Bahlou

DATABESKYTTELSE · GDPR ARTIKEL 28

Databehandleraftale

mellem Bahlou ApS og den dataansvarlige

VERSION 2.1

25. november 2026

Bahlou ApS · CVR-nr. 44660342

Arne Jacobsens Allé 7, 2. · 2300 København S

Indholdsfortegnelse

1. Indledning og formål 3
2. Definitioner, forrang og ansvar 3
3. Den dataansvarliges forpligtelser 4
4. Databehandlerens forpligtelser og instruks 4
5. Fortrolighed 4
6. Behandlingssikkerhed 5
7. Underdatabehandlere 5
8. Overførsel til tredjelande 5
9. Bistand til den dataansvarlige 6
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
C6. CPR-opslag via CPR-administrationen 13
C7. Chat og maskering 14
C8. Kundevalgte webhooks til eksterne systemer 14
Underskrifter 15

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

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 unødig forsinkelse orientere Bahlou om forhold, der kan påvirke sikkerheden eller lovligheden af behandlingen.

Den dataansvarlige har ansvaret for sit behandlingsgrundlag, sin journalføringspligt, sine opbevaringsperioder og den brug, som egne autoriserede brugere gør af oplysningerne. Bahlou har ansvar for sine egne handlinger og undladelser, herunder overholdelse af dokumenteret instruks, aftalte sikkerhedsforanstaltninger og håndtering af persondatasikkerhedsbrud.

4. Databehandlerens forpligtelser og instruks

Bahlou behandler alene personoplysninger efter dokumenteret instruks fra den dataansvarlige. Aftalen, bilagene og den dataansvarliges dokumenterede valg og konfiguration inden for de aftalte funktioner udgør den løbende instruks. Bilag C fastsætter de særlige instrukser for CPR-opslag, chat og kundevalgte webhooks.

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 begrunder 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 Bahlous brug af de underdatabehandlere, der er angivet i Bilag B, for de angivne ydelser og på de angivne betingelser.

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. Manglende rettidig indsigelse betragtes som godkendelse. Ved rettidig indsigelse afklarer parterne forholdet, før leverandøren behandler den dataansvarliges oplysninger. Hvis en løsning ikke kan findes, kan Bahlou undlade at anvende leverandøren, tilbyde en rimelig alternativ løsning mod eventuel merbetaling eller opsige den berørte del af tjenesten med 30 dages varsel uden ansvar for indirekte tab.

Bahlou pålægger ved skriftlig aftale underdatabehandleren de samme databeskyttelsesforpligtelser, som gælder for den relevante behandling efter denne Aftale. Bahlou er fuldt ansvarlig over for den dataansvarlige for underdatabehandlerens opfyldelse af disse forpligtelser, jf. GDPR artikel 28, stk. 4.

Bahlou holder identitet og kontaktoplysninger for relevante led i leverandørkæden tilgængelige for den dataansvarlige og informerer om relevante ændringer, så den dataansvarlige kan vurdere dem og gøre indsigelse inden brug. For Bahlous direkte underdatabehandlere gælder fristen på mindst 30 dage.

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 instruksen, 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, sætter Bahlou overførslen i bero, medmindre overførslen kan fortsætte på et andet gyldigt grundlag med de nødvendige supplerende foranstaltninger og en dokumenteret instruks. 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, medmindre akut handling er nødvendig for at begrænse et sikkerhedsbrud.

10. Brud på persondatasikkerheden

Bahlou underretter den dataansvarlige uden unødig 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 unødig 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.

Ved hændelser vedrørende CPR-opslag gælder også Bilag C6 og Bahlous eventuelle underretningspligter efter aftalen med CPR-administrationen.

11. Returnering, sletning og ophør

Ved behandlingens ophør sletter Bahlou personoplysningerne eller returnerer dem efter den dataansvarliges dokumenterede valg. Ved returnering leveres oplysningerne i et struktureret og almindeligt anvendt format, hvorefter Bahlou sletter de eksisterende kopier. Hvis EU-ret eller en medlemsstats nationale ret kræver opbevaring, begrænser Bahlou behandlingen til det lovpligtige formål og den krævede periode.

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 i det omfang, det er nødvendigt for aftalt udtræk, sikker afvikling og sletning. 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 eller en revisor bemyndiget af denne kan som udgangspunkt gennemføre én ordinær kontrol pr. 12-månedersperiode. Bahlou giver mulighed for og bidrager til yderligere revision og inspektion, når det er nødvendigt for at kontrollere efterlevelsen af GDPR artikel 28, herunder ved sikkerhedsbrud, begrundet mistanke om manglende efterlevelse eller myndighedskrav.

Inspektion på stedet kræver som udgangspunkt 30 dages skriftligt varsel. Varslet forkortes, når omstændighederne kræver det. Inspektionen skal være rimeligt afgrænset og gennemføres af den dataansvarlige eller en bemyndiget revisor under passende krav til fortrolighed og beskyttelse af andre kunders oplysninger. Parterne tilrettelægger kontrollen, så den kan gennemføres effektivt med mindst mulig forstyrrelse af driften.

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.

For eksisterende kundeforhold træder version 2.1 i kraft ved parternes dokumenterede accept. Nye underdatabehandlere for eksisterende kunder håndteres efter den allerede gældende aftales procedure, jf. afsnit 7.

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, herunder kundevalgte webhooks efter C8, samt import, eksport og migrering,
- CPR-opslag efter særskilt ansøgning, godkendelse og aktivering, jf. C6,
- besvarelse af henvendelser via platformens aktiverede chatfunktion, jf. C7, 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

- den dataansvarliges patienter, kunder, potentielle kunder og brugere af chat- og bookingfunktioner,
- den dataansvarliges 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.

A6. Supplerende beskrivelse af valgte funktioner

CPR-opslag

Behandlingen omfatter forespørgsler ved brug af personnummer, visning af de oplysninger, som CPR kan udlevere i den godkendte løsning, og eventuel registrering i den relevante kundepost efter instruks. Oplysningerne kan omfatte navn, adresse og fødselsdato, hvor det pågældende felt udleveres og er nødvendigt. Der behandles også oplysninger om ansøgning, autorisation og brug til dokumentation og kontrol efter C6.

Chat

Behandlingen omfatter gennemgang og maskering af chatindhold, udvælgelse af den kontekst, der er nødvendig for at svare, samt behandling af maskeret tekst og nødvendige tekniske metadata i overensstemmelse med C7.

Kundevalgte webhooks

Behandlingen omfatter afsendelse af de aftalte hændelser og felter til modtagere, som den dataansvarlige vælger. Ved ekstern måling og markedsføring begrænses felterne efter C8.

Bilag B - Underdatabehandlere og tredjelandsoverførsler

B1. Direkte underdatabehandlere

Den dataansvarlige godkender ved Aftalens ikrafttræden brugen af nedenstående leverandører til de angivne formål og under betingelserne i B2.

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
OpenAI Ireland Ltd.	737350 (Irland)	1st Floor, The Liffey Trust Centre 117-126 Sheriff Street Upper Dublin 1, D01 YC43, Irland	Chat og behandling af maskeret tekst efter C7

CPR-administrationen er den offentlige registerkilde for CPR-opslag, jf. C6. Kundevalgte webhookmodtagere håndteres efter C8.

B2. Behandlingslande og overførselsgrundlag

Bahlou holder en opdateret skriftlig oversigt til dette bilag over de faktiske behandlingslande, herunder hosting og fjernadgang, modtagere og det konkrete overførselsgrundlag pr. relevant ydelse. En leverandørs adresse i listen angiver dens etablering. Oversigten omfatter de relevante underliggende leverandører og stilles til rådighed for den dataansvarlige. En tredjelandsoverførsel kræver den dokumenterede instruks efter afsnit 8.

Ved overførsel til en amerikansk modtager kan EU-U.S. Data Privacy Framework anvendes, hvis den relevante juridiske enhed har en aktiv certificering, der dækker behandlingen. Når overførslen baseres på EU-Kommissionens standardkontraktbestemmelser, skal Bahlou sikre korrekt modul, dokumenteret overførselsvurdering og nødvendige supplerende foranstaltninger. Direkte fjernadgang fra Indien på Bahlous vegne er betinget af modul 3 for overførsel fra databehandler til underdatabehandler og disse øvrige krav.

OpenAI Ireland Ltd. er etableret i Irland. Før OpenAI behandler personoplysninger for den dataansvarlige, skal Bahlou dokumentere den relevante OpenAI-aftale og konfiguration, herunder behandlings- og supportlande, opbevaring og eventuelle videreoverførsler efter OpenAIs databehandleraftale og GDPR kapitel V. Kravene i afsnit 7, 8 og C7 gælder.

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 nødvendige, skal adgangen være dokumenteret, begrænset til mindst mulige data, tidsbegrænset, autoriseret og logget. Maskerede eller pseudonymiserede oplysninger behandles fortsat som personoplysninger, når de kan henføres til en person. Oplysninger må anvendes uden for instruksen, hvis de er reelt og irreversibelt anonymiserede.

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 tredjelandsadgang

Support- og udviklingsadgang sker gennem autentificerede forbindelser og kontrollerede konti. Adgang skal være behovsbaseret og må ikke deles mellem personer. Tredjelandsadgang må alene ske for identificerede juridiske enheder og lokationer og på det grundlag, der er dokumenteret efter Bilag B og afsnit 8.

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.

C6. CPR-opslag via CPR-administrationen

Bahlou foretager kun CPR-opslag på den dataansvarliges vegne via sin direkte tilslutning til CPR-administrationen og inden for den konkrete adgangsaftale med CPR-administrationen. CPR-opslag bruges til det dokumenterede og godkendte formål for den relevante juridiske enhed.

Ansøgning og aktivering

En bemyndiget ejer eller administrator ansøger pr. juridisk enhed og CVR-nummer. Ansøgningen angiver den relevante persongruppe, opslagets konkrete formål og nødvendighed, behandlingsgrundlaget, kontaktpersonen og den sikkerhedsansvarlige. Ansøgningen må ikke indeholde personnumre eller patientoplysninger. Ansøgeren accepterer de gældende, versionsangivne vilkår for CPR-opslag. Bahlou registrerer ansøgningen, vilkårsversionen, hvem der accepterede og hvornår, samt Bahlous afgørelse.

Bahlou gennemgår ansøgningen og kan indhente supplerende oplysninger eller afslå den. Funktionen kan først aktiveres, når Bahlou har godkendt formålet, kontrolleret at den konkrete CPR-aftale dækker kundens brug, og sikret, at eventuelle krav om kundespecifik registrering eller godkendelse hos CPR-administrationen er opfyldt. Den godkendte ansøgning dokumenterer den dataansvarliges instruks. Ved væsentlige ændringer skal den dataansvarlige orientere Bahlou og indhente fornyet godkendelse før brug til det ændrede formål.

Den dataansvarliges brug og kontrol

Den dataansvarlige fastlægger og dokumenterer behandlingsgrundlaget efter GDPR artikel 6 og overholder databeskyttelseslovens § 11 ved behandling af personnummer. Den dataansvarlige sikrer desuden, at CPR-reglerne er overholdt. Hvert opslag og den efterfølgende brug skal være nødvendige for det godkendte formål. Private opslag, uvedkommende søgninger, markedsføring og masseopslag via funktionen er forbudt. Oplysninger må kun videregives inden for de regler og adgangsvilkår, der gælder for CPR. Den dataansvarlige tildeler adgang til navngivne medarbejdere med arbejdsbetinget behov, fjerner den straks ved ophør og fører løbende kontrol sammen med sin sikkerhedsansvarlige.

Bahlous adgangskontrol, logning og reaktion

Bahlou kontrollerer aktiv virksomhedsgodkendelse og den enkelte brugers CPR-rettighed på serveren ved hvert opslag. Adgangen er slået fra som standard og er underlagt personlig adgang, multifaktorgodkendelse og de IP- og øvrige tekniske krav for den konkrete adgang. Bahlou fører en fortegnelse over autorisationer og registrerer virksomhed, bruger, tidspunkt, formål, transaktionstype og status for opslaget. Almindelige applikationslogs må ikke indeholde personnumre eller CPR-svar.

Bahlou sikrer afgrænset adgang til kontroloplysninger om den enkelte virksomhed og månedlig statistik fordelt på transaktionstyper. Parterne kontrollerer anvendelsen inden for deres respektive roller og CPR-vilkår. Bahlous sikkerhedsansvarlige kontrollerer den månedlige statistik. Opbevaring og sletning af CPR-specifikke logoplysninger følger en dokumenteret, formålsafgrænset frist, der respekterer de konkrete CPR-vilkår. Bahlou bistår med registreredes rettigheder og kan identificere den relevante dataansvarlige i det omfang, CPR-vilkårene kræver det.

Parterne orienterer hinanden uden unødig forsinkelse ved begrundet mistanke om misbrug. Bahlou kan straks blokere den berørte adgang ved risiko for misbrug, manglende dokumentation eller bortfald af adgangen hos CPR-administrationen. Bahlou håndterer egne forpligtelser efter afsnit 6, 8 og 10 og underretter CPR-administrationen, når de konkrete adgangsvilkår kræver det.

C7. Chat og maskering

Ved brug af chatfunktionen behandler Bahlou tekst og den nødvendige kontekst for at besvare henvendelser. Bahlou maskerer direkte identifikatorer inden afsendelse til den godkendte OpenAI-tjeneste og begrænser det afsendte til den tekst og de tekniske oplysninger, der er nødvendige for svaret. Bahlou skal holde eventuelle nøgler til genidentifikation adskilt og undlade at sende dem, personnumre, data fra CPR-opslag, journaloplysninger eller andre helbredsoplysninger til OpenAI. Hvis disse oplysninger ikke kan fjernes på betryggende vis, blokerer Bahlou afsendelsen af indholdet.

Bahlou behandler maskeret chatindhold som personoplysninger, så længe det kan henføres til en person. OpenAI anvendes i så fald som underdatabehandler efter Bilag B. Bahlou konfigurerer tjenesten, så indholdet ikke bruges til modeltræning, begrænser opbevaring til det, der er nødvendigt for funktionen og anvendte sikkerhedsformål, og dokumenterer samt afprøver maskeringen og konfigurationen.

C8. Kundevalgte webhooks til eksterne systemer

Den dataansvarliges dokumenterede valg af modtager, destination, hændelser og datafelter udgør instruksen til Bahlou om at afsende oplysninger via webhook. Bahlou har ansvar for sikker afsendelse efter instruksen. Hvis Bahlou foretager en tredjelandsoverførsel, dokumenteres modtager, land og overførselsgrundlag for den konkrete integration som led i instruksen efter afsnit 8.

Den dataansvarlige har ansvar for formålet, lovligheden af videregivelsen, oplysningspligt, eventuelt påkrævet samtykke samt valg og konfiguration af modtageren. Hvis modtageren behandler oplysninger på den dataansvarliges vegne, indgår den dataansvarlige den nødvendige databehandleraftale. Hvis modtageren behandler til egne formål eller formålet fastlægges i fællesskab, afklarer den dataansvarlige de relevante roller og forpligtelser. Den dataansvarlige håndterer krav vedrørende modtagerens efterfølgende behandling og eventuelle videreoverførsler.

Ved webhooks til ekstern markedsføring eller måling af markedsføring begrænser parterne overførslen til aftalte, nødvendige hændelser og felter. Bahlou må til disse formål ikke sende personnumre, data fra CPR-opslag, journaldata eller oplysninger, der kan afsløre helbredsforhold, herunder via behandlingsnavne, URL-parametre eller fritekst. En leverandør, som Bahlou selv engagerer til at behandle oplysninger for den dataansvarlige, er omfattet af afsnit 7.

Underskrifter

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

For den dataansvarlige		For Bahlou ApS	
Virksomhed		Virksomhed	Bahlou ApS
Navn		Navn	Bilal Kjær Shareef
Dato		Dato	25/11-2026
Underskrift		Underskrift	