4
5. Sikkerhed ved behandling	5
6. Brug af underdatabehandlere	5
7. Overførsler til tredjelande eller internationale organisationer	6
8. Bistand til den Dataansvarlige	6
9. Brud på persondata	7
10. Sletning og returnering af data	7
11. Adgang og revision	7
12. Ansvar	8
13. Ikrafttræden og ophør	8
14. Meddelelser	8
15. Gældende lov og værneting	8
Bilag A - Oplysninger om behandlingen	9
Bilag B - Underdatabehandlere	11
Bilag C - Informationssikkerhed	17

1. Baggrund for databehandleraftalen

- 1.1. Denne databehandleraftale (" **Databehandleraftalen** ") fastsætter de rettigheder og forpligtelser, der gælder for behandling af personoplysninger af Databehandleren, der handler på vegne af den Dataansvarlige.
- 1.2. Formålet med denne Databehandleraftale er at sikre, at parterne overholder 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 ("den **generelle forordning om databeskyttelse** " eller " **GDPR** "). og gældende dansk lov, der implementerer den generelle forordning om databeskyttelse (herefter samlet benævnt " **databeskyttelseslovgivningen** ").
- 1.3. Databehandlerens behandling af personoplysninger udføres med henblik på at opfylde hovedaftalen mellem parterne: "Vilkår og betingelser" (" **Hovedaftalen** "). Behandlingen er beskrevet mere detaljeret i bilag A (Oplysninger om behandlingen).
- 1.4. I denne Databehandleraftale skal "personoplysninger", "Dataansvarlig", "Databehandler", "registreret", "behandling", "brud på persondatasikkerheden", "tilsynsmyndighed" og "tredjelande" forstås i overensstemmelse med databeskyttelseslovgivningen.
- 1.5. I tilfælde af uoverensstemmelse mellem denne Databehandleraftale og hovedaftalen har Databehandleraftalen forrang i alle forhold vedrørende Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige.
- 1.6. Denne Databehandleraftale består af denne hoveddel af aftalen og følgende bilag: Bilag A (Oplysninger om behandlingen), Bilag B (Underdatabehandlere) og Bilag C (Informationssikkerhed).
- 1.7. Databehandleraftalen og tilhørende dokumenter opbevares i et skriftligt elektronisk format af begge parter.
- 1.8. Parterne er enige om, at den engelske version af Databehandleraftalen er den autoritative og officielle version af denne aftale. I tilfælde af uoverensstemmelser eller uoverensstemmelser har den engelske version forrang frem for oversatte versioner.
- 1.9. Denne Databehandleraftale fritager ikke Databehandleren for forpligtelser, der direkte pålægges Databehandleren i henhold til databeskyttelseslovgivningen.

2. Den Dataansvarliges rettigheder og forpligtelser

- 2.1. Den Dataansvarlige er ansvarlig for at sikre, at behandlingen af personoplysninger sker i overensstemmelse med databeskyttelseslovgivningen.
- 2.2. Den Dataansvarlige har ret og pligt til at fastsætte formålet med behandlingen af personoplysninger og de midler, der skal anvendes.
- 2.3. Den Dataansvarlige er blandt andet ansvarlig for at sikre, at den behandling, som den instruerer Databehandleren om at udføre, er understøttet af et lovligt grundlag.

3. Databehandleren handler efter instruktioner

- 3.1. Databehandleren må kun behandle personoplysninger i overensstemmelse med dokumenterede instruktioner fra den Dataansvarlige, medmindre Databehandleren er forpligtet i henhold til EU/EØS-retten eller en medlemsstats ret, som Databehandleren er underlagt, til at behandle personoplysninger på en anden måde. Hvis en sådan retlig forpligtelse opstår, skal Databehandleren underrette den Dataansvarlige om det retlige krav inden behandlingen, medmindre denne lov forbyder en sådan underretning af hensyn til vigtige samfundsinteresser, jf. artikel 28(3)(a).
- 3.2. Databehandleren skal straks underrette den Dataansvarlige, hvis Databehandleren mener, at en instruktion fra den Dataansvarlige overtræder databeskyttelseslovgivningen.

4. Fortrolighed

- 4.1. Databehandleren skal sikre, at adgangen til de personoplysninger, der behandles på den Dataansvarliges vegne, er begrænset til personer, der er bemyndiget til at have sådan adgang.
- 4.2. Databehandleren skal sikre, at de personer, der er bemyndiget til at behandle personoplysninger på den Dataansvarliges vegne, er underlagt en lovbestemt eller kontraktlig tavshedspligt.
- 4.3. Efter anmodning fra den Dataansvarlige skal Databehandleren kunne påvise, at ansatte og andre personer, der er bemyndiget til at behandle personoplysninger på den Dataansvarliges vegne, er underlagt en tavshedspligt.

5. Sikkerhed ved behandling

- 5.1. Databehandleren skal implementere alle de foranstaltninger, der kræves i henhold til artikel 32 i GDPR. Det betyder, at Databehandleren under hensyntagen til den teknologiske udvikling, implementeringsomkostningerne og den pågældende behandlings art, omfang, kontekst og formål samt risici af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder skal implementere passende tekniske og organisatoriske foranstaltninger for at sikre et tilstrækkeligt sikkerhedsniveau for behandling af personoplysninger.
- 5.2. Ovenstående forpligtelse indebærer, at Databehandleren skal udføre en risikovurdering og derefter træffe foranstaltninger til at håndtere identificerede risici. Sådanne foranstaltninger kan *blandt andet* omfatte følgende:
 - 5.2.1. Pseudonymisering og kryptering af personoplysninger;
 - 5.2.2. foranstaltninger til at sikre den fortsatte fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester;
 - 5.2.3. foranstaltninger til at sikre muligheden for rettidig genoprettelse af tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse; og/eller
 - 5.2.4. en proces til regelmæssig testning, analyse og vurdering af effektiviteten af de tekniske og organisatoriske foranstaltninger i forbindelse med behandlingen.
- 5.3. De relevante foranstaltninger er specificeret i bilag C (Informationssikkerhed). Den Dataansvarlige skal give Databehandleren alle nødvendige oplysninger til at identificere og vurdere sådanne risici. I forbindelse med den Dataansvarliges eller Databehandlerens efterfølgende behov for implementering af yderligere sikkerhedsforanstaltninger skal sådanne yderligere foranstaltninger være specificeret i hovedaftalen eller i bilag C (Informationssikkerhed).

6. Brug af underdatabehandlere

- 6.1. Databehandleren skal overholde betingelserne i artikel 28 (2) og (4) i den generelle forordning om databeskyttelse for at kunne engagere en anden Databehandler til behandling i henhold til denne Databehandleraftale ("**underdatabehandler** ").
- 6.2. Databehandleren må ikke anvende en underdatabehandler til at behandle personoplysninger i henhold til denne Databehandleraftale uden den Dataansvarliges forudgående skriftlige samtykke.
- 6.3. Den Dataansvarlige giver hermed Databehandleren sin generelle tilladelse til at anvende underdatabehandlere til at opfylde Databehandleraftalen. Underdatabehandlere, der er i brug på tidspunktet for indgåelse af denne Databehandleraftale, er angivet i bilag B (Underdatabehandlere).

- 6.4. I tilfælde af udskiftning af en eller flere af de underdatabehandlere, der er nævnt i bilag B (Underdatabehandlere), eller udpegelse af nye underdatabehandlere, skal Databehandleren underrette den Dataansvarlige inden for rimelig tid, inden den nye underdatabehandler anvendes. Den Dataansvarlige kan gøre indsigelse mod sådanne ændringer, hvis der er rimelig grund til at antage, at engagementet vil reducere det beskyttelsesniveau, der er garanteret for personoplysningerne i henhold til denne Databehandleraftale. Hvis den Dataansvarlige gør indsigelse mod brugen af underdatabehandleren, skal parterne i god tro indlede drøftelser med det formål at finde en løsning, der imødekommer den Dataansvarliges bekymringer.
- 6.5. Når Databehandleren engagerer en underdatabehandler i overensstemmelse med dette punkt 6, skal Databehandleren sikre, at underdatabehandleren er bundet af de samme forpligtelser som dem, der påhviler Databehandleren i henhold til denne Databehandleraftale.
- 6.6. Databehandlerens brug af underdatabehandlere skal ikke reducere eller begrænse Databehandlerens ansvar og forpligtelser i henhold til denne Databehandleraftale.

7. Overførsler til tredjelande eller internationale organisationer

- 7.1. Databehandleren må ikke uden den Dataansvarliges forudgående skriftlige samtykke overføre eller på anden måde foranledige, at personoplysninger overføres uden for EU/EØS-området til tredjelande eller internationale organisationer, der ikke er anerkendt af Europa-Kommissionen som lande, der sikrer et tilstrækkeligt beskyttelsesniveau for personoplysninger. Før et sådant samtykke gives, kan den Dataansvarlige kræve, at Databehandleren træffer passende sikkerhedsforanstaltninger, herunder (men ikke begrænset til) at sikre, at overførslen sker på grundlag af EU-Kommissionens standardkontraktbestemmelser for overførsel af personoplysninger til tredjelande.

8. Bistand til den Dataansvarlige

- 8.1. Databehandleren skal ved hjælp af passende tekniske og organisatoriske foranstaltninger bistå den Dataansvarlige med at besvare anmodninger fra registrerede vedrørende udøvelsen af den registreredes rettigheder over for den Dataansvarlige i henhold til kapitel III i GDPR.
- 8.2. Under hensyntagen til behandlingens art og de oplysninger, der er tilgængelige for Databehandleren, skal Databehandleren bistå den Dataansvarlige med at sikre overholdelse af den Dataansvarliges forpligtelser i henhold til artikel 32-36 i GDPR. Det betyder, at Databehandleren skal bistå den Dataansvarlige med at sikre overholdelse af:

8.2.1.forpligtelsen til at udføre en konsekvensanalyse vedrørende databeskyttelse, hvis en type behandling sandsynligvis vil resultere i en høj risiko for fysiske personers rettigheder og frihedsrettigheder ("**konsekvensanalyse vedrørende databeskyttelse**" eller "**DPIA**").

8.2.2.forpligtelsen til at konsultere tilsynsmyndigheden (Datatilsynet) før behandling, hvis en DPIA viser, at behandlingen vil resultere i en høj risiko, hvis den Dataansvarlige ikke implementerer foranstaltninger til at afbøde risikoen.

8.3. Databehandleren har ret til compensation for tid brugt på bistand til den Dataansvarlige, hvis dette er aftalt i hovedaftalen eller i bilag C (Informationssikkerhed).

9. Brud på persondata

9.1. Databehandleren skal underrette den Dataansvarlige uden unødigt forsinkelse efter at være blevet opmærksom på et brud på persondatasikkerheden hos Databehandleren eller en underdatabehandler. Databehandleren skal yde de nødvendige oplysninger og bistand, så den Dataansvarlige kan opfylde sine underretningsforpligtelser i henhold til databeskyttelseslovgivningen. Databehandleren skal endvidere træffe alle nødvendige foranstaltninger for at begrænse virkningen af bruddet på persondatasikkerheden.

10.Sletning og returnering af data

10.1.Ved ophør af Databehandleraftalen kan den Dataansvarlige, hvis det er muligt, instruere Databehandleren om at returnere alle personoplysninger, som Databehandleren behandler på vegne af den Dataansvarlige, til den Dataansvarlige eller til en tredjepart udpeget af den Dataansvarlige. Den Dataansvarlige kan også anmode om sletning af personoplysningerne. Databehandleren skal inden for rimelig tid efter at have modtaget en sådan instruks sende en skriftlig bekræftelse på, at personoplysningerne er returneret og/eller slettet.

11.Adgang og revision

11.1.Databehandleren skal stille alle nødvendige oplysninger til rådighed for den Dataansvarlige for at påvise Databehandlerens overholdelse af artikel 28 i GDPR og denne Databehandleraftale. Databehandleren skal muliggøre og bidrage til revisioner, herunder inspektioner, der udføres af den Dataansvarlige eller en anden revisor, der er bemyndiget af den Dataansvarlige, til at verificere, at Databehandleren overholder sine forpligtelser i henhold til denne Databehandleraftale.

11.2.Den detaljerede procedure for den Dataansvarliges tilsyn med Databehandleren er beskrevet i bilag C (Informationssikkerhed).

- 11.3. Den Dataansvarliges tilsyn med eventuelle underdatabehandlere udføres via Databehandleren. Den detaljerede procedure herfor er beskrevet i bilag C (Informationssikkerhed).

12. Ansvar

- 12.1. Ansvarsbegrænsningen anført i Hovedaftalen gælder ligeledes for enhver misligholdelse af denne Databehandleraftale begået af en part.
- 12.2. Parternes ansvar for tab, som registrerede eller andre fysiske personer lider som følge af overtrædelser af databeskyttelseslovgivningen, er underlagt artikel 82 i GDPR, uden at ovenstående begrænsning er omfattet af dette.

13. Ikrafttræden og ophør

- 13.1. Denne Databehandleraftale træder i kraft på datoen for begge parters underskrift af denne Databehandleraftale.
- 13.2. Hver part kan anmode om genforhandling af Databehandleraftalen, hvis ændringer i lovgivningen eller mangler i Databehandleraftalen giver grundlag herfor.
- 13.3. Eventuelle efterfølgende ændringer vedrørende aflønning, vilkår eller lignende forhold vil være angivet i hovedaftalen eller i bilag C (Informationssikkerhed).
- 13.4. Databehandleraftalen kan opsiges i overensstemmelse med bestemmelserne i Hovedaftalen.
- 13.5. Databehandleraftalen forbliver gældende, så længe Databehandleren behandler personoplysninger på vegne af den Dataansvarlige. Uanset ophør af hovedaftalen forbliver Databehandleraftalen gældende, indtil behandlingen ophører, og personoplysningerne slettes af Databehandleren og eventuelle involverede underdatabehandlere.

14. Meddelelser

- 14.1. Meddelelser eller andre former for kommunikation mellem den Dataansvarlige og Databehandleren, som skal gives skriftligt i henhold til denne Databehandleraftale, skal sendes via e-mail som angivet i bilag A (Oplysninger om behandlingen).

15. Gældende lov og værneting

- 15.1. Bestemmelserne i Hovedaftalen om lovvalg og værneting finder tilsvarende anvendelse på denne Databehandleraftale.

Bilag A - Oplysninger om behandlingen

1. Formål med behandlingen - Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige sker med det formål at give adgang til og brug af EasyPractice-plattformen, herunder: - Klienthåndtering - Journalføring - Booking af aftaler/onlinekurser/arrangementer - Kommunikation mellem terapeuter og patienter - Fakturering og betaling

2. Behandlingens art - Behandlingen sker via den EasyPractice-plattform, som den Dataansvarlige bruger. Dette omfatter opbevaring og administration af klient- og patientjournaler, bookingoplysninger, kommunikation og faktureringsdata.

3. Behandlingens varighed - Behandlingen fortsætter, så længe Hovedaftalen mellem parterne er gældende, og indtil alle personoplysninger er slettet eller returneret til den Dataansvarlige i overensstemmelse med denne Databehandleraftale.

4. Kategorier af registrerede - Den Dataansvarliges medarbejdere, der bruger platformen - Den Dataansvarliges klienter/patienter, der booker aftaler eller interagerer via platformen

5. Typer af personoplysninger - Navn - E-mail - Kontaktoplysninger (adresse, telefonnummer) - CPR-nummer (hvor det er lovpligtigt) - Sundhedsdata (som særlig kategori af data) - Bruger-ID tildelt af systemet - Betalings-id'er (f.eks. fakturanummer, transaktions-ID)

6. Særlige kategorier af data - Sundhedsdata i overensstemmelse med artikel 9 i GDPR.

7. Brug af underdatabehandlere må kun anvendes til de formål, der er nødvendige for at levere de tjenester, der er beskrevet i dette bilag A. Alle underdatabehandlere skal behandle data i nøje overensstemmelse med den Dataansvarliges instruktioner og kun for at udføre deres udpegede funktioner.

- Lever platformen til controlleren. Plattformen inkluderer følgende funktioner til slutbrugere:
 - Klienthåndtering
 - Journalføring
 - Booking af aftaler/onlinekurser/arrangementer
 - Kommunikation mellem terapeuter og patienter
 - Fakturering og betaling

Databehandlerens behandling af personoplysninger på vegne af den Dataansvarlige vedrører primært (behandlingens karakter):

Behandlingen vil foregå via den platform ("**Systemet** "), der stilles til rådighed for den enkelte [terapeut](#). Platformen fungerer som et system til registrering af medlemmer eller klienter hos den enkelte terapeut. Derudover anvendes systemet til journalføring i tilfælde, hvor der er klienter, der går til en terapeut.

I forhold til klienter kan det også være nødvendigt, i henhold til sundhedslovgivningen, at registrere patientens CPR-nummer i forbindelse med ydelsesberettiget behandling.

Behandlingen omfatter følgende typer af personoplysninger om de registrerede:

- E-mail
- Navn
- CPR-nummer
- Identifikation til online betaling
- Kontaktoplysninger (adresse, telefonnummer)
- Bruger-ID-nummer udstedt af systemet

Behandlingen omfatter følgende kategorier af registrerede:

- Kunden og kundens medarbejdere, der har oprettet en profil og/eller bruger systemet til klientregistrering.
- Kundens kunder, der har oprettet en profil i Online Booking direkte via systemet.

Særlige kategorier af personoplysninger:

- Sundhedsdata

Bilag B - Underdatabehandlere

Ved at indgå denne Databehandleraftale har den Dataansvarlige godkendt brugen af følgende underdatabehandlere:

Navn	Behandlingens art og formål	Kategorier af personoplysninger	Placering
Wannafind	Cloud hosting udbyder	Alle personoplysninger - vores databaser og servere er hostet her.	https://www.wannafind.dk/ , Danmark
Amazon Web Services	Cloud hosting og teknisk serviceudbyder, behandler sikkerhedskopier	Alle personoplysninger.	Kun EU-regioner
Google	Teknisk serviceudbyder - kort, analyser, kalenderfunktioner	IP-adresse brugt i analyser (kun hvis aktiveret af brugeren); Google Kalender sender klientnavne (kun hvis aktiveret af brugeren).	https://analytics.google.com/ , https://calendar.google.com/ , USA
Intercom, Inc.	Cloud-baseret in-app support chatplatform	Alle personoplysninger - vores kunder kan dele alle data i supportanmodninger.	Irland
Mailgun Technologies Inc.	E-mail leveringstjeneste.	E-mailadresser, beskedindhold.	USA
MailChimp	E-mail marketing- og automatiseringsplatform.	E-mailadresser, abonnentdata, kampagnedata (kun hvis aktiveret af brugeren).	USA
Cpsms	SMS-beskedtjeneste.	Telefonnumre, beskedindhold.	Danmark
SMS DK	SMS-beskedtjeneste.	Telefonnumre, beskedindhold.	Danmark

Stripe	Behandling af online betalinger og abonnementer.	Betalingskortoplysninger, faktureringsadresse, transaktionshistorik.	USA og EU
Posthog	Produktanalyseplatform	Brugerhændelser, webstedsinteraktioner (kun anonymiserede bruger-ID'er og ingen PII deles).	USA og EU
MixPanel	Produktanalyseplatform	Brugerhændelser, webstedsinteraktioner og potentielt andre brugerdata.	USA
ChartMogul	Abonnementsanalyseplatform.	Abonnementsdata, indtægtsoplysninger og kundedata.	USA
Hubspot, Inc.	Marketingautomatisering og CRM-plattform.	Brugerkontaktinformation, marketingdata og kundedata.	Tyskland
HotJar	Webstedsanalyse og brugerfeedback.	Webstedsbesøgendes adfærd, feedbackdata (f.eks. undersøgelser, heatmaps).	EU
Onpay	Betalingsgateway.	Betalingsdata, transaktionsdetaljer.	Danmark
Dinero	Finansielt regnskabsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktiveret af brugeren).	Danmark
Economic	Finansielt regnskabsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktiveret af brugeren).	Danmark
Fiken	Finansielt regnskabsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktiveret af brugeren).	Norge

Fortnox	Finansielt regnskabsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktiveret af brugeren).	Sverige
Helsenett	Digitale tjenester for sundhedspersonale	Patientdata, medicinske journaler og andre følsomme sundhedsoplysninger (kun hvis aktiveret af brugeren).	Norge
Zapier	Automatiseringsserviceudbydere	Data fra tilsluttede apps, som kan inkludere brugerdata (kun hvis aktiveret af brugeren).	USA
Altcha	Cloud-baseret SMS spam-detektionstjeneste	Brugerinteraktionsdata til bot-detektion.	EU
Billy	Finansielt regnskabsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktiveret af brugeren).	Danmark
Danmark	Sundhedsforsikrings tjeneste	Forsikringsrelaterede data, skadesdata, policetagere (kun hvis aktiveret af brugeren).	Danmark
Helfo	Sundhedsforsikrings tjeneste	Patientdata, sundhedsdata og finansielle data relateret til sundhedstjenester (kun hvis aktiveret af brugeren).	Norge
Criipto	Digital identitet og signering.	Brugeridentitetsdata, signeringsdata.	Danmark
Netsuite	Enterprise resource planning software	Forskellige forretningsdata, som kan inkludere kundedata, finansielle data osv.	USA

Facebook	Social autentificeringsløsning og analyseudbyder	Offentlig Facebook-profilinformation (kun hvis aktiveret af brugeren).	USA
Cloudflare	Domæneadministrations-tjeneste	Webstedsbesøgendes data, IP-adresser, sikkerhedslogs.	USA
Mobilepay	Betalingsløsning	Betalingsdata, transaktionsdetaljer, brugerinformation (kun hvis aktiveret af brugeren).	Danmark
Epay	Betalingsløsning	Betalingsdata, transaktionsdetaljer.	Danmark
Vipps	Betalingsløsning	Betalingsdata, transaktionsdetaljer, brugerinformation (kun hvis aktiveret af brugeren).	Norge
Zettle	Mobilt salgssted (mPOS) system.	Transaktionsdata, betalingsinformation (kun hvis aktiveret af brugeren).	Sverige
New Relic	Ydeevneovervågning og observerbarhed.	Applikationsydeevnedata, som kan inkludere nogle brugerdata.	USA
Notion	Team samarbejds- og dokumentationssoftware	Brugergenereret indhold, som kan inkludere personoplysninger.	USA
Pusher	Realtidskommunikationssoftware	Data relateret til realtidshændelser og beskeder, som kan inkludere brugerdata.	Storbritannien
What is my browser	Tjeneste til identifikation af browserinformation.	Browsertype, version og andre tekniske detaljer.	N/A (Placering ikke specificeret i kilden)

IpApi	Geolocation via IP-adresse opslagstjeneste	IP-adresser.	USA
Geoplugin	Geolocation via IP-adresse opslagstjeneste	IP-adresser.	N/A (Placering ikke specificeret i kilden)
Bing	Analyseudbyder, brugt til sporing af konverteringer	Søgeforespørgsler, brugeradfærd på Bing.	USA
Sentry	Fejlmonitorerings- og rapporteringssoftware	Fejllogs, som kan indeholde nogle brugerdata.	USA
Speechmatics	Realtids tale-til-tekst transskriptionssoftware	Lyddata, transskriptioner.	Storbritannien
Campaign Monitor	E-mail marketingplatform	E-mailadresser, abonnentdata, kampagnedata.	USA
Tryg Behandlerbooking	Online bookingsplatform for terapeuter.	Terapeutdata, klientdata, aftaledata og kommunikation mellem terapeuter og klienter (kun hvis aktiveret af brugeren).	Danmark
Digicare	Digitale løsninger til sundhedsvæsenet.	Patientdata, medicinske journaler, kommunikationsdata mellem patienter og sundhedsudbydere og aftaledata (kun hvis aktiveret af brugeren).	Norge
Exorlive	Digital trænings- og træningsplatform.	Bruger træningsdata, sundhedsdata (kun hvis aktiveret af brugeren).	Norge

Medcom	Dansk sundhedskommunikationsnetværk.	Patientdata, medicinske journaler og andre følsomme sundhedsoplysninger (kun hvis aktiveret af brugeren).	Danmark
KMD	Leverer datatransmissionstjenester (VANS-protokol) for Medcom-data.	Patientdata, medicinske journaler og andre følsomme sundhedsoplysninger relateret til Medcom (kun hvis aktiveret af brugeren).	Danmark

Bemærk: Eventuelle nye underdatabehandlere vil blive underrettet den Dataansvarlige på forhånd, så der kan gøres indsigelser. Underdatabehandlere må kun behandle data til de formål, der er beskrevet i bilag A.

Bilag C - Informationssikkerhed

1. Sikkerhedsforanstaltninger - Databehandleren skal implementere følgende tekniske og organisatoriske foranstaltninger i overensstemmelse med artikel 32 i GDPR:

a. Behandlingssikkerhed - Sikker brugergodkendelse (f.eks. 2FA) - Rollebaserede adgangskontroller - TLS-kryptering undervejs, AES-256-kryptering i hvile - Regelmæssig sårbarhedsscanning og penetrationstest

b. Risikovurdering - Årlige interne og eksterne risikovurderinger - Løbende overvågning af risikoeksponering

c. Antivirus og firewall - Firewallsystemer i virksomhedsklassen - Opdateret antivirussoftware på alle endpoints

d. IP-låsning og certifikater - HTTPS med gyldige SSL-certifikater

e. Bruger- og administratoradgang - Princippet om færrest rettigheder - Onboarding-/offboarding-adgangsprocedurer

f. Overvågning og logføring - Systemaktivitetslogfiler med revisionsspor - Alarmer i realtid for mistænkelig adfærd

g. Organisatoriske foranstaltninger - Interne databeskyttelsespolitikker - Årlig GDPR- og sikkerhedstræning for alle medarbejdere

h. Sikker kommunikation - Krypterede kommunikationskanaler (HTTPS, TLS) - Sikre beskedsystemer

i. Kryptering - Kryptering af personoplysninger både under transit og i lagring - Krypteringsnøgler administreres og roteres sikkert

j. Backup - Daglige krypterede backups gemt i EU-datacentre - Regelmæssig test af backup og gendannelse

k. Fysisk sikkerhed - Sikrede datacentre med 24/7 overvågning

l. Medarbejdersikkerhed - Fortrolighedsaftaler underskrevet af alle medarbejdere - Adgang begrænset til autoriseret personale

m. Andre foranstaltninger - Hændelsesplan på plads

2. Instruktioner - Databehandleren må kun behandle personoplysninger baseret på de dokumenterede instruktioner fra den Dataansvarlige som defineret i denne Databehandlertaftale og eventuelle yderligere skriftlige instruktioner udstedt i løbet af aftalens løbetid.

3. Opbevarings- og sletningsrutine - Data gemmes i aftalens løbetid. Ved ophør eller på den Dataansvarliges anmodning: - Data slettes inden for 30 dage
- Skriftlig bekræftelse på sletning gives - Sikre sletningsprocedurer anvendes på alle medier

4. Behandlingens placering - Alle data behandles og gemmes inden for EU/EØS. Ingen data overføres til tredjelande uden forudgående skriftligt samtykke fra den Dataansvarlige.

5. Overførsler til tredjelande - Der sker ingen overførsler af personoplysninger til tredjelande, medmindre andet er skriftligt aftalt med den Dataansvarlige. Hvis sådanne overførsler foretages, vil der blive implementeret passende sikkerhedsforanstaltninger (f.eks. standardkontraktsklausuler).

6. Revision og kontrol - Databehandleren foretager en årlig intern revision af sine databehandlings- og informationssikkerhedskontroller. Resultaterne dokumenteres og er tilgængelige for den Dataansvarlige efter anmodning. Databehandleren tillader også den Dataansvarlige at foretage sin egen revision eller udpege en tredjepart (som ikke må være Databehandlerens konkurrent) til at udføre en revision med rimeligt varsel og inden for normal åbningstid.

7. Konkurs / Tredjepartsbegunstiget - I tilfælde af Databehandlerens konkurs skal den Dataansvarlige (eller en udpeget tredjepart) have adgang til at hente personoplysninger og sikkerhedskopier for at sikre kontinuitet og beskyttelse af de registreredes rettigheder.

Sikkerhedsniveauet skal afspejle:

- Behandling af en stor mængde almindelige personoplysninger som omfattet af artikel 6 i GDPR, og i nogle tilfælde også følsomme personoplysninger som omfattet af artikel 9 i GDPR. Der skal i overensstemmelse hermed fastsættes et "passende" sikkerhedsniveau.

Databehandleren har derefter ret og pligt til at træffe beslutninger om de tekniske og organisatoriske sikkerhedsforanstaltninger, der skal anvendes for at sikre det nødvendige (og aftalte) sikkerhedsniveau for dataene.

Databehandleren skal dog – i alle tilfælde og mindst – implementere følgende foranstaltninger, der er aftalt med den Dataansvarlige (baseret på den risikovurdering, der er foretaget af den Dataansvarlige):

Pseudonymisering anvendes til statistik.