

Databehandleravtale

Mellom:

Behandlingsansvarlig

Mobbhjelpen AS
Kontaktperson: mobilhege@gmail.com

og

Databehandler

EasyPractice ApS
Vesterbrogade 74
1620 København V
Denmark
Org-nummer: 35642536
Kontakt: kontakt@easypractice.net

Indhold

Indhold	2
1. Bakgrunn for databehandleravtalen	3
2. Den Dataansvarliges rettigheter og forpliktelser	4
3. Databehandleren handler etter instruksjoner	4
4. Fortrolighet	4
5. Sikkerhet ved behandling	5
6. Bruk av underdatabehandlere	5
7. Overførslar til tredjeland eller internasjonale organisasjoner	6
8. Bistand til den Dataansvarlige	6
9. Brudd på personopplysningssikkerheten	7
10. Sletting og returnering av data	7
11. Tilgang og revisjon	7
12. Ansvar	8
13. Ikrafttredelse og opphør	8
14. Meldinger	8
15. Gjeldende lov og verneting	8
Vedlegg A – Informasjon om behandlingen	10
Vedlegg B - Underdatabehandlere	12
Vedlegg C - Informasjonssikkerhet	19

1. Bakgrunn for databehandleravtalen

- 1.1. Denne databehandleravtalen (" **Databehandleravtalen** ") fastsetter rettighetene og forpliktelsene som gjelder for Databehandlerens behandling av personopplysninger på vegne av den Dataansvarlige.
- 1.2. Formålet med denne Databehandleravtalen er å sikre at partene overholder Europa-Parlamentets og Rådets forordning (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 opphevelse av direktiv 95/46/EF (" **den generelle personvernforordningen** " eller " **GDPR** "), og gjeldende norsk lovgivning som implementerer den generelle personvernforordningen (heretter samlet benevnt " **personvernlovgivningen** ").
- 1.3. Databehandlerens behandling av personopplysninger utføres med det formål å oppfylle hovedavtalen mellom partene: "Vilkår og betingelser" (" **Hovedavtalen** "). Behandlingen er mer detaljert beskrevet i Vedlegg A (Informasjon om behandlingen).
- 1.4. I denne Databehandleravtalen skal "personopplysninger", "Dataansvarlig", "Databehandler", "registrert", "behandling", "brudd på personopplysningssikkerheten", "tilsynsmyndighet" og "tredjeland" forstås i samsvar med personvernlovgivningen.
- 1.5. I tilfelle uoverensstemmelse mellom denne Databehandleravtalen og Hovedavtalen, skal Databehandleravtalen ha forrang i alle forhold vedrørende Databehandlerens behandling av personopplysninger på vegne av den Dataansvarlige.
- 1.6. Denne Databehandleravtalen består av denne hoveddelen av avtalen og følgende vedlegg: Vedlegg A (Informasjon om behandlingen), Vedlegg B (Underdatabehandlere) og Vedlegg C (Informasjonssikkerhet).
- 1.7. Databehandleravtalen og tilhørende dokumenter skal oppbevares i et skriftlig elektronisk format av begge parter.
- 1.8. Partene er enige om at den engelske versjonen av Databehandleravtalen er den autoritative og offisielle versjonen av denne avtalen. I tilfelle av uoverensstemmelser eller motstrid, skal den engelske versjonen ha forrang fremfor oversatte versjoner.
- 1.9. Denne Databehandleravtalen fritar ikke Databehandleren fra forpliktelser som direkte pålegges Databehandleren i henhold til personvernlovgivningen.

2. Den Dataansvarliges rettigheter og forpliktelser

- 2.1. Den Dataansvarlige er ansvarlig for å sikre at behandlingen av personopplysninger skjer i samsvar med personvernlovgivningen.
- 2.2. Den Dataansvarlige har rett og plikt til å fastsette formålet med behandlingen av personopplysninger og de midlene som skal benyttes.
- 2.3. Den Dataansvarlige er blant annet ansvarlig for å sikre at behandlingen som den instruerer Databehandleren om å utføre, er understøttet av et lovlig grunnlag.

3. Databehandleren handler etter instruksjoner

- 3.1. Databehandleren må kun behandle personopplysninger i samsvar med dokumenterte instruksjoner fra den Dataansvarlige, med mindre Databehandleren er forpliktet i henhold til EU/EØS-retten eller en medlemsstats rett, som Databehandleren er underlagt, til å behandle personopplysninger på en annen måte. Hvis en slik rettslig forpliktelse oppstår, skal Databehandleren underrette den Dataansvarlige om det rettslige kravet før behandlingen, med mindre denne loven forbyr en slik underretning av hensyn til viktige samfunnsinteresser, jf. artikkel 28(3)(a).
- 3.2. Databehandleren skal straks underrette den Dataansvarlige hvis Databehandleren mener at en instruksjon fra den Dataansvarlige overtrer personvernlovgivningen.

4. Fortrolighet

- 4.1. Databehandleren skal sikre at tilgangen til personopplysningene som behandles på den Dataansvarliges vegne, er begrenset til personer som er bemyndiget til å ha slik tilgang.
- 4.2. Databehandleren skal sikre at personene som er bemyndiget til å behandle personopplysninger på den Dataansvarliges vegne, er underlagt en lovbestemt eller kontraktsfestet taushetsplikt.
- 4.3. Etter anmodning fra den Dataansvarlige skal Databehandleren kunne påvise at ansatte og andre personer som er bemyndiget til å behandle personopplysninger på den Dataansvarliges vegne, er underlagt taushetsplikt.

5. Sikkerhet ved behandling

- 5.1. Databehandleren skal implementere alle de tiltak som kreves i henhold til artikkel 32 i GDPR. Dette innebærer at Databehandleren, under hensyntagen til den teknologiske utviklingen, implementeringskostnadene og den aktuelle behandlingens art, omfang, kontekst og formål, samt risikoer av varierende sannsynlighet og alvor for fysiske personers rettigheter og friheter, skal implementere passende tekniske og organisatoriske tiltak for å sikre et tilstrekkelig sikkerhetsnivå for behandling av personopplysninger.
- 5.2. Ovenstående forpliktelse innebærer at Databehandleren skal utføre en risikovurdering og deretter treffe tiltak for å håndtere identifiserte risikoer. Slike tiltak kan *blant annet omfatte* følgende:
 - 5.2.1. Pseudonymisering og kryptering av personopplysninger;
 - 5.2.2. tiltak for å sikre den fortsatte konfidensialitet, integritet, tilgjengelighet og robusthet i behandlingssystemer og -tjenester;
 - 5.2.3. tiltak for å sikre muligheten for rettidig gjenoppretting av tilgjengeligheten til og tilgangen til personopplysninger i tilfelle en fysisk eller teknisk hendelse; og/eller
 - 5.2.4. en prosess for regelmessig testing, analyse og vurdering av effektiviteten av de tekniske og organisatoriske tiltakene i forbindelse med behandlingen.
- 5.3. De relevante tiltakene er spesifisert i vedlegg C (Informasjonssikkerhet). Den Dataansvarlige skal gi Databehandleren all nødvendig informasjon for å identifisere og vurdere slike risikoer. I forbindelse med den Dataansvarliges eller Databehandlerens etterfølgende behov for implementering av ytterligere sikkerhetstiltak, skal slike ytterligere tiltak være spesifisert i hovedavtalen eller i vedlegg C (Informasjonssikkerhet).

6. Bruk av underdatabehandlere

- 6.1. Databehandleren skal overholde betingelsene i artikkel 28 (2) og (4) i den generelle personvernforordningen for å kunne engasjere en annen databehandler til behandling i henhold til denne Databehandleravtalen (" **underdatabehandler** ").
- 6.2. Databehandleren må ikke anvende en underdatabehandler til å behandle personopplysninger i henhold til denne Databehandleravtalen uten den Dataansvarliges forhåndsgodkjenning.
- 6.3. Den Dataansvarlige gir herved Databehandleren sin generelle tillatelse til å anvende underdatabehandlere for å oppfylle Databehandleravtalen. Underdatabehandlere som er i bruk på tidspunktet for inngåelse av denne Databehandleravtalen, er angitt i vedlegg B (Underdatabehandlere).

- 6.4. I tilfelle utskifting av en eller flere av underdatabehandlerne som er nevnt i vedlegg B (Underdatabehandlere), eller utnevnelse av nye underdatabehandlere, skal Databehandleren underrette den Dataansvarlige innen rimelig tid før den nye underdatabehandleren anvendes. Den Dataansvarlige kan protestere mot slike endringer dersom det er rimelig grunn til å anta at engasjementet vil redusere beskyttelsesnivået som er garantert for personopplysningene i henhold til denne Databehandleravtalen. Dersom den Dataansvarlige protesterer mot bruken av underdatabehandleren, skal partene i god tro innlede drøftelser med det formål å finne en løsning som imøtekommer den Dataansvarliges bekymringer.
- 6.5. Når Databehandleren engasjerer en underdatabehandler i samsvar med dette punktet, skal Databehandleren sikre at underdatabehandleren er bundet av de samme forpliktelsene som påhviler Databehandleren i henhold til denne Databehandleravtalen.
- 6.6. Databehandlerens bruk av underdatabehandlere skal ikke redusere eller begrense Databehandlerens ansvar og forpliktelser i henhold til denne Databehandleravtalen.

7. Overførslar til tredjeland eller internasjonale organisasjoner

- 7.1. Databehandleren må ikke, uten den Dataansvarliges forhåndsgodkjenning, overføre eller på annen måte foranledige at personopplysninger overføres utenfor EU/EØS-området til tredjeland eller internasjonale organisasjoner som ikke er anerkjent av Europa-Kommisjonen som land som sikrer et tilstrekkelig beskyttelsesnivå for personopplysninger. Før et slikt samtykke gis, kan den Dataansvarlige kreve at Databehandleren treffer passende sikkerhetstiltak, herunder (men ikke begrenset til) å sikre at overføringen skjer på grunnlag av EU-Kommisjonens standardkontraktsbestemmelser for overføring av personopplysninger til tredjeland.

8. Bistand til den Dataansvarlige

- 8.1. Databehandleren skal, ved hjelp av passende tekniske og organisatoriske tiltak, bistå den Dataansvarlige med å besvare anmodninger fra registrerte vedrørende utøvelsen av den registrertes rettigheter overfor den Dataansvarlige i henhold til kapittel III i GDPR.
- 8.2. Under hensyntagen til behandlingens art og de opplysninger som er tilgjengelige for Databehandleren, skal Databehandleren bistå den Dataansvarlige med å sikre overholdelse av den Dataansvarliges forpliktelser i henhold til artikkel 32-36 i GDPR. Dette innebærer at Databehandleren skal bistå den Dataansvarlige med å sikre overholdelse av:
- 8.2.1. forpliktelsen til å utføre en konsekvensanalyse vedrørende personvern dersom en type behandling sannsynligvis vil resultere i

en høy risiko for fysiske personers rettigheter og friheter
(“ **konsekvensanalyse vedrørende personvern** ” eller “ **DPIA** ”).

8.2.2. forpliktelsen til å konsultere tilsynsmyndigheten (Datatilsynet) før behandling dersom en DPIA viser at behandlingen vil resultere i en høy risiko, dersom den Dataansvarlige ikke implementerer tiltak for å redusere risikoen.

8.3. Databehandleren har rett til kompensasjon for tid brukt på bistand til den Dataansvarlige, dersom dette er avtalt i hovedavtalen eller i vedlegg C (Informasjonssikkerhet).

9. Brudd på personopplysningssikkerheten

9.1. Databehandleren skal underrette den Dataansvarlige uten unødig forsinkelse etter å ha blitt oppmerksom på et brudd på personopplysningssikkerheten hos Databehandleren eller en underdatabehandler. Databehandleren skal gi de nødvendige opplysninger og bistand slik at den Dataansvarlige kan oppfylle sine underrettelsesforpliktelser i henhold til personvernlovgivningen. Databehandleren skal videre treffe alle nødvendige tiltak for å begrense virkningen av bruddet på personopplysningssikkerheten.

10. Sletting og returnering av data

10.1. Ved opphør av Databehandleravtalen kan den Dataansvarlige, hvis det er mulig, instruere Databehandleren om å **returnere alle personopplysninger** som Databehandleren behandler på vegne av den Dataansvarlige, til den Dataansvarlige eller til en tredjepart utpekt av den Dataansvarlige. Den Dataansvarlige kan også anmode om sletting av personopplysningene. Databehandleren skal innen rimelig tid etter å ha mottatt en slik instruks sende en skriftlig bekreftelse på at personopplysningene er returnert og/eller slettet.

11. Tilgang og revisjon

11.1. Databehandleren skal stille alle nødvendige opplysninger til rådighet for den Dataansvarlige for å påvise Databehandlerens overholdelse av artikkel 28 i GDPR og denne Databehandleravtalen. Databehandleren skal muliggjøre og bidra til **revisjoner, herunder inspeksjoner**, som utføres av den Dataansvarlige eller en annen revisor som er bemyndiget av den Dataansvarlige, for å verifisere at Databehandleren overholder sine forpliktelser i henhold til denne Databehandleravtalen.

11.2. Den detaljerte prosedyren for den Dataansvarliges tilsyn med Databehandleren er beskrevet i vedlegg C (Informasjonssikkerhet).

11.3. Den Dataansvarliges tilsyn med eventuelle underdatabehandlere utføres via Databehandleren. Den detaljerte prosedyren for dette er beskrevet i vedlegg C (Informasjonssikkerhet).

12. Ansvar

- 12.1. Ansvarsbegrensningen anført i Hovedavtalen gjelder tilsvarende for ethvert mislighold av denne Databehandleravtalen begått av en part.
- 12.2. Partenes ansvar for tap som registrerte eller andre fysiske personer lider som følge av overtredelser av personvernlovgivningen, er underlagt artikkel 82 i GDPR, uten at ovenstående begrensning omfattes av dette.

13. Ikrafttredelse og opphør

- 13.1. Denne Databehandleravtalen trer i kraft på datoen for begge parter signatur av denne Databehandleravtalen.
- 13.2. Hver part kan anmode om reforhandling av Databehandleravtalen dersom endringer i lovgivningen eller mangler i Databehandleravtalen gir grunnlag for dette.
- 13.3. Eventuelle etterfølgende endringer vedrørende godtgjørelse, vilkår eller lignende forhold vil være angitt i hovedavtalen eller i vedlegg C (Informasjonssikkerhet).
- 13.4. Databehandleravtalen kan sies opp i samsvar med bestemmelsene i Hovedavtalen.
- 13.5. Databehandleravtalen forblir gjeldende så lenge Databehandleren behandler personopplysninger på vegne av den Dataansvarlige. Uavhengig av opphør av Hovedavtalen forblir Databehandleravtalen gjeldende inntil behandlingen opphører og personopplysningene slettes av Databehandleren og eventuelle involverte underdatabehandlere.

14. Meldinger

- 14.1. Meldinger eller andre former for kommunikasjon mellom den Dataansvarlige og Databehandleren, som skal gis skriftlig i henhold til denne Databehandleravtalen, skal sendes via e-post som angitt i vedlegg A (Informasjon om behandlingen).

15. Gjeldende lov og vernetting

- 15.1. Bestemmelsene i Hovedavtalen om lovvalg og vernetting finner tilsvarende anvendelse på denne Databehandleravtalen.

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

Vedlegg A – Informasjon om behandlingen

1. Formål med behandlingen - Databehandlerens behandling av personopplysninger på vegne av den Dataansvarlige skjer med det formål å gi tilgang til og bruk av EasyPractice-plattformen, herunder: - Klienthåndtering - Journalføring - Booking av avtaler/onlinekurs/arrangementer - Kommunikasjon mellom terapeuter og pasienter - Fakturering og betaling
 2. Behandlingens art - Behandlingen skjer via den EasyPractice-plattformen som den Dataansvarlige bruker. Dette omfatter oppbevaring og administrasjon av klient- og pasientjournaler, bookinginformasjon, kommunikasjon og faktureringsdata.
 3. Behandlingens varighet - Behandlingen fortsetter så lenge Hovedavtalen mellom partene er gjeldende, og inntil alle personopplysninger er slettet eller returnert til den Dataansvarlige i samsvar med denne Databehandleravtalen. Sure, here is the Norwegian translation of
 4. Kategorier av registrerte - Den Dataansvarliges medarbeidere som bruker plattformen, den Dataansvarliges klienter/pasienter som booker avtaler eller interagerer via plattformen.
 5. Typer av personopplysninger - Navn, E-post, Kontaktopplysninger (adresse, telefonnummer), Fødselsnummer/personnummer (der det er lovpålagt), Helsedata (som en særlig kategori av data), Bruker-ID tildelt av systemet, Betalings-ID-er (f.eks. fakturanummer, transaksjons-ID).
 6. Særlige kategorier av data - Helsedata i samsvar med artikkel 9 i GDPR.
 7. Underdatabehandlere må kun anvendes til de formål som er nødvendige for å levere tjenestene som er beskrevet i dette vedlegg A. Alle underdatabehandlere skal behandle data i nøye samsvar med den Dataansvarliges instruksjoner og kun for å utføre sine utpekte funksjoner.
- Levering av plattformen til den Dataansvarlige. Plattformen inkluderer følgende funksjoner for sluttbrukere:
 - Klienthåndtering
 - Journalføring
 - Booking av avtaler/onlinekurs/arrangementer
 - Kommunikasjon mellom terapeuter og pasienter
 - Fakturering og betaling

Databehandlerens behandling av personopplysninger på vegne av den Dataansvarlige vedrører primært (behandlingens karakter):

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

I forhold til klienter kan det også være nødvendig, i henhold til helselovgivningen, å registrere pasientens fødselsnummer/personnummer i forbindelse med ytelsesberettiget behandling.

Behandlingen omfatter følgende typer av personopplysninger om de registrerte:

- E-post
- Navn
- Fødselsnummer/Personnummer
- Identifikasjon til online betaling
- Kontaktopplysninger (adresse, telefonnummer)
- Bruker-ID-nummer utstedt av systemet

Behandlingen omfatter følgende kategorier av registrerte:

- Kunden og kundens medarbeidere som har opprettet en profil og/eller bruker systemet til klientregistrering
- Kundens kunder som har opprettet en profil i Online Booking direkte via systemet.

Særlige kategorier av personopplysninger:

- Helsedata

Vedlegg B - Underdatabehandlere

Ved å inngå denne Databehandleravtalen har den Dataansvarlige godkjent bruken av følgende underdatabehandlere:

Navn	Behandlings art og formål	Kategorier av personopplysninger	Sted
Wannafind	Skytjenesteleverandør	Alle personopplysninger - våre databaser og servere er hostet her.	https://www.wannafind.dk/ , Danmark
Amazon Web Services	Skytjeneste- og teknisk tjenesteleverandør, behandler sikkerhetskopier	Alle personopplysninger.	Kun EU-regioner
Google	Teknisk tjenesteleverandør - kart, analyser, kalenderfunksjoner	IP-adresse brukt i analyser (kun hvis aktivert av brukeren); Google Kalender sender klientnavn (kun hvis aktivert av brukeren).	https://analytics.google.com/ , https://calendar.google.com/ , USA
Intercom, Inc.	Skybasert in-app support chatplattform	Alle personopplysninger - våre kunder kan dele alle data i supportforespørsler.	Irland
Mailgun Technologies Inc.	E-postleveringstjeneste.	E-postadresser, meldingsinnhold.	USA

MailChimp	E-postmarkedsførings- og automatiseringsplattform.	E-postadresser, abonnentdata, kampanjedata (kun hvis aktivert av brukeren).	USA
Cpsms	SMS-meldingstjeneste.	Telefonnumre, meldingsinnhold.	Danmark
SMS DK	SMS-meldingstjeneste.	Telefonnumre, meldingsinnhold.	Danmark
Stripe	Behandling av online betalinger og abonnementer.	Betalingskortdetaljer, faktureringsadresse, transaksjonshistorikk.	USA og EU
Posthog	Produktanalyseplattform	Brukerhendelser, nettstedsinteraksjoner (kun anonymiserte bruker-ID-er og ingen PII deles).	USA og EU
MixPanel	Produktanalyseplattform	Brukerhendelser, nettstedsinteraksjoner og potensielt andre brukerdata.	USA
ChartMogul	Abonnementsanalyseplattform.	Abonnementsdata, inntektsinformasjon og kundedata.	USA
Hubspot, Inc.	Markedsføringsautomatisering og CRM-plattform.	Brukerkontaktinformasjon, markedsføringsdata og kundedata.	Tyskland

HotJar	Nettstedsanalyse og brukerfeedback.	Nettstedsbesøksatferd, tilbakemeldingsdata (f.eks. undersøkelser, varmekart).	EU
Onpay	Betalingsgateway.	Betalingsdata, transaksjonsdetaljer.	Danmark
Dinero	Finansiell regnskapsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktivert av brukeren).	Danmark
Economic	Finansiell regnskapsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktivert av brukeren).	Danmark
Fiken	Finansiell regnskapsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktivert av brukeren).	Norge
Fortnox	Finansiell regnskapsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktivert av brukeren).	Sverige
Helsenett	Digitale tjenester for helsepersonell	Pasientdata, medisinske journaler og annen sensitiv helseinformasjon (kun hvis aktivert av brukeren).	Norge

Zapier	Automatiseringslevere randør	Data fra tilkoblede apper, som kan inkludere brukerdata (kun hvis aktivert av brukeren).	USA
Altcha	Skybasert SMS spam-deteksjonstjeneste	Brukerinteraksjons data for bot-deteksjon.	EU
Billy	Finansiell regnskapsapp	Finansielle data, faktureringsdata og kundedata (kun hvis aktivert av brukeren).	Danmark
Danmark	Helseforsikringstjeneste	Forsikringsrelaterte data, skadedata, poliseinnehaverdata (kun hvis aktivert av brukeren).	Danmark
Helfo	Helseforsikringstjeneste	Pasientdata, helsetjenestedata og finansielle data relatert til helsetjenester (kun hvis aktivert av brukeren).	Norge
Cripto	Digital identitet og signering.	Brukeridentitetsdata, signeringsdata.	Danmark
Netsuite	Enterprise resource planning software	Diverse forretningsdata, som kan inkludere kundedata, finansielle data osv.	USA

Facebook	Sosial autentiseringsløsning og analysetjeneste	Offentlig Facebook-profilinformasjon (kun hvis aktivert av brukeren).	USA
Cloudflare	Domeneadministrasjonstjeneste	Nettstedsbesøksdata, IP-adresser, sikkerhetslogger.	USA
Mobilepay	Betalingsløsning	Betalingsdata, transaksjonsdetaljer, brukerinformasjon (kun hvis aktivert av brukeren).	Danmark
Epay	Betalingsløsning	Betalingsdata, transaksjonsdetaljer.	Danmark
Vipps	Betalingsløsning	Betalingsdata, transaksjonsdetaljer, brukerinformasjon (kun hvis aktivert av brukeren).	Norge
Zettle	Mobilt salgssted (mPOS) system.	Transaksjonsdata, betalingsinformasjon (kun hvis aktivert av brukeren).	Sverige
New Relic	Ytelsesovervåking og observerbarhet.	Applikasjonsytelsesdata, som kan inkludere noen brukerdata.	USA
Notion	Team samarbeids- og dokumentasjonsprogramvare	Brukergenerert innhold, som kan inkludere personopplysninger.	USA

Pusher	Sanntidskommunikasjonsprogramvare	Data relatert til sanntidshendelser og meldinger, som kan inkludere brukerdata.	Storbritannia
What is my browser	Tjeneste for identifisering av nettleserinformasjon .	Nettlesertype, versjon og andre tekniske detaljer.	N/A (Sted ikke spesifisert i kilden)
IpApi	Geolocation via IP-adresse oppslagstjeneste	IP-adresser.	USA
Geoplugin	Geolocation via IP-adresse oppslagstjeneste	IP-adresser.	N/A (Sted ikke spesifisert i kilden)
Bing	Analysertjeneste, brukt for sporing av konverteringer	Søkeforespørsler, brukeratferd på Bing.	USA
Sentry	Feilovervåkings- og rapporteringsprogramvare	Feillogger, som kan inneholde noen brukerdata.	USA
Speechmatics	Sanntids tale-til-tekst transkripsjonsprogramvare	Lyddata, transkripsjoner.	Storbritannia
Campaign Monitor	E-postmarkedsførings plattform	E-postadresser, abonnentdata, kampanjedata.	USA
Tryg Behandlerbooking	Online bookingsplattform for terapeuter.	Terapeutdata, klientdata, avtaledata og kommunikasjon mellom terapeuter og klienter (kun hvis aktivert av brukeren).	Danmark

Digicare	Digitale løsninger for helsevesenet.	Pasientdata, medisinske journaler, kommunikasjonsdata mellom pasienter og helsepersonell, og avtaledata (kun hvis aktivert av brukeren).	Norge
Exorlive	Digital trenings- og treningsplattform.	Bruker treningsdata, helsedata (kun hvis aktivert av brukeren).	Norge
Medcom	Dansk helsekommunikasjonsnettverk.	Pasientdata, medisinske journaler og annen sensitiv helseinformasjon (kun hvis aktivert av brukeren).	Danmark
KMD	Behandlingens art og formål	Kategorier av personopplysninger	Sted

Merk: Eventuelle nye underdatabehandlere vil bli varslet den Dataansvarlige på forhånd, slik at det kan gjøres innsigelser. Underdatabehandlere må kun behandle data til de formål som er beskrevet i vedlegg A.

Vedlegg C - Informasjonssikkerhet

1. Sikkerhetstiltak - Databehandleren skal implementere følgende tekniske og organisatoriske tiltak i samsvar med artikkel 32 i GDPR:

a. Behandlingssikkerhet - Sikker brukerautentisering (f.eks. 2FA) - Rollebaserte adgangskontroller - TLS-kryptering under overføring, AES-256-kryptering i ro - Regelmessig sårbarhetsskanning og penetrasjonstesting

b. Risikovurdering - Årlige interne og eksterne risikovurderinger - Løpende overvåking av risikoeksponering

c. Antivirus og brannmur - Brannmursystemer av bedriftsklasse - Oppdatert antivirusprogramvare på alle endepunkter

d. IP-låsing og sertifikater - HTTPS med gyldige SSL-sertifikater

e. Bruker- og administratoradgang - Prinsippet om færrest rettigheter - Onboarding-/offboarding-tilgangsprosedyrer

f. Overvåking og logging - Systemaktivetslogger med revisjonsspor - Sanntidsalarmer for mistenkelig adferd

g. Organisasjonsmessige tiltak - Interne personvernpolicyer - Årlig GDPR- og sikkerhetstrening for alle ansatte

h. Sikker kommunikasjon - Krypterte kommunikasjonskanaler (HTTPS, TLS) - Sikre meldingssystemer

i. Kryptering - Kryptering av personopplysninger både under overføring og i lagring - Krypteringsnøkler administreres og roteres sikkert

j. Sikkerhetskopiering - Daglige krypterte sikkerhetskopier lagret i EU-datasentre - Regelmessig testing av sikkerhetskopiering og gjenoppretting

k. Fysisk sikkerhet - Sikrede datasentre med 24/7 overvåking

l. Medarbeidersikkerhet - Konfidensialitetsavtaler signert av alle ansatte - Tilgang begrenset til autorisert personale

m. Andre tiltak - Hendelsesplan på plass

2. Instruksjoner - Databehandleren må kun behandle personopplysninger basert på de dokumenterte instruksjonene fra den Dataansvarlige som definert i denne Databehandleravtalen og eventuelle ytterligere skriftlige instruksjoner utstedt i løpet av avtalens løpetid.

3. Oppbevarings- og sletterutine - Data lagres i avtalens løpetid. Ved opphør eller på den Dataansvarliges anmodning: - Data slettes innen 30 dager - Skriftlig bekreftelse på sletting gis - Sikre sletteprosedyrer anvendes på alle medier.

4. Behandlingens plassering - Alle data behandles og lagres innenfor EU/EØS. Ingen data overføres til tredjeland uten forutgående skriftlig samtykke fra den Dataansvarlige.

5. Overførslar til tredjeland - Det skjer ingen overførslar av personopplysninger til tredjeland, med mindre annet er skriftlig avtalt med den Dataansvarlige. Hvis slike overførslar foretas, vil passende sikkerhetstiltak (f.eks. standardkontraktsklausuler) bli implementert.

6. Revisjon og kontroll

Databehandleren foretar en årlig intern revisjon av sine databehandlings- og informasjonssikkerhetskontroller. Resultatene dokumenteres og er tilgjengelige for den Dataansvarlige etter anmodning. Databehandleren tillater også den Dataansvarlige å foreta sin egen revisjon eller utpeke en tredjepart (som ikke må være Databehandlerens konkurrent) til å utføre en revisjon med rimelig varsel og innenfor normal åpningstid.

7. Konkurs / Tredjepartsbegunstiget - I tilfelle Databehandlerens konkurs skal den Dataansvarlige (eller en utpekt tredjepart) ha tilgang til å hente personopplysninger og sikkerhetskopier for å sikre kontinuitet og beskyttelse av de registrertes rettigheter.

Sikkerhetsnivået skal afspejle:

- Behandlingen omfatter en stor mengde alminnelige personopplysninger som omfattes av artikkel 6 i GDPR, og i noen tilfeller også sensitive personopplysninger som omfattes av artikkel 9 i GDPR. Det skal i samsvar hermed fastsettes et "passende" sikkerhetsnivå.

Databehandleren har deretter rett og plikt til å treffe beslutninger om de tekniske og organisatoriske sikkerhetstiltakene som skal anvendes for å sikre det nødvendige (og avtalte) sikkerhetsnivået for dataene.

Databehandleren skal imidlertid – i alle tilfeller og minst – implementere følgende tiltak som er avtalt med den Dataansvarlige (basert på den risikovurderingen som er foretatt av den Dataansvarlige):

Pseudonymisering anvendes til statistikk.