



DATABESKYTTELSE · GDPR ARTIKEL 28

Databehandlersaftale

mellem Bahlou ApS og den dataansvarlige

VERSION 2.0

2. september 2026

Bahlou ApS | CVR-nr. 44660342

Arne Jacobsens Allé 7, 2. · 2300 København S

Indholdsfortegnelse

Oversigten følger aftalens struktur og integrerede bilag.

1. Indledning og formål	3
2. Definitioner, forrang og ansvar	3
3. Den dataansvarliges forpligtelser	3
4. Databehandlerens forpligtelser og instruks	4
5. Fortrolighed	4
6. Behandlingssikkerhed	4
7. Underdatabehandlere	5
8. Overførsel til tredjelande	5
9. Bistand til den dataansvarlige	5
10. Brud på persondatasikkerheden	6
11. Returnering, sletning og ophør	6
12. Dokumentation, revision og kontrol	7
13. Kontakt, ændringer og ikrafttræden	7
Bilag A - Beskrivelse af behandlingen	8
Bilag B - Underdatabehandlere og tredjelandsoverførsler	10
Bilag C - Instruks og sikkerhedsforanstaltninger	11
Underskrifter	13

1. Indledning og formål

Denne databehandleraftale ("Aftalen") er indgået mellem:

Den dataansvarlige	Virksomhedsnavn: _____ CVR-nr.: _____ Adresse: _____
Databehandleren	Bahlou ApS, CVR-nr. 44660342, Arne Jacobsens Allé 7, 2., 2300 København S ("Bahlou")

Aftalen regulerer Bahlous behandling af personoplysninger på vegne af den dataansvarlige i forbindelse med levering af Bahlou-platformen og de funktioner, som den dataansvarlige vælger at anvende.

Formålet er at sikre, at behandlingen sker i overensstemmelse med Europa-Parlamentets og Rådets forordning (EU) 2016/679 (GDPR), særligt artikel 28, stk. 3, samt relevant national databeskyttelseslovgivning.

Aftalen udgør en del af parternes hovedaftale. Bilag A-C er en integreret del af Aftalen. Aftalen kan indgås og opbevares elektronisk.

2. Definitioner, forrang og ansvar

2.1 Definitioner

- **Personoplysninger:** enhver form for information om en identificeret eller identificerbar fysisk person, jf. GDPR artikel 4, nr. 1.
- **Behandling:** enhver aktivitet omfattet af GDPR artikel 4, nr. 2, herunder indsamling, registrering, opbevaring, videregivelse og sletning.
- **Underdatabehandler:** en tredjepart, som Bahlou engagerer til at behandle personoplysninger på vegne af den dataansvarlige.
- **Tredjeland:** et land uden for EU/EØS.

2.2 Forrang

Ved uoverensstemmelse har denne Aftale forrang alene for så vidt angår parternes databeskyttelsesretlige forpligtelser. Hovedaftalens bestemmelser om blandt andet betaling, misligholdelse, ansvar, ansvarsbegrænsning, lovvalg og værneting gælder fortsat, medmindre andet udtrykkeligt fremgår af denne Aftale eller følger af ufravigelig ret.

2.3 Ingen udvidelse af ansvar

Aftalen udvider ikke parternes ansvar ud over, hvad der følger af GDPR, anden ufravigelig lovgivning og hovedaftalen. Intet i Aftalen begrænser en tilsynsmyndigheds beføjelser eller registreredes rettigheder.

3. Den dataansvarliges forpligtelser

Den dataansvarlige bestemmer formål og væsentlige hjælpemidler for behandlingen og er ansvarlig for, at behandlingen er lovlig. Den dataansvarlige skal blandt andet:

- sikre et gyldigt behandlingsgrundlag og, hvor relevant, et gyldigt grundlag efter GDPR artikel 9 og dansk ret,
- opfylde oplysningspligten over for de registrerede,
- sikre, at de oplysninger og instrukser, der gives til Bahlou, er lovlige, relevante og nødvendige,
- konfigurere brugerroller og adgange forsvarligt og sikre, at egne brugere beskytter loginoplysninger og anvender tilgængelige sikkerhedsfunktioner,
- holde egne kontaktoplysninger og sikkerhedskontakter opdaterede, og
- uden unødigt forsinkelse orientere Bahlou om forhold, der kan påvirke sikkerheden eller lovligheden af behandlingen.

Bahlou er ikke ansvarlig for den dataansvarliges behandlingsgrundlag, journalføringspligt, opbevaringsperioder eller handlinger foretaget af den dataansvarliges autoriserede brugere, medmindre ansvaret følger af Bahlous egne forpligtelser efter ufravigelig ret eller hovedaftalen.

4. Databehandlerens forpligtelser og instruks

Bahlou behandler alene personoplysninger efter dokumenteret instruks fra den dataansvarlige. Aftalen, bilagene, den dataansvarliges dokumenterede konfiguration og lovlige anvendelse af platformen udgør den løbende instruks.

Bahlou må ikke anvende personoplysningerne til egne formål. Bahlou underretter straks den dataansvarlige, hvis en instruks efter Bahlous vurdering er i strid med GDPR eller anden relevant databeskyttelseslovgivning. Bahlou kan sætte den berørte behandling i bero, indtil instruksen er ændret eller lovligheden er dokumenteret.

Instrukser, der går ud over den aftalte funktionalitet eller kræver væsentlige tekniske eller organisatoriske ændringer, forudsætter særskilt aftale om gennemførelse, tid og eventuelle omkostninger. Dette begrænser ikke Bahlous lovpligtige bistand efter GDPR.

5. Fortrolighed

Bahlou sikrer, at personer med adgang til personoplysninger:

- er underlagt lovpligtig eller kontraktuel fortrolighed,
- kun har adgang, når det er nødvendigt for deres arbejdsopgaver, og
- har modtaget relevante instruktioner om databeskyttelse og informationssikkerhed.

Adgang ophører eller ændres, når arbejdsopgaven eller tilknytningen ikke længere begrundes den. Bahlou kan dokumentere de overordnede rammer for disse forpligtelser uden at udlevere fortrolige personaleoplysninger.

6. Behandlingssikkerhed

Bahlou gennemfører passende tekniske og organisatoriske foranstaltninger efter GDPR artikel 32 under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål samt de konkrete risici. De aftalte minimumsforanstaltninger fremgår af Bilag C.

Bahlou kan ændre foranstaltningerne som følge af teknisk udvikling eller ændret risikobillede, forudsat at det samlede beskyttelsesniveau ikke væsentligt forringes. Den dataansvarlige kan

anmode om yderligere foranstaltninger; sådanne foranstaltninger kræver særskilt skriftlig aftale, hvis de går ud over Bahlous standardleverance eller medfører væsentlige omkostninger.

7. Underdatabehandlere

Den dataansvarlige giver generel skriftlig godkendelse til de underdatabehandlere, der er identificeret i Bilag B.

Bahlou underretter aktivt den dataansvarlige elektronisk mindst 30 dage før en planlagt tilføjelse eller udskiftning af en direkte underdatabehandler. Underretningen skal give tilstrækkelige oplysninger om identitet, funktion, behandlingslokation og eventuelt overførselsgrundlag til, at den dataansvarlige kan vurdere ændringen.

Den dataansvarlige kan inden fristens udløb gøre skriftlig, konkret og sagligt begrundet indsigelse af databeskyttelsesmæssige grunde. Parterne søger i rimeligt omfang en løsning. Hvis en løsning ikke kan findes, kan Bahlou vælge ikke at anvende underdatabehandleren, tilbyde en rimelig alternativ løsning mod eventuel merbetaling eller opsigelse den berørte del af tjenesten med 30 dages varsel uden ansvar for indirekte tab. Manglende rettidig indsigelse betragtes som godkendelse.

Bahlou pålægger underdatabehandleren databeskyttelsesforpligtelser, der i det væsentlige svarer til Bahlous forpligtelser efter denne Aftale, og Bahlou er over for den dataansvarlige ansvarlig for underdatabehandlerens opfyldelse i overensstemmelse med GDPR artikel 28, stk. 4.

8. Overførsel til tredjelande

Bahlou må kun overføre eller give fjernadgang til personoplysninger uden for EU/EØS efter en klar, dokumenteret instruks og et gyldigt overførselsgrundlag efter GDPR kapitel V. Godkendte modtagere og relevante overførselsgrundlag fremgår af Bilag B.

En generel eller uafgrænset formulering om mulige overførsler til ikke-angivne tredjelande udgør ikke i sig selv en instruks. Bahlou må alene fravige instruks, hvis behandlingen kræves i henhold til EU-retten eller en medlemsstats nationale ret, der gælder for Bahlou. Bahlou underretter i så fald den dataansvarlige før behandlingen, medmindre den pågældende ret forbyder underretning af hensyn til vigtige samfundsmæssige interesser.

Hvis et anvendt overførselsgrundlag ændres eller bortfalder, kan Bahlou erstatte det med et andet gyldigt grundlag og nødvendige supplerende foranstaltninger. Den dataansvarlige orienteres om væsentlige ændringer efter proceduren i afsnit 7.

9. Bistand til den dataansvarlige

Under hensyntagen til behandlingens karakter og de oplysninger, Bahlou råder over, bistår Bahlou den dataansvarlige med:

- besvarelse af anmodninger om registreredes rettigheder efter GDPR kapitel III,
- overholdelse af forpligtelserne i GDPR artikel 32-36, herunder sikkerhed, brud, konsekvensanalyser og eventuel forhåndshøring, og
- oplysninger, der er nødvendige for at påvise overholdelse af GDPR artikel 28.

Almindelig bistand, som kan ydes gennem Bahlous standardfunktionalitet eller følger direkte af Bahlous egne lovpligtige forpligtelser, er inkluderet. Ekstraordinært arbejde, der skyldes den

dataansvarliges særlige instrukser, manglende efterlevelse eller behov uden for standardfunktionaliteten, kan faktureres efter medgået tid og gældende sats. Bahlou giver så vidt muligt et estimat på forhånd; dette gælder ikke, hvis akut handling er nødvendig for at begrænse et sikkerhedsbrud.

10. Brud på persondatasikkerheden

Bahlou underretter den dataansvarlige uden unødigt forsinkelse og tilstræber underretning senest 24 timer efter, at Bahlou er blevet bekendt med et brud på persondatasikkerheden, der berører oplysninger omfattet af Aftalen.

En foreløbig underretning kan gives, selv om alle oplysninger endnu ikke foreligger. Bahlou fremsender supplerende oplysninger uden unødigt forsinkelse, efterhånden som de bliver tilgængelige. Underretningen skal, i det omfang oplysningerne er tilgængelige, indeholde:

- bruddets karakter, herunder berørte kategorier og omtrentligt antal registrerede og registreringer,
- kontaktpunkt for yderligere oplysninger,
- sandsynlige konsekvenser, og
- trufne eller foreslåede afhjælpende foranstaltninger.

Underretning efter dette afsnit er ikke i sig selv en anerkendelse af ansvar. Den dataansvarlige er ansvarlig for vurdering og eventuel anmeldelse til tilsynsmyndigheden og de registrerede, mens Bahlou yder den aftalte bistand.

11. Returnering, sletning og ophør

Ved behandlingens ophør skal Bahlou efter den dataansvarliges dokumenterede valg returnere personoplysningerne i et struktureret og almindeligt anvendt format og/eller slette dem, medmindre EU-ret eller dansk ret kræver fortsat opbevaring.

Den dataansvarlige skal anmode om et tilgængeligt standardudtræk senest 30 dage efter hovedaftalens ophør. Specialudtræk, konvertering eller migreringsbistand ud over standardfunktionaliteten kan faktureres efter særskilt aftale.

Bahlou kan opretholde en begrænset afviklingsperiode på op til 90 dage efter ophør med henblik på udtræk, tvister, sikker afvikling og sletning. Herefter slettes produktionsdata, medmindre andet er aftalt eller følger af lov. Data i backups isoleres fra almindelig brug og slettes eller overskrives efter Bahlous dokumenterede backupcyklus. Den normale maksimale backup-retention er 30 dage; teknisk endelig overskrivning gennemføres senest 60 dage efter, at data er udgået af den aktive backupcyklus.

Den dataansvarlige er ansvarlig for at sikre lovpligtig opbevaring af journaler og andre oplysninger. Bahlou har ikke en selvstændig pligt til at fastlægge eller håndhæve den dataansvarliges opbevaringsperioder. Hvis fortsat opbevaring hos Bahlou ønskes efter ophør, kræver det en særskilt skriftlig aftale og instruks.

12. Dokumentation, revision og kontrol

Bahlou stiller de oplysninger til rådighed, som er nødvendige for at påvise efterlevelse af GDPR artikel 28. Kontrol gennemføres som udgangspunkt dokumentbaseret og kan understøttes af relevante tredjepartserklæringer, certificeringer, sikkerhedsbeskrivelser eller spørgeskemaer.

Den dataansvarlige kan som udgangspunkt gennemføre én kontrol pr. 12-månedersperiode. Begrænsningen gælder ikke ved et væsentligt sikkerhedsbrud, konkret dokumenteret mistanke om væsentlig manglende efterlevelse eller bindende krav fra en kompetent myndighed.

Inspektion på stedet kræver mindst 30 dages skriftligt varsel, medmindre kortere varsel er nødvendigt på grund af et sikkerhedsbrud eller myndighedskrav. Inspektionen skal ske inden for normal arbejdstid, være rimeligt afgrænset, udføres af en uafhængig og fortrolighedsforpligtet person og må ikke give adgang til andre kunders oplysninger, kildekode, sikkerhedshemmeligheder eller oplysninger, som Bahlou ikke lovligt kan udlevere. Kontrollen må ikke unødigt forstyrre Bahlous drift.

Den dataansvarlige afholder egne og Bahlous rimelige omkostninger ved ekstraordinær kontrol og fysisk inspektion, medmindre kontrollen påviser en væsentlig overtrædelse, som kan henføres til Bahlou. Myndigheders lovlige kontrol begrænses ikke af dette afsnit.

13. Kontakt, ændringer og ikrafttræden

Meddelelser om underdatabehandlere, sikkerhedsbrud og databeskyttelse sendes til parternes registrerede kontaktpersoner. Den dataansvarlige skal sikre, at kontaktoplysningerne er korrekte og overvåges.

Bahlous kontakt for databeskyttelse og sikkerhedsbrud er support@bahlou.dk. Henvendelser til adressen overvåges og håndteres efter Bahlous interne beredskabsprocedure.

Bahlou kan opdatere Bilag B efter proceduren i afsnit 7 og Bilag C for at afspejle faktiske tekniske og organisatoriske ændringer, hvis beskyttelsesniveauet ikke væsentligt forringes. Andre væsentlige ændringer kræver skriftlig aftale.

Aftalen træder i kraft ved parternes accept og gælder, så længe Bahlou behandler personoplysninger på vegne af den dataansvarlige. Hovedaftalens lovvalg og værneting gælder. Hvis hovedaftalen ikke regulerer dette, er Aftalen underlagt dansk ret med Københavns Byret som aftalt værneting, medmindre ufravigelig ret bestemmer andet.

Bilag A - Beskrivelse af behandlingen

A1. Formål

Formålet er at levere de Bahlou-funktioner, som den dataansvarlige aktiverer og anvender, herunder:

- online booking, kalender, kunde- og medarbejderadministration,
- journalføring og behandlingsdokumentation, herunder billeder og skabeloner,
- kommunikation via e-mail og SMS,
- betaling, fakturering, gavekort, klippekort og relaterede transaktioner, hvor funktionerne anvendes,
- markedsføringsfunktioner og segmentering efter den dataansvarliges aktivering og instruks,
- integrationer, import, eksport og migrering, og
- drift, sikkerhed, vedligeholdelse, support og fejlsøgning.

Bahlou behandler ikke oplysningerne til egne markedsførings-, analyse- eller produktudviklingsformål, medmindre oplysningerne er reelt og irreversibelt anonymiserede, eller der foreligger et særskilt lovligt grundlag og en tydelig rollefordeling uden for denne Aftale.

A2. Kategorier af personoplysninger

Almindelige oplysninger

- navn, adresse, telefonnummer, e-mailadresse, fødselsdato, køn og sprog,
- kunde-, booking-, behandlings- og kommunikationshistorik,
- samtykke- og præferenceoplysninger,
- medarbejder-, bruger-, rolle- og kalenderoplysninger, og
- tekniske oplysninger som IP-adresse, enhed, tidsstempler og logdata.

Fortrolige og nationalt regulerede oplysninger

- CPR-nummer eller andet nationalt identifikationsnummer, når den dataansvarlige anvender funktioner, der kræver det, og
- økonomiske oplysninger, fakturadata og transaktionsoplysninger, men ikke fulde kortoplysninger, medmindre andet særskilt er aftalt.

Særlige kategorier efter GDPR artikel 9

- journalnotater og helbredsoplysninger,
- oplysninger om udførte eller planlagte behandlinger, kontraindikationer og særlige helbredshensyn,
- billeder og anden behandlingsdokumentation, og
- oplysninger, der indirekte kan afsløre helbredsforhold.

A3. Kategorier af registrerede

- klinikkens patienter, kunder og potentielle kunder, hvis oplysninger registreres i platformen,
- klinikkens medarbejdere, behandlere, læger, administratorer og andre autoriserede brugere,
- kontaktpersoner, ejere og repræsentanter hos den dataansvarlige, og
- andre personer, hvis oplysninger lovligt registreres af den dataansvarlige i forbindelse med de valgte funktioner.

A4. Behandlingens karakter

Behandlingen kan omfatte indsamling, registrering, strukturering, opbevaring, visning, søgning, sammenstilling, ændring, transmission efter instruks, begrænsning, eksport, sikkerhedskopiering, gendannelse, anonymisering og sletning. Automatisk behandling sker alene som led i aktiverede funktioner og dokumenteret instruks.

A5. Varighed

Behandlingen sker under hovedaftalens løbetid og i den afviklings- og backupperiode, der følger af afsnit 11. Bahlou kan suspendere adgang ved misligholdelse efter hovedaftalen uden at ændre parternes databeskyttelsesretlige forpligtelser.

Bilag B - Underdatabehandlere og tredjelandsoverførsler

Ved Aftalens ikrafttræden har den dataansvarlige godkendt brugen af følgende underdatabehandlere:

LEVERANDØR	CVR / REG.NR.	ADRESSE	BEHANDLING
ONLINECITY.IO ApS	27364276	Buchwaldsgade 50 5000 Odense C Danmark	SMS
DigitalOcean, LLC	5118787 (Delaware)	105 Edgeview Drive, Suite 425 Broomfield, CO 80021 USA	Hosting
Xmatiq Technologies	AAX 1439	C-702, Krish Cubical Thaltej, Ahmedabad 380059 Indien	Udvikling
Mailgun Technologies, Inc.	6297323 (Delaware)	112 E Pecan St, Suite 1135 San Antonio, TX 78205 USA	E-mail
Cloudflare, Inc.	Delaware corporation	101 Townsend St. San Francisco, CA 94107 USA	Sikkerhed

For underdatabehandlere etableret uden for EU/EØS eller med fjernadgang fra tredjelande sker overførsel alene på et gyldigt grundlag efter GDPR kapitel V. For certificerede amerikanske modtagere anvendes EU-U.S. Data Privacy Framework, og ellers EU-Kommissionens standardkontraktbestemmelser med relevante supplerende foranstaltninger.

Adgang fra Indien må først gives, når standardkontraktbestemmelsernes modul 2, en dokumenteret overførselsvurdering og relevante supplerende sikkerhedsforanstaltninger er på plads.

Bilag C - Instruks og sikkerhedsforanstaltninger

C1. Behandlingsinstruks og produktionsadgang

Bahlou behandler personoplysninger for at levere de valgte funktioner i Bilag A. Adgang til produktionsdata må alene ske, når det er nødvendigt for drift, sikkerhed, support, fejlsøgning, import eller migrering.

Udvikling og test udføres som udgangspunkt uden produktionsdata. Hvis produktionsdata undtagelsesvis er nødvendig, skal adgangen være dokumenteret, begrænset til mindst mulige data, tidsbegrænset, autoriseret og logget. Maskerede eller pseudonymiserede oplysninger behandles fortsat som personoplysninger. Kun reelt irreversible anonymiserede oplysninger kan anvendes uden for instruksen.

C2. Minimumsforanstaltninger

Styring og fortrolighed

- dokumenterede roller og ansvar for informationssikkerhed,
- fortrolighedsforpligtelser og relevant oplæring, og
- periodisk vurdering af risici og relevante sikkerhedsforanstaltninger.

Identitet og adgang

- personlige bruger- og administratorkonti, princippet om mindst mulig adgang og rettidig lukning af adgange,
- periodisk adgangsreview for privilegerede konti, og
- multifaktorgodkendelse for højrisikoadgang, herunder administrative konti og konti med adgang til journaldata, databaser, infrastruktur eller produktionsmiljø.

Kryptering

- kryptering af data under overførsel med tidssvarende TLS, og
- kryptering ved opbevaring for databaser, filopbevaring og backups samt begrænset adgang til kryptografiske nøgler.

Logning og sporbarhed

- logning af adgang til og væsentlige ændringer i journaloplysninger, privilegerede handlinger og relevante sikkerhedshændelser,
- beskyttelse af logs mod uautoriseret ændring og adgang, og
- opbevaring af relevante auditlogs i 24 måneder, medmindre et dokumenteret formål eller lovkrav begrunder en anden periode.

Backup og beredskab

- regelmæssig backup med adgangsbegrænsning og adskillelse fra produktionsmiljøet,
- dokumenterede gendannelsesprocedurer og periodiske restore-tests, og
- en dokumenteret backup- og gendannelsesplan med risikobaserede mål for datatab og genetablering samt maksimal normal backup-retention på 30 dage.

Sikker udvikling og drift

- adskillelse af udviklings-, test- og produktionsmiljøer, hvor det er relevant,
- ændringsstyring, kodegennemgang og begrænset produktionsadgang, og
- risikobaseret sårbarhedshåndtering: kritiske sikkerhedsrettelser gennemføres hurtigst muligt og som udgangspunkt inden for 24-72 timer, højrisikoforhold inden for 7 dage og øvrige forhold efter dokumenteret risikovurdering.

Hændelser og kontinuitet

- procedurer for identifikation, begrænsning, dokumentation og opfølgning på sikkerhedshændelser, og
- beredskab for gendannelse af tilgængelighed og adgang til personoplysninger efter en fysisk eller teknisk hændelse.

C3. Support og tredjemarksadgang

Support- og udviklingsadgang sker gennem autentificerede forbindelser og kontrollerede konti. Adgang skal være behovsbaseret og må ikke deles mellem personer. Tredjemarksadgang må alene ske fra en identificeret juridisk enhed og lokation i Bilag B og på det dér angivne overførselsgrundlag.

Produktionsadgang godkendes alene af Bahlous ejere og tildeles navngivne personer med mindst mulige rettigheder. Adgangen gælder normalt højst 24 timer eller den kortere tid, opgaven varer, lukkes automatisk eller straks efter opgaven og kræver ny godkendelse ved forlængelse. Tildeling og brug af adgangen logges, og relevante logs kontrolleres som led i Bahlous sikkerhedsopfølgning.

C4. Hosting og datalokation

Bahlou anvender DigitalOcean til hosting og infrastruktur. Adgang til produktionsmiljøet begrænses efter princippet om mindst mulig adgang og kræver autorisation efter C3. Leverandørens support får kun adgang, når det er nødvendigt for at levere eller sikre tjenesten. Relevante underdatabehandlere i leverandørkæden er omfattet af kravene i afsnit 7 og 8.

C5. Tilsyn med underdatabehandlere

Bahlou vurderer før brug og derefter risikobaseret, om underdatabehandlere stiller tilstrækkelige garantier. Tilsynet kan baseres på kontrakter, sikkerhedsdokumentation, certificeringer, revisionserklæringer, spørgeskemaer og afhjælpningsplaner. Væsentlige mangler følges op, og anvendelsen ophører eller begrænses, hvis et tilstrækkeligt beskyttelsesniveau ikke kan opretholdes.

Underskrifter

Aftalen kan underskrives elektronisk. Ved underskrift bekræfter parterne den version, der er identificeret på forsiden.

For den dataansvarlige

Virksomhed: _____

Navn: _____

Dato: _____

Underskrift: _____

For Bahlou ApS

Bahlou ApS

Navn: Bilal Kær Shareef

Dato: 02/09-2026

Underskrift:  _____