Bahlou

Databehandleraftale

Version. 2026

1. Indledning og formål

Denne databehandleraftale ("Aftalen") er indgået mellem:

- **Den dataansvarlige**: [Virksomhedsnavn, CVR og adresse]
- **Databehandleren**: **Bahlou ApS**, CVR-nr. **44660342**, c/o Arne Jacobsens Allé 72300 København

Aftalen fastlægger vilkår og rammer for, hvordan Bahlou ApS behandler personoplysninger på vegne af den dataansvarlige i forbindelse med levering af **Bahlous tjenester**, herunder brugen af Bahlou-platformen og eventuelle tilhørende systemer og services.

Formålet er at sikre, at behandling af personoplysninger sker i overensstemmelse med **Europa-Parlamentets og Rådets forordning (EU) 2016/679** af 27. april 2016 ("Databeskyttelsesforordningen" eller "GDPR"), særligt artikel 28, stk. 3, samt relevant national lovgivning.

Denne aftale udgør det fulde grundlag for behandlingen af personoplysninger og er gældende, uanset hvad der måtte være aftalt i hovedaftalen eller andre kontraktgrundlag mellem parterne, i det omfang det vedrører behandling af personoplysninger.

Aftalen består af følgende bilag, der er en integreret del af Aftalen:

- **Bilag A** – Beskrivelse af behandlingen
- **Bilag B** – Underdatabehandlere
- **Bilag C** – Instruks og sikkerhedsforanstaltninger

Parterne forpligter sig til at opbevare Aftalen skriftligt, elektronisk eller fysisk, og kunne fremvise den på anmodning fra tilsynsmyndigheder.

---

2. Definitioner og forrang

2.1 Definitioner

I denne Aftale anvendes følgende begreber med nedenstående betydning:

- **Personoplysninger**: Enhver form for information om en identificeret eller identificerbar fysisk person, jf. GDPR art. 4, nr. 1.

- **Behandling**: Enhver aktivitet, som omfattes af GDPR art. 4, nr. 2 – fx indsamling, registrering, opbevaring, sletning mv.

- **Den dataansvarlige**: Den part, der bestemmer formål og midler med behandlingen af personoplysninger.

- **Databehandleren**: Den part, der behandler personoplysninger på vegne af den dataansvarlige.

- **Underdatabehandler**: Tredjepart, som databehandleren engagerer til at udføre hele eller dele af behandlingen på den dataansvarliges vegne.

- **Tredjeland**: Et land uden for EU/EØS.

2.2 Forrang
Ved uoverensstemmelser mellem denne Aftale og andre aftaler mellem parterne, skal denne Aftale have forrang for så vidt angår forhold vedrørende behandling af personoplysninger.

---

3. Den dataansvarliges forpligtelser

Den dataansvarlige er ansvarlig for, at behandlingen af personoplysninger sker lovligt og i overensstemmelse med gældende databeskyttelseslovgivning, herunder GDPR. Det indebærer blandt andet at sikre:

- at der foreligger gyldigt behandlingsgrundlag for alle personoplysninger, der overlades til databehandleren,

- at de registrerede oplyses korrekt i overensstemmelse med artikel 13 og 14,

- at der kun videregives relevante, nødvendige og opdaterede data til behandling.

Den dataansvarlige har instruktionsbeføjelsen og er forpligtet til at give skriftlige, dokumenterede instrukser om formål og midler for behandlingen. Databehandleren må ikke anvende oplysningerne til egne formål.

---

4. Databehandlerens forpligtelser og instruks

Databehandleren må udelukkende behandle personoplysninger på baggrund af dokumenteret instruks fra den dataansvarlige – enten som defineret i denne Aftale og bilagene eller givet skriftligt undervejs.

Databehandleren skal straks underrette den dataansvarlige, hvis en instruks efter databehandlerens vurdering er i strid med gældende lovgivning.

Databehandleren skal sikre, at behandlingen sker sikkert, fortroligt og i overensstemmelse med de krav, der følger af denne Aftale og bilagene.

---

5. Fortrolighed

Databehandleren må ikke videregive eller anvende personoplysninger til andre formål end dem, der fremgår af Aftalen og den dataansvarliges instrukser.

Databehandleren skal sikre, at alle medarbejdere, konsulenter og andre, som behandler personoplysninger under databehandlerens ansvar:

- er underlagt en lovpligtig eller kontraktuel fortrolighedsforpligtelse,
- kun har adgang til personoplysninger, i det omfang det er nødvendigt for at udføre deres arbejdsopgaver, og
- har modtaget passende instruktion i håndtering af personoplysninger og informationssikkerhed.

Databehandleren skal på anmodning kunne dokumentere, at disse forpligtelser er overholdt.

---

6. Behandlingssikkerhed

Databehandleren skal træffe passende tekniske og organisatoriske foranstaltninger for at sikre, at behandlingen af personoplysninger sker med et sikkerhedsniveau, der svarer til de risici, som behandlingen indebærer, jf. GDPR artikel 32.

Foranstaltningerne fastsættes af databehandleren under hensyntagen til behandlingens karakter og de oplysninger, den dataansvarlige har givet.

Den dataansvarlige er ansvarlig for at foretage den nødvendige risikovurdering for de pågældende behandlinger og kan anmode om yderligere sikkerhedstiltag, som dokumenteres særskilt i Bilag C.

---

7. Underdatabehandlere

Databehandleren må anvende underdatabehandlere til at udføre hele eller dele af behandlingen, forudsat:

- at den dataansvarlige er informeret om og ikke har gjort indsigelse mod de anvendte underdatabehandlere, jf. Bilag B, og
- at databehandleren sikrer, at underdatabehandlere pålægges databeskyttelsesforpligtelser svarende til dem i denne Aftale.

Bahlou ApS kan frit udskifte eller tilføje underdatabehandlere med 10 dages skriftligt varsel. Manglende indsigelse betragtes som accept. Databehandleren hæfter over for den dataansvarlige for underdatabehandlerens overholdelse af denne Aftale.

---

8. Overførsel til tredjelande

Databehandleren må kun overføre personoplysninger uden for EU/EØS, hvis:

- det sker på baggrund af en dokumenteret instruks fra den dataansvarlige, eller
- det er nødvendigt for opfyldelse af lovkrav, og den dataansvarlige er informeret, medmindre det er lovligt undtaget.

Databehandleren er berettiget til at benytte underdatabehandlere i tredjelande, såfremt der foreligger et gyldigt overførselsgrundlag efter GDPR kapitel V, og dette fremgår af Bilag B.

---

9. Bistand til den dataansvarlige

Databehandleren yder bistand til den dataansvarlige i det omfang og i det format, som er proportionalt med behandlingens karakter og den dataansvarliges behov, og kun i det omfang bistanden ikke påhviler databehandleren selv.

Dette omfatter, efter særskilt anmodning:

- Teknisk bistand til opfyldelse af den dataansvarliges forpligtelser ved registreredes anmodninger (jf. GDPR kapitel III),

- Bidrag til sikkerheds- og risikovurderinger (GDPR art. 32–36),
- Understøttelse i tilfælde af sikkerhedsbrud.

Databehandleren kan fakturere bistand efter medgået tid og gældende timesats, medmindre bistanden skyldes databehandlerens egne fejl.

---

10. Underretning ved brud på persondatasikkerheden

Databehandleren skal uden unødig forsinkelse – og senest 48 timer efter opdagelse – underrette den dataansvarlige om sikkerhedsbrud, der vedrører personoplysninger omfattet af denne Aftale.

Underretningen skal så vidt muligt indeholde:

- en beskrivelse af bruddets karakter,
- hvilke typer af data og registrerede der potentielt er berørt,
- sandsynlige konsekvenser,
- hvilke afhjælpende foranstaltninger der er truffet eller foreslås.

Databehandleren bistår den dataansvarlige med de informationer, denne har brug for til eventuel anmeldelse til tilsynsmyndigheder eller registrerede, jf. GDPR artikel 33 og 34.

---

11. Sletning og tilbagelevering

Ved ophør af behandlingen – fx som følge af aftalens ophør – skal databehandleren efter den dataansvarliges valg enten:

- slette alle personoplysninger behandlet på vegne af den dataansvarlige, eller
- returnere oplysningerne i et struktureret og almindeligt anvendt format.

Hvis den dataansvarlige ikke har meddelt et valg inden 3 måneder fra ophør, slettes oplysningerne uden yderligere varsel, medmindre andet følger af gældende lovgivning.

Ved behandling af journaldata eller andre oplysninger omfattet af lovpligtige opbevaringsperioder, foretager databehandleren ikke sletning, før den lovpligtige periode er udløbet, og kun efter skriftlig instruktion fra den dataansvarlige.

Databehandleren er ikke forpligtet til at kontrollere, om særlige opbevaringsregler gælder, men vil på anmodning bistå med tilbagelevering eller overførsel i overensstemmelse med den dataansvarliges instrukser.

---

12. Revision og kontrol

Den dataansvarlige har ret til, én gang årligt, at få indsigt i databehandlerens efterlevelse af denne Aftale og relevante lovkrav. Dette sker via:

- gennemgang af årlig tredjepartsrevisor-erklæring (fx ISAE 3000) stillet til rådighed af databehandleren,

- eller efter behov: fysisk inspektion mod forudgående varsel på mindst 30 dage.

Omkostninger i forbindelse med revision afholdes af den dataansvarlige, medmindre væsentlige fejl påvises. Databehandleren er berettiget til at fakturere for medgået tid ved fysisk tilsyn, medmindre andet er aftalt.

Bilag A – Beskrivelse af behandlingen

A1. Formål med behandlingen

Formålet med databehandlerens behandling af personoplysninger på vegne af den dataansvarlige er at muliggøre brugen af **Bahlous tjenester**, herunder Bahlou-platformen og tilhørende systemer, som stilles til rådighed for kosmetiske og wellness-klinikker.

Behandlingen sker med henblik på at understøtte følgende funktioner:

- Håndtering af online booking og kundekommunikation
- Journalføring og opbevaring af behandlingsdokumentation
- Kundeadministration og kalendersystem
- Integration til betalings- og faktureringsløsninger
- Overførsel og eksport af journaler ved behov
- Automatiserede påmindelser, markedsføringstjenester (efter instruks)
- Systemdrift, vedligehold og support

Databehandlerens rolle er udelukkende at understøtte den dataansvarliges brug af disse funktioner. Behandlingen sker derfor **udelukkende efter instruks** og **til de formål, den dataansvarlige har besluttet**.

A2. Kategorier af personoplysninger

Databehandleren behandler følgende kategorier af personoplysninger på vegne af den dataansvarlige:

Almindelige personoplysninger

- Navn
- Kontaktoplysninger (telefonnummer, e-mail, adresse)
- Fødselsdato
- Køn

- Aftale- og bookinghistorik
- Kommunikation (fx beskeder, notifikationer, påmindelser)

Oplysninger om helbred og behandling (følsomme oplysninger, GDPR art. 9)

- Journalnotater
- Information om udførte og planlagte behandlinger
- Billeder relateret til behandlinger (før/efter)
- Samtykkeoplysninger
- Særlige helbredsmæssige hensyn eller kontraindikationer

Betalings- og transaktionsdata

- Fakturadata (uden kortoplysninger)
- Købshistorik
- Tidsstempler for betalinger

Tekniske og driftsmæssige data

- Brug af systemfunktioner (logning til dokumentation)
- IP-adresse og enhedsoplysninger (begrænset og efter behov)
- Tidsstempler for adgang og ændringer (fx journaladgang)

A3. Kategorier af registrerede

Databehandleren behandler personoplysninger om følgende kategorier af registrerede på vegne af den dataansvarlige:

1. Klinikkens kunder (slutbrugere)

- Personer, der har booket eller modtaget behandling hos den dataansvarlige

- Personer, som har oprettet sig online eller er blevet registreret manuelt af klinikken
- Personer, der har samtykket til journalføring og behandling

2. Klinikkens medarbejdere og behandlere

- Brugere oprettet i systemet med adgang til kundedata, kalender mv.
- Personer med roller, hvor rettigheder og logning er relevante for behandlingssikkerhed og journalføring

3. Kontaktpersoner hos den dataansvarlige

- Ejere, administratorer og ansvarlige kontaktpersoner med adgang til systemet
- Bruges til drift, kommunikation og adgangsstyring

A4. Behandlingens karakter og operationer

Databehandlerens behandling består i at stille et digitalt system (Bahlou og tilknyttede platforme) til rådighed for den dataansvarlige, hvor personoplysninger opbevares, behandles og håndteres i overensstemmelse med den dataansvarliges instruks og brug.

Behandlingen omfatter følgende operationer:

- **Indsamling og registrering** af personoplysninger via online booking, manuelle input eller dataoverførsler
- **Opbevaring og strukturering** af oplysninger i databaser og journalsystem
- **Visning og adgang** for autoriserede brugere
- **Redigering og opdatering** af eksisterende data
- **Overførsel** af data ved systemskifte eller klinikejerskifte (inkl. journaler, kundedata og aftaler)
- **Logning** af brugeradfærd og ændringer for sikkerhed og revisionsspor
- **Sletning og anonymisering** af data efter instruks eller ved udløb af opbevaringsperiode
- **Backup og gendannelse** for at sikre dataintegritet og driftsstabilitet

- **Support og fejlsøgning**, hvor adgang til data midlertidigt kan være nødvendigt (under fortrolighed)

- **Automatisk udsendelse** af notifikationer og kommunikation til registrerede (efter aktivering af funktion)

Databehandleren foretager ingen behandling for egne formål og handler alene efter dokumenteret instruks.

A5. Varighed af behandlingen

Databehandleren behandler personoplysninger, så længe den dataansvarlige har en aktiv aftale med Bahlou ApS om brug af Bahlou eller relaterede tjenester.

Ved opsigelse eller ophør af samarbejdet:

- Behandlingen fortsætter i en **afviklingsperiode på op til 90 dage**, med henblik på dataudtræk, overførsel og afmelding.

- Herefter slettes eller returneres personoplysninger, jf. Aftalens §11, medmindre gældende lovgivning eller anden aftale kræver fortsat opbevaring.

Ved inaktivitet eller misligholdelse af betaling kan databehandleren suspendere adgangen til systemet og efter nærmere varsel indlede sletning efter samme principper.

For journaloplysninger og andre oplysninger med lovbestemt opbevaringspligt gælder, at disse kun slettes efter udløb af den relevante periode, og kun efter instruks fra den dataansvarlige.

Bilag B – Underdatabehandlere

B1. Generel godkendelse og ændringsprocedure

Den dataansvarlige giver ved Aftalens indgåelse **generel godkendelse** til, at databehandleren anvender underdatabehandlere til at udføre hele eller dele af behandlingen af personoplysninger.

Databehandleren forpligter sig til:

- at føre en opdateret liste over underdatabehandlere i Bilag B2 eller via et angivet link,
- at sikre, at alle underdatabehandlere er underlagt skriftlige databehandleraftaler, der pålægger dem tilsvarende forpligtelser som i denne Aftale, og
- at sikre, at alle underdatabehandlere overholder gældende databeskyttelseslovgivning.

Ændringer i underdatabehandlere sker uden særskilt skriftlig varsel. Den dataansvarlige har dog ret til at gøre skriftlig og begrundet indsigelse mod nye underdatabehandlere **senest 10 dage efter offentliggørelse** af ændringen.

Manglende indsigelse betragtes som stiltiende accept. Det påhviler den dataansvarlige at holde sig orienteret om ændringer.

B2. Liste over godkendte underdatabehandlere

Databehandleren benytter følgende underdatabehandlere i forbindelse med levering af Bahlous tjenester, herunder Bahlou-platformen:

Kontakter			
Navn	CVR	Adresse	Formål med behandling
ONLINESITY.IO ApS	27364276	Buchwaldsgade 50 5000 Odense C Danmark	Afsendelse af SMS på vegne af kunden
DigitalOcean, LLC	5118787	105 Edgeview Drive, Suite 425, Broomfield,	Hosting og drift af platform (cloudservere)

Kontakter			
		CO 80021, USA.	PostgreSQL database
XMatiq			Softwareudvikling
Pipedrive OÜ	11958539	Mustamäe tee 3a, Tallinn, Estland	CRM-system til håndtering af leads og kundeinformation
Cloud Flare	29412006	Højvangen 4, 8660 Skanderborg, Danmark	DNS-administration
Mailgun Technologies Inc.	6297323	112 E Pecan St. #1135, San Antonio, TX	Afsendelse af e-mails (transaktionelle beskeder og notifikationer)

B3. Garantier og krav til underdatabehandlere

Databehandleren forpligter sig til kun at anvende underdatabehandlere, der lever op til kravene i GDPR og denne Aftale.

Før en underdatabehandler tages i brug, skal databehandleren sikre, at:

- der er indgået en skriftlig databehandleraftale, som pålægger underdatabehandleren databeskyttelsesforpligtelser svarende til dem i denne Aftale,
- underdatabehandleren træffer passende tekniske og organisatoriske sikkerhedsforanstaltninger i overensstemmelse med GDPR artikel 32,
- data kun overføres til tredjelande, hvis det sker med gyldigt overførselsgrundlag, herunder anvendelse af **EU-Kommissionens standardbestemmelser (SCC)** eller anden godkendt mekanisme.

Dette omfatter også adgang for underdatabehandlere eller interne ressourcer i tredjelande som led i udvikling, support eller drift, forudsat at overførslen er reguleret af et gyldigt overførselsgrundlag i henhold til GDPR kapitel V.

Databehandleren foretager en rimelig vurdering af sine underdatabehandleres databeskyttelsesniveau og kan på anmodning give dokumentation herfor.

Databehandleren hæfter over for den dataansvarlige for, at underdatabehandlere behandler personoplysninger i overensstemmelse med databehandlerens forpligtelser i henhold til denne Aftale.

Bilag C – Instruks og sikkerhedsforanstaltninger

C1. Behandlingsinstruks

Databehandleren behandler personoplysninger udelukkende med det formål at stille Bahlous digitale løsninger, herunder Bahlou-platformen, til rådighed for den dataansvarlige. Behandlingen sker på baggrund af den dataansvarliges brug af systemet og dækker funktioner som online booking, kundehåndtering, journalføring, kommunikation og dataoverførsel, jf. Bilag A.

Databehandlerens adgang til personoplysninger sker som led i:

- den daglige drift og vedligeholdelse af platformen,
- teknisk support og fejlsøgning,

- import eller migrering af data (herunder kundelister, bookinger og journaler),
- forbedring og videreudvikling af systemet, hvor adgang kan ske i anonymiseret eller maskeret form.

Databehandlerens medarbejdere, herunder support og udvikling, har adgang til personoplysninger i det omfang, det er nødvendigt for at levere den aftalte service. Udviklere har alene adgang i kontrolleret og maskeret form.

Visse behandlinger udføres automatisk som led i systemets funktionalitet, herunder:

- udsendelse af SMS og e-mails med påmindelser, bekræftelser og notifikationer,
- oprettelse og håndtering af bookinger, journaler og samtykker,
- teknisk logning og dokumentation af brugeraktivitet,
- import og strukturelt overførsel af kunde- og journaldata.

Brugen af systemet betragtes som en generel instruks, og databehandleren handler i overensstemmelse hermed. Opgaver uden for den almindelige funktionalitet, såsom permanent sletning eller eksport af alle data, kræver særskilt anmodning fra den dataansvarlige.

Databehandleren foretager ikke selvstændige beslutninger om behandlingen og anvender ikke personoplysninger til egne formål.

C2. Tekniske og organisatoriske sikkerhedsforanstaltninger

Databehandleren har implementeret passende tekniske og organisatoriske foranstaltninger i overensstemmelse med GDPR artikel 32 for at sikre et passende sikkerhedsniveau.

Adgangskontrol

- Adgang til personoplysninger er begrænset til autoriserede medarbejdere og underdatabehandlere.
- Medarbejdere har kun adgang til data i det omfang, det er nødvendigt for deres rolle (princip om mindst mulig adgang).
- Adgang styres gennem personlige logins, adgangsstyring og tofaktorgodkendelse, hvor det er relevant.

Systemlogning og revisionsspor

- Al adgang til følsomme data, herunder journaloplysninger, logges og overvåges.
- Logdata benyttes til intern kontrol, fejlsøgning og dokumentation.

Kryptering og dataintegritet

- Data opbevares i sikre datacentre og er krypteret ved overførsel (TLS/SSL).
- Kritiske oplysninger og backups kan også være krypteret ved opbevaring (at rest).
- Backup foretages regelmæssigt og opbevares i separate miljøer med adgangskontrol.

Backup og gendannelse

- Der foretages løbende backup for at sikre dataintegritet og mulighed for gendannelse i tilfælde af fejl eller hændelser.
- Gendannelsesprocedurer er dokumenteret og testes periodisk.

Tavshedspligt og intern politik

- Alle medarbejdere er underlagt tavshedspligt.
- Interne procedurer og træning sikrer, at medarbejdere håndterer personoplysninger korrekt og lovligt.
- Adgang til følsomme oplysninger logges og kontrolleres regelmæssigt.

Håndtering af brud på persondatasikkerheden

- Eventuelle brud på persondatasikkerheden anmeldes uden unødig forsinkelse til den dataansvarlige.
- Databehandleren har interne procedurer for identificering, håndtering og dokumentation af brud.

C3. Adgang og support

Databehandlerens adgang til personoplysninger er begrænset til situationer, hvor det er nødvendigt for at opfylde den aftalte service over for den dataansvarlige.

Adgang forekommer typisk i følgende tilfælde:

- **Import og datamigrering**, fx ved onboarding eller klinikoverdragelse,
- **Systemvedligeholdelse og overvågning** af driftskritiske funktioner.

Databehandlerens medarbejdere har alene adgang til data via sikre forbindelser og autentificerede konti. Udviklere har adgang i maskeret eller anonymiseret form, medmindre andet er nødvendigt og dokumenteret.

Adgangen kontrolleres og logges, og der føres revisionsspor over systemmæssige aktiviteter.

Alle medarbejdere og relevante underdatabehandlere er instrueret i korrekt databehandling og underlagt tavshedspligt.

C4. Hosting og datamiljø

Personoplysninger behandlet af databehandleren opbevares i sikre datacentre leveret af **DigitalOcean**, med primær lokation i **EU/EØS** Amsterdam.

Systemet hostes og drives som cloudløsning, og alle relevante sikkerhedscertificeringer og driftsstandarder overholdes, herunder ISO 27001 hos underdatabehandlere.

Databehandlerens drift og udvikling involverer også medarbejdere og samarbejdspartnere i tredjelande, herunder **Indien**, med adgang til data i kontrollerede, maskeret form, når det er nødvendigt for teknisk vedligeholdelse eller support.

Overførsel til tredjelande sker i henhold til GDPR kapitel V og er reguleret ved anvendelse af **EU-Kommissionens standardbestemmelser (SCC)** eller anden gyldig overførselsmekanisme.

Databehandleren fører kontrol med datamiljøet og gennemfører periodiske sikkerhedsvurderinger og opdateringer for at sikre fortsat compliance og stabil drift.

_____  _____

[Kundens navn] Bahlou ApS

Dato: _____ Dato: 03.02.2026