Ocealis Ltd
Company no. 11788017 · www.ocealis.net

Version 1.1
29 October 2026

Data Processing Agreement

Processing of personal data under the Terms of Service

> **Document structure.** This DPA forms part of, and is incorporated into, the Ocealis **Terms of Service** ("Terms"). It governs the processing of personal data and **prevails over the Terms and the SLA on data-protection matters** (Terms clause 17.10). Capitalised terms not defined here have the meaning given in the Terms.

1. Parties and roles

1.1 This DPA is between **Ocealis Ltd** (company number **11788017**), trading as Ocealis ("Processor", "we"), and the Customer ("Controller", "you").

1.2 In respect of personal data within Customer Data, **you are the Controller and we are the Processor**. You determine the purposes and means of processing; we process on your behalf.

1.3 Where we engage another organisation to process personal data on our behalf, that organisation is a **Sub-processor** (clause 6).

2. Definitions

2.1 **"Data Protection Law"** means the UK GDPR, the Data Protection Act 2018, and other applicable data-protection law as amended.

2.2 **"Personal Data"**, **"processing"**, **"data subject"**, **"personal data breach"**, **"controller"**, and **"processor"** have the meanings in Data Protection Law.

2.3 **"Customer Personal Data"** means Personal Data within Customer Data processed by us under the Terms.

2.4 Details of the processing are set out in **Annex 1**; our security measures in **Annex 2**; and authorised Sub-processors in **Annex 3**.

3. Processing instructions

3.1 We will process Customer Personal Data only on your documented instructions, including as set out in the Terms, this DPA, and your use and configuration of the Service, unless required to do otherwise by law (in which case we will inform you unless legally prohibited).

3.2 We will inform you if, in our opinion, an instruction infringes Data Protection Law.

3.3 You confirm that you have a lawful basis for the processing and for providing Customer Personal Data to us, that (where you include special category data) a condition under Article 9 of the UK GDPR applies, and that you have provided any required notices to data subjects (including crew).

4. Confidentiality and personnel

4.1 We ensure that persons authorised to process Customer Personal Data are bound by appropriate confidentiality obligations and have received appropriate data-protection training, and we limit access on a least-privilege basis.

5. Security

5.1 We implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, as required by Article 32 of the UK GDPR. Our measures are described in **Annex 2** and include encryption in transit and at rest, encrypted local storage on Bridge devices, per-device authentication, tenant isolation, access controls, and backups.

5.2 We will not materially reduce the overall level of security of the Service during the term.

6. Sub-processors

6.1 You provide **general authorisation** for us to engage Sub-processors to process Customer Personal Data. Current Sub-processors are listed in **Annex 3**.

6.2 We will impose data-protection obligations on each Sub-processor that are no less protective than those in this DPA, and we remain liable to you for each Sub-processor's performance.

6.3 We will give you notice of any intended addition or replacement of a Sub-processor **at least 30 days in advance, by email or in-product notice**. If you reasonably object on data-protection grounds, we will work with you in good faith to address the concern; if we cannot, you may terminate the affected part of the Service.

7. International transfers

7.1 Customer Personal Data is hosted and stored at rest within the United Kingdom, and model processing for Pilot is performed within the United Kingdom and/or the European Economic Area.

7.2 To respond to queries, Pilot transmits data to third-party AI providers for processing within the UK and/or EEA: (a) query text and entity reference vocabulary (including vessel and crew names) and the results of database queries, which may include personal data, are sent to Amazon Web Services for inference using Anthropic Claude models via Amazon Bedrock in a UK/EU region (Anthropic does not receive this data); and (b) where the Customer uses document indexing, document content is sent to OpenAI's API under UK/European data residency for embedding. Personal data transmitted is limited to that necessary to fulfil the relevant query or feature.

7.3 Restricted transfers. Certain Sub-processors are, or are part of groups, established outside the UK (including in the United States) and may access Customer Personal Data from outside the UK for limited purposes such as support, maintenance, and security operations, or process limited service metadata outside the UK. Any such restricted transfer is made under an appropriate safeguard recognised by Data Protection Law, being the UK–US Data Bridge (where the recipient is certified), the UK International Data Transfer Agreement, or the UK Addendum to the EU Standard Contractual Clauses, as set out in the relevant Sub-processor's data processing terms. We will make details of the applicable safeguards available on request.

7.4 No training and retention. Customer Personal Data transmitted to the AI providers is not used by them to train or improve their models, in accordance with their respective commercial terms, and where configured, model requests and responses are not retained at rest.

8. Assisting the Controller

8.1 Taking into account the nature of the processing, we will assist you by appropriate technical and organisational measures, insofar as possible, in fulfilling your obligations to respond to data-subject requests under Chapter III of the UK GDPR.

8.2 We will assist you in ensuring compliance with your obligations under Articles 32–36 (security, breach notification, data-protection impact assessments, and prior consultation), taking into account the information available to us.

9. Data-subject rights

9.1 Where we receive a request directly from a data subject (for example, a crew member) relating to Customer Personal Data, we will not respond directly but will, without undue delay, inform you so that you can respond as Controller, unless you have configured the Service for you to handle such requests yourself.

9.2 The Service provides functionality enabling you to access, correct, export, and erase Customer Personal Data to support your response to data-subject requests (subject to clause 10).

10. Erasure within an append-only architecture

10.1 The Service uses an append-only, event-sourced data model that preserves a complete, attributable audit trail. This means Personal Data is not erased by destructive deletion of records in the ordinary course.

10.2 **Erasure mechanism.** Where you instruct us to erase Personal Data (including to give effect to a data subject's right to erasure), we will remove it from all readable projections and views and render it no longer accessible or recoverable through the Service — using appropriate technical means, which may include appending a redaction event and/or destroying the encryption key under which the data is held — while preserving the structural, non-identifying integrity of the event record where lawful. Where the Personal Data also exists in backups, it will be rendered inaccessible and deleted or overwritten in the ordinary course of our backup retention cycle.

10.3 We will give effect to a valid erasure instruction without undue delay and in any event within 30 days, and confirm completion to you.

10.4 **Limits on erasure.** Erasure may be lawfully refused, limited, or deferred to the extent retention is required:

- by law;
- by a regulatory record-keeping obligation (for example, mandatory retention periods for working-time, rest-hours, certification, or other Workboat Code / MLC / STCW records); or
- for the establishment, exercise, or defence of legal claims.

Where such a limit applies, we will tell you and explain the basis.

11. Personal data breach

11.1 We will notify you **without undue delay** after becoming aware of a personal data breach affecting Customer Personal Data, and in any event within **48 hours** of becoming aware.

11.2 Our notification will include, to the extent available, the nature of the breach, the categories and approximate number of data subjects and records affected, likely consequences, and the measures taken or proposed. Where the information is not all available at once, we may provide it in phases without undue further delay.

11.3 We will assist you in meeting your own obligations to notify the ICO and affected data subjects under Articles 33 and 34, but we will not notify the ICO or data subjects on your behalf unless you instruct us to.

12. Audit

12.1 We will make available to you information reasonably necessary to demonstrate compliance with Article 28, and will allow for and contribute to audits, including inspections, conducted by you or an auditor you mandate.

12.2 To minimise disruption, an audit will in the first instance be satisfied by our providing relevant certifications, third-party audit reports, security documentation, or a completed security questionnaire. We operate as a remote organisation without physical offices, and the physical infrastructure on which the Service runs is operated by our sub-processors; assurance regarding that infrastructure is provided through the sub-processors' own certifications and audit reports. Where you reasonably require further assurance, we will accommodate a remote audit (for example, by

video conference and screen-share) on reasonable prior notice, during normal working hours, subject to confidentiality, and no more than once in any 12-month period except following a personal data breach or where required by a supervisory authority.

---

13. Return and deletion on termination

13.1 On termination or expiry of the Terms, you may export Customer Data during the Export Period set out in SLA clause 10.

13.2 After the Export Period, we will delete or return Customer Personal Data in our possession, and delete existing copies, **except** to the extent retention is required by law or permitted under clause 10.4, in which case we will continue to protect it and process it only as necessary for the retention purpose.

---

14. Liability

14.1 Each party's liability under or in connection with this DPA is subject to the limitations and exclusions set out in clause 13 of the **Terms**.

Annex 1 — Details of processing

- **Subject matter:** provision of the Ocealis platform for maritime fleet, crew, and compliance management.
- **Duration:** the Subscription Term, plus the Export Period and any lawful retention period.
- **Nature and purpose:** hosting, storing, organising, displaying, querying, and synchronising Customer Data to enable vessel, equipment, crew, certification, working-time, defect, and operational record-keeping, and AI-assisted querying via Pilot.
- **Categories of data subjects:** the Customer's crew, shore staff, and other Authorised Users.
- **Types of Personal Data:** identification and contact details; employment and role information; certification and qualification records; working-time and rest-hours records; and any health or medical-fitness data the Customer chooses to include.
- **Special category data:** The Service may process special category data — in particular health or medical-fitness data, such as seafarer medical fitness certificates — where the Customer chooses to include it. The Customer's responsibilities in respect of such data are set out in clause 3.3.

Annex 2 — Technical and organisational security measures

- **Encryption in transit:** industry-standard TLS for all client–server communication.
- **Encryption at rest:** AES-256 encryption of stored data.
- **Bridge devices:** Customer Data stored in an encrypted local store (SQLCipher); offline data protected on-device.
- **Authentication:** modern authentication for Console, including single sign-on where enabled; per-device cryptographic key pairs for Bridge, supporting individual identification and revocation of lost or compromised devices.
- **Tenant isolation:** multi-tenant architecture with application-layer scoping and, where applicable, database row-level security.
- **Access control:** least-privilege access to production and administrative systems.
- **Backups and recovery:** regular automated backups; target RPO/RTO as set out in SLA clause 8.
- **Integrity:** append-only event model; continuous monitoring and alerting for data-integrity events (SLA clause 8.5).
- **Vulnerability management:** process for receiving, triaging, and remediating vulnerabilities; responsible disclosure to **support@ocealis.net**.

Annex 3 — Authorised Sub-processors

Sub-processor	Purpose	Location
Supabase	Database and data services	UK (eu-west-2)
Vercel	Application hosting	UK (lhr1)
Amazon Web Services (Bedrock), using Anthropic Claude models	AI model inference for Pilot	UK / EU
OpenAI	Document embedding for Pilot	UK / EU