UTKAST — ikke signert. Dette dokumentet er til bruk i innkjøpsvurdering og gir en realistisk oversikt over avtalens innhold. Den bindende databehandleravtalen (Bilag 3) fastsettes og signeres digitalt av begge parter ved avtaleinngåelse.

DATABEHANDLERAVTALE

Bilag til hovedavtalen om bruk av Medibook – gjelder behandling av personopplysninger etter GDPR art. 28.

1. Partene

Behandlingsansvarlig («Kunden»): Klinikken som har opprettet en konto i Medibook.

Databehandler («Leverandøren»): Avalio AS, org.nr. 938 040 117, Seehusens gate 77A, 4024 Stavanger.

2. Bakgrunn og formål

Kunden bruker Medibook, en SaaS-løsning for booking, journalføring og klientoppfølging for behandlingsklinikker. I den forbindelse behandler Leverandøren personopplysninger, herunder helseopplysninger, på vegne av Kunden. Denne avtalen regulerer Leverandørens behandling av disse opplysningene.

3. Instruks og formål med behandlingen

Leverandøren skal kun behandle personopplysninger etter dokumentert instruks fra Kunden, herunder som beskrevet i hovedavtalen, med mindre annet kreves av EU-rett eller norsk rett. Behandlingen omfatter lagring, drift og tilgjengeliggjøring av systemet slik at Kunden kan gjennomføre booking, journalføring, fakturering og klientoppfølging.

4. Kategorier av registrerte og personopplysninger

- **Registrerte:** Kundens klienter/pasienter, samt Kundens ansatte og brukere av systemet.
- **Personopplysninger:** Navn, kontaktinformasjon, fødselsdato, avtale-/bookinghistorikk, betalingsinformasjon (ikke fullt kortnummer), og helseopplysninger i journal (behandlingshistorikk, bilder, skjemasvar, signaturer).

5. Underdatabehandlere

Kunden gir generelt forhåndssamtykke til at Leverandøren benytter underdatabehandlere for delfunksjoner av tjenesten, blant annet:

- **Stripe** – kortbetaling
- **Vipps MobilePay** – mobilbetaling
- **Fiken** – regnskap/bokføring (kun for klinikker som aktivt kobler til Fiken)
- **Sveve** – utsendelse av SMS-varsler (kun for klinikker som aktiverer SMS)
- Driftsleverandør for serverdrift/lagring i Norden

Leverandøren skal informere Kunden ved planlagte endringer i underdatabehandlere, slik at Kunden kan motsette seg endringen.

6. Sikkerhetstiltak

Leverandøren skal gjennomføre egnede tekniske og organisatoriske tiltak for å sikre et sikkerhetsnivå som er egnet i forhold til risikoen, herunder:

- Kryptert lagring av personopplysninger og journalinnhold
- Tilgangsstyring basert på roller (terapeut, resepsjon, lege, admin)
- Tilgangslogg for alle journaloppslag
- To-faktor-autentisering (2FA) for brukerkontoer
- Lagring av data i Norden, uten overføring til tredjeland

7. Bistand til Kunden

Leverandøren skal, så langt det er mulig, bistå Kunden med å oppfylle sine forpliktelser etter GDPR, herunder ved henvendelser fra registrerte om innsyn, retting eller sletting, og ved gjennomføring av personvernkonsekvensanalyser (DPIA). Medibook har et innebygd DPIA-verktøy som støtte for dette.

8. Avvikshåndtering

Leverandøren skal varsle Kunden uten ugrunnet opphold etter å ha blitt kjent med et brudd på personopplysningssikkerheten som involverer Kundens data, og bistå Kunden med den informasjonen som er nødvendig for at Kunden skal kunne oppfylle sin varslingsplikt overfor Datatilsynet og eventuelt de registrerte.

9. Sletting og retur av data ved opphør

Ved opphør av avtaleforholdet skal Leverandøren, etter Kundens valg, slette eller returnere alle personopplysninger til Kunden, og slette eksisterende kopier med mindre lagring kreves av lov. Nærmere frister og fremgangsmåte reguleres av hovedavtalen.

10. Revisjon og kontroll

Kunden har rett til å gjennomføre revisjon av Leverandørens behandling av personopplysninger, eller la en uavhengig tredjepart gjøre dette, for å dokumentere etterlevelse av denne avtalen.

11. Varighet

Denne avtalen gjelder så lenge Leverandøren behandler personopplysninger på vegne av Kunden i henhold til hovedavtalen.

12. Lovvalg og verneting

Avtalen reguleres av norsk rett. Tvister søkes løst i minnelighet, og bringes ellers inn for ordinære norske domstoler.