Data Processing Agreement

Effective Date: April 14, 2026 · **Version:** 1.0 · **Service:** YachtSalesHQ (yachtsaleshq.com)

This Data Processing Agreement ("**DPA**") forms part of the agreement between the customer ("**Controller**") and YachtSalesHQ ("**Processor**") governing use of the YachtSalesHQ service (the "**Service**"). It applies whenever the Service processes personal data on the Controller's behalf and is required by Article 28 of the EU General Data Protection Regulation ("**GDPR**"), the UK GDPR, and equivalent provisions of the California Consumer Privacy Act as amended ("**CCPA**").

This DPA is based on the open-licensed *Common Paper Cloud Service Agreement — Data Processing Addendum* (CC BY 4.0) with modifications to reflect the Service's architecture, subprocessor list, and contact details. By using the Service, the Controller accepts this DPA. A countersigned copy is available on request by emailing support@yachtsaleshq.com.

1. Definitions

- **Personal Data:** any information relating to an identified or identifiable natural person processed by the Processor on the Controller's behalf through the Service.
- **Controller** and **Processor:** bear the meanings given in Article 4 of the GDPR. Under the CCPA, the equivalent roles are "Business" and "Service Provider" (Cal. Civ. Code §1798.140).
- **Data Subject:** the natural person to whom Personal Data relates.
- **Subprocessor:** any third party engaged by the Processor to process Personal Data in connection with providing the Service.
- **Standard Contractual Clauses** or **SCCs:** the clauses annexed to European Commission Implementing Decision (EU) 2021/914 of 4 June 2021, applicable to transfers of Personal Data to third countries.

2. Roles, scope, and duration

The Controller determines the purposes and means of processing Personal Data it uploads to, or generates within, the Service (buyer and seller contacts, activities, deals, tasks, and related records). The Processor processes that Personal Data solely on the Controller's documented instructions, for the purpose of providing the Service and the features the Controller uses. Processing runs for the term of the customer's use of the Service and terminates on account deletion.

Nature of processing: storage, retrieval, organization, indexing, export, transmission, and secure deletion, performed through the Service's standard functionality.

Categories of Data Subjects: the Controller's own account users, and the individuals whose contact information the Controller enters into the Service (typically yacht buyers, sellers, and

related contacts).

Types of Personal Data: name; email; phone; free-text notes and activity records; budget and boat-preference details; price and commission figures; and authentication metadata (session identifiers, IP address, user agent).

3. Controller instructions

The Processor will act only on the Controller's instructions as set out in this DPA and the main service agreement, unless required to act otherwise by applicable law. If the Processor believes an instruction violates applicable data protection law, it will inform the Controller promptly and may suspend performance of that instruction pending clarification.

4. Confidentiality and personnel

The Processor ensures that any individual authorized to process Personal Data is bound by a duty of confidentiality (by contract or by law). Access to Personal Data is limited to those personnel who require it to provide and support the Service.

5. Security measures

The Processor maintains appropriate technical and organizational measures to protect Personal Data against unauthorized or unlawful processing and against accidental loss, destruction, damage, alteration, or disclosure. A non-exhaustive summary of current measures:

- **Encryption in transit:** TLS 1.2+ for all connections to the Service, with HSTS.
- **Authentication:** passwords hashed with Argon2id; session cookies are HTTP-only and secure-flagged; optional social login via Google OAuth.
- **Access control:** row-level authorization on every query — a customer can only read, write, or export their own records.
- **Hosting:** a hardened Linux host on DigitalOcean, with a reverse proxy terminating TLS. Administrative access is limited to the operator, via SSH key authentication only.
- **Backups:** automated database snapshots before every deployment, with continuous replication to encrypted object storage (Backblaze B2) once enabled.
- **Logging:** authentication events, administrative actions, and compliance-relevant events (consent, export, deletion) are retained in an audit log.
- **Operational security:** deployment is automated, with pre-flight checks that block destructive migrations and an auto-snapshot taken before any schema change.

6. Subprocessors

The Controller authorizes the Processor to engage the subprocessors listed in **Annex A** below. The Processor remains responsible for the acts and omissions of its subprocessors as it would for its own. The Processor will notify the Controller of any intended addition or replacement of subprocessors with a reasonable opportunity to object, and will impose data protection obligations on each subprocessor that are no less protective than those in this DPA.

7. Data subject rights

The Service provides in-application tooling that lets the Controller honor Data Subject rights (access, portability, rectification, erasure, restriction, objection) without contacting the Processor:

- **Access and portability:** Settings → Export my data, and per-contact Export contact data, produce a structured, machine-readable bundle.
- **Erasure:** Settings → Delete my account removes the Controller's entire account and all linked records in a single atomic transaction. Per-contact Permanently delete (GDPR) removes the contact, their activities, their tasks, and their identifying fields from any associated deal.
- **Rectification and restriction:** every record is editable in the application interface.

If the Controller nonetheless requires the Processor's direct assistance to respond to a Data Subject request, the Processor will provide reasonable cooperation, taking into account the nature of the processing and the information available to the Processor.

8. Personal data breach

The Processor will notify the Controller without undue delay — and in any event within 72 hours — after becoming aware of a Personal Data breach affecting the Controller's data, and will provide information reasonably required for the Controller to meet its own breach-notification obligations under Article 33 of the GDPR or equivalent law. Notification will be sent by email to the address the Controller has on file with the Processor.

9. Data protection impact assessments

The Processor will provide reasonable cooperation and information needed by the Controller to conduct data protection impact assessments and, where required, prior consultations with supervisory authorities, in respect of processing carried out by the Processor.

10. International transfers

The Processor and its subprocessors listed in Annex A operate primarily in the United States. Where the Controller is established in the European Economic Area, the United Kingdom, or Switzerland, and Personal Data is transferred to the United States (or any other country that has not received an

adequacy decision applicable to the Controller's jurisdiction), the Standard Contractual Clauses — Module Two (controller-to-processor) — are incorporated by reference and apply to those transfers. For transfers from the United Kingdom, the International Data Transfer Addendum issued by the UK Information Commissioner's Office applies. Docking Clause 7 is selected; the optional redress mechanism in Clause 11(a) is not selected; Option 1 of Clause 17 applies; the supervisory authority is the supervisory authority of the member state where the Controller is established, or if the Controller is established outside the EU, the Irish Data Protection Commission.

11. Deletion and return of personal data

On termination of the Controller's use of the Service, or at the Controller's earlier request, the Processor will delete all Personal Data in its possession. The Controller may export its data at any time prior to termination using the in-application Export tool. Retention beyond termination is limited to records the Processor is required by law to retain (for example, to meet tax or auditing obligations).

12. Audits

The Processor will make available to the Controller all information reasonably necessary to demonstrate compliance with this DPA. Given the Service's scale, the Processor expects audit rights to be exercised through written questionnaires. On-site audits may be requested where a Controller reasonably demonstrates they are required by a supervisory authority and will be scheduled at a mutually agreeable time, with confidentiality obligations applying to any information reviewed.

13. CCPA — service provider terms

For purposes of the CCPA, the Controller is a "Business" and the Processor is a "Service Provider." The Processor will process Personal Information of California residents only on the Controller's behalf and for the specific business purpose of providing the Service. The Processor will not sell, share, or retain, use, or disclose Personal Information for any purpose other than that purpose (including any "commercial purpose" as defined by the CCPA) and will not combine Personal Information received from the Controller with Personal Information received from any other source except as permitted by §7050(b) of the CCPA regulations. The Processor certifies that it understands these restrictions and will comply with them.

14. Liability and governing law

Liability under this DPA is subject to the limitation of liability set forth in the main service agreement between the parties. This DPA is governed by the laws of the United States (the governing state to

be specified by the Processor on a finalized signed copy). The Standard Contractual Clauses retain their own governing law as set out in Clause 17 of the SCCs.

15. Changes and precedence

The Processor may update this DPA to reflect changes in applicable law, the Service's architecture, or its subprocessor list. Material changes will be communicated to the Controller with at least 30 days' notice. In the event of a conflict between this DPA and any other agreement between the parties with respect to processing of Personal Data, this DPA controls.

Annex A — Subprocessors

The Processor uses the following subprocessors to provide the Service. All subprocessors are bound by written data protection obligations.

Subprocessor	Purpose	Location
DigitalOcean, LLC	Application hosting and database storage	United States (NYC3 / SFO3 regions)
Google LLC	OAuth sign-in for customers who choose Google login	United States
Functional Software, Inc. d/b/a Sentry	Error telemetry (scrubbed of Personal Data on ingest)	United States
Telegram FZ–LLC	Administrative security notifications (sign-in alerts to the operator only; no customer data transmitted)	United Arab Emirates / international
Backblaze, Inc.	Encrypted off-site backup storage (B2)	United States

Annex B — Technical and organizational measures

See Section 5 of this DPA. An up-to-date summary is also published at yachtsaleshq.com/privacy.

Annex C — Standard contractual clauses

The parties incorporate the European Commission's Standard Contractual Clauses (Module Two, controller-to-processor) by reference for any transfer of Personal Data from the European Economic Area to a country outside its adequacy scope. The SCCs are available at eur-lex.europa.eu/eli/dec_impl/2021/914/oj. For transfers originating from the United Kingdom, the UK International Data Transfer Addendum applies.

Contact

Questions, notices, and countersignature requests under this DPA should be sent to support@yachtsaleshq.com.

Processor
YachtSalesHQ

_____
Signature

_____
Name & title

_____
Date

Controller

_____
Signature

_____
Name & title

_____
Date