Data Processing Agreement

SupaSailing Platform — Version 1.1 — effective 1 November 2026

This Data Processing Agreement ("**DPA**") forms part of the Agreement between the Customer identified in the Order Form or, for online sign-up, the organisation that holds the account (the "**Controller**") and **SUPASAILING, S.L.**, Calle Blanquerna 53, 1-C, 07003 Palma de Mallorca, Spain, NIF B24999450 (the "**Processor**"). It sets out the terms required by Article 28 of Regulation (EU) 2016/679 ("**GDPR**") and Spanish Organic Law 3/2018 ("**LOPDGDD**"). Capitalised terms not defined here have the meaning given in the General Terms of Service.

1. Subject matter, duration, nature and purpose

1.1 The Processor processes personal data on behalf of the Controller only to provide the Service ordered in the Order Form. The subject matter, nature and purpose of the processing, the types of personal data and the categories of data subjects are described, for each subscribed Module, in **Annex I**.

1.2 The processing lasts for the term of the Agreement and, after it, for the transitional, retrieval and erasure periods described in clause 11 and in the General Terms (clause 14).

1.3 This DPA applies where and to the extent the Processor processes personal data as a processor for the Controller. The Processor acts as an independent controller only for the data it needs to manage its own relationship with the Customer (contact persons, billing, support records, and security logs), as described in its privacy policy.

2. Instructions

2.1 The Processor processes personal data only on the documented instructions of the Controller, including with regard to transfers to third countries, unless required to do so by Union or Member State law to which the Processor is subject; in that case the Processor informs the Controller of that legal requirement before processing, unless the law prohibits it on important grounds of public interest.

2.2 The Agreement, the configuration of the Service by the Controller and its Authorised Users, and the use of the Service's features are the Controller's complete documented instructions. Additional instructions must be given in writing and be consistent with the Agreement.

2.3 The Processor immediately informs the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions.

2.4 The Processor does not process the personal data for its own purposes and does not use it to train or improve artificial intelligence models. A processor that determines its own purposes becomes a controller (Article 28(10) GDPR; Article 33.2 LOPDGDD); the Processor will not do so.

3. Confidentiality

The Processor ensures that persons authorised to process the personal data (employees and contractors) have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality, access only the data necessary for their tasks, and receive appropriate data protection training.

4. Security of processing

4.1 The Processor implements the technical and organisational measures described in **Annex II**, which ensure a level of security appropriate to the risk, as required by Article 32 GDPR, including as appropriate: encryption; the ongoing confidentiality, integrity, availability and resilience of the systems; the ability to restore availability and access to personal data in a timely manner after an incident; and a process for regularly testing and evaluating the effectiveness of the measures.

4.2 The Processor may update the measures as technology evolves, provided the overall level of security is not reduced.

4.3 The Controller is responsible for the security of its own devices and accounts, for enabling the security features the

Service offers (such as multi-factor authentication) and for granting access only to appropriate Authorised Users.

5. Special categories of personal data

5.1 Some Modules allow the Controller to store special categories of personal data within the meaning of Article 9 GDPR, such as health data contained in seafarer medical fitness certificates (e.g. ENG1), guests' medical requirements and allergies, or absence records for sickness, as indicated in Annex I.

5.2 The Controller decides whether to store such data and is responsible for having a condition under Article 9(2) GDPR (and, where relevant, national law) to process it. The Processor processes such data only to provide the Service, applies the access restrictions and encryption in Annex II, and does not send it to artificial intelligence features unless the Controller or its Authorised Users submit it to those features.

6. Sub-processors

6.1 **General authorisation.** The Controller gives the Processor general written authorisation to engage the sub-processors listed in **Annex III** and, subject to clause 6.2, other sub-processors.

6.2 **Changes.** The Processor keeps an up-to-date list of sub-processors at https://supasailing.com/legal/subprocessors and informs the Controller by email of any intended addition or replacement at least **thirty (30) days** in advance, giving the Controller the opportunity to object. The Controller may object on reasonable data protection grounds within that period. If the parties cannot resolve the objection, the Controller may terminate the affected Module with effect from the date the new sub-processor would be engaged and receive a refund of prepaid Fees for the unused period. In an emergency affecting the security or continuity of the Service, the notice period may be shorter, with prompt notice to the Controller.

6.3 **Flow-down.** The Processor imposes on each sub-processor, by written contract, data protection obligations that provide at least the same level of protection as this DPA, in particular sufficient guarantees to implement appropriate technical and organisational measures.

6.4 **Liability.** The Processor remains fully liable to the Controller for the performance of its sub-processors' obligations.

6.5 **Services enabled by the Controller.** Third-party services that the Controller or its Authorised Users choose to connect to the Service (listed as "Controller-enabled integrations" in Annex III), such as messaging apps, bank accounts, payment accounts or email mailboxes of the Controller, are not sub-processors of the Processor. The Controller instructs the Processor to exchange data with them when it enables them, and their processing is governed by the Controller's own relationship with those providers.

7. International transfers

7.1 The Service is hosted in the European Economic Area and, for the Modules indicated in Annex I, in the United Kingdom, which benefits from an adequacy decision of the European Commission (Commission Implementing Decision of 19 December 2025, valid until 27 December 2031).

7.2 The Processor transfers personal data outside the EEA, or allows access from outside the EEA, only to the extent necessary to provide the Service and only where the transfer complies with Chapter V GDPR, relying on: (a) an adequacy decision, including the EU-US Data Privacy Framework (Commission Implementing Decision (EU) 2023/1795) for recipients certified under it; or (b) the standard contractual clauses approved by Commission Implementing Decision (EU) 2021/914 (Module Three, processor to processor), together with supplementary measures where needed after a transfer impact assessment. The mechanism for each sub-processor is stated in Annex III.

7.3 If a transfer mechanism is invalidated, the Processor will promptly rely on an alternative mechanism or, failing that, stop the affected transfer and inform the Controller.

8. Assistance to the Controller

8.1 **Data subject requests.** Taking into account the nature of the processing, the Processor assists the Controller by appropriate technical and organisational measures in responding to requests from data subjects exercising their rights

under Chapter III GDPR. The Service allows the Controller to access, rectify, export and delete personal data. If the Processor receives a request directly, it forwards it to the Controller without undue delay and does not respond itself, except to direct the data subject to the Controller.

8.2 **Compliance.** The Processor assists the Controller in ensuring compliance with Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments and prior consultation), taking into account the nature of the processing and the information available to the Processor.

8.3 Assistance beyond what the Service provides as standard may be charged at reasonable rates agreed in advance, except where the need for assistance results from the Processor's breach.

9. Personal data breaches

9.1 The Processor notifies the Controller **without undue delay, and in any event within forty-eight (48) hours**, after becoming aware of a personal data breach affecting the Controller's personal data, by email to the Controller's contact in the Order Form or, failing that, to the owner of the Controller's account.

9.2 The notification describes, as far as then known: the nature of the breach, including the categories and approximate number of data subjects and records concerned; the name and contact details of the Processor's contact point; the likely consequences; and the measures taken or proposed to address the breach and mitigate its effects. Where not all information is available at once, the Processor provides it in phases without undue further delay.

9.3 The Processor takes the measures necessary to contain the breach and mitigate its effects, cooperates with the Controller, and documents the breach. Notification of a breach is not an acknowledgement of fault or liability.

10. Audits and information

10.1 The Processor makes available to the Controller all information necessary to demonstrate compliance with Article 28 GDPR, including this DPA, the description of measures in Annex II, its records of processing (Article 30(2) GDPR) as they concern the Controller, and relevant certifications or reports of its sub-processors.

10.2 The Processor allows for and contributes to audits, including inspections, conducted by the Controller or an independent auditor mandated by it who is bound by confidentiality, not more than once every twelve (12) months (except after a personal data breach or at the request of a supervisory authority), with at least thirty (30) days' notice, during business hours and without disproportionate disruption. Audits of sub-processors are carried out through the information and reports they provide. Each party bears its own costs of an audit.

11. End of the processing

11.1 At the end of the provision of the Service, at the Controller's choice, the Processor returns to the Controller all personal data (by making it available for export in the formats described in the General Terms, Schedule A) and deletes it, or deletes it directly, together with existing copies, within the periods described in clause 14 of the General Terms: a transitional period and a retrieval period of at least thirty (30) days each, followed by erasure.

11.2 Copies in encrypted backups are overwritten within the normal backup cycle of no more than ninety (90) days and are not processed in the meantime except for disaster recovery.

11.3 Where Union or Member State law requires the Processor to keep personal data, or while liabilities arising from the processing may be claimed, the Processor may keep it duly blocked (Article 32 and Article 33.4 LOPDGDD), accessible only to courts, public prosecutors and competent authorities, for the applicable limitation period, and then delete it.

11.4 On request, the Processor confirms the deletion in writing.

12. Liability and precedence

12.1 Each party's liability under this DPA is subject to the limitations of the General Terms, without prejudice to the rights of data subjects under Article 82 GDPR and to any liability that cannot be limited by law.

12.2 In case of conflict between this DPA and any other part of the Agreement on the protection of personal data, this

DPA prevails, except for the particular conditions individually agreed in the Order Form.

12.3 This DPA remains in force for as long as the Processor processes personal data on behalf of the Controller.

13. Contact points

- **Processor:** SUPASAILING, S.L. — legal@supasailing.com — Calle Blanquerna 53, 1-C, 07003 Palma de Mallorca, Spain. The Processor has not appointed a data protection officer, as it is not required to under Article 37 GDPR and Article 34 LOPDGDD; privacy matters are handled at the address above.
- **Controller:** the contact person and email stated in the Order Form or, for online sign-up, the owner of the Controller's account.

ANNEX I — DESCRIPTION OF THE PROCESSING

Nature of the processing (all Modules): hosting and storage; organisation, structuring and retrieval; display to Authorised Users; transmission of notifications (email, SMS and, where enabled, messaging apps); processing by artificial intelligence features when used; backup and restoration; export and deletion.

Purpose (all Modules): providing, securing and supporting the Service ordered by the Controller, in accordance with the Controller's instructions.

Duration: the term of the Agreement plus the exit periods in clause 11.

Fleet Management

Categories of data subjects

- crew members and employees of the Customer
- guests and charter clients
- owners, managers and users of the Customer
- suppliers, contractors and other contacts

Categories of personal data

- identification and contact data (name, email, phone, address, photo)
- identity documents (passport number, issuing country and expiry, visas), date and place of birth, nationality, gender
- emergency contacts
- professional data: certificates and courses (e.g. STCW), rank, department, schedules, rest hours, timesheets, warnings and notes
- bank account and tax identification data for crew payments; card and account transactions if the Customer connects its finance providers
- vessel positions and trips, including location shared in emergency alerts
- documents, signatures in logbooks and forms, messages and voice notes sent to the assistant

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- health data in seafarer medical fitness certificates (e.g. ENG1)
- guests' medical requirements, dietary needs and allergies
- crew absence status for sickness; medical emergency alerts

Database location: London, United Kingdom (adequacy decision). Application servers: Paris, France (EU).

Ferry

Categories of data subjects

- crew members and employees of the Customer
- guests and charter clients
- owners, managers and users of the Customer
- suppliers, contractors and other contacts

Categories of personal data

- identification and contact data (name, email, phone, address, photo)
- identity documents (passport number, issuing country and expiry, visas), date and place of birth, nationality, gender
- emergency contacts
- professional data: certificates and courses (e.g. STCW), rank, department, schedules, rest hours, timesheets, warnings and notes
- bank account and tax identification data for crew payments; card and account transactions if the Customer connects its finance providers
- vessel positions and trips, including location shared in emergency alerts
- documents, signatures in logbooks and forms, messages and voice notes sent to the assistant

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- health data in seafarer medical fitness certificates (e.g. ENG1)
- guests' medical requirements, dietary needs and allergies
- crew absence status for sickness; medical emergency alerts

Database location: London, United Kingdom (adequacy decision). Application servers: Paris, France (EU).

Merchant

Categories of data subjects

- crew members and employees of the Customer
- guests and charter clients
- owners, managers and users of the Customer
- suppliers, contractors and other contacts

Categories of personal data

- identification and contact data (name, email, phone, address, photo)
- identity documents (passport number, issuing country and expiry, visas), date and place of birth, nationality, gender
- emergency contacts
- professional data: certificates and courses (e.g. STCW), rank, department, schedules, rest hours, timesheets, warnings and notes
- bank account and tax identification data for crew payments; card and account transactions if the Customer connects its finance providers
- vessel positions and trips, including location shared in emergency alerts
- documents, signatures in logbooks and forms, messages and voice notes sent to the assistant

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- health data in seafarer medical fitness certificates (e.g. ENG1)
- guests' medical requirements, dietary needs and allergies
- crew absence status for sickness; medical emergency alerts

Database location: London, United Kingdom (adequacy decision). Application servers: Paris, France (EU).

Dock

Categories of data subjects

- berth holders, yard customers and vessel owners, their family members, companions, representatives and authorised third parties
- suppliers and partners
- employees and contractors of the Customer
- surveyors, external uploaders and signatories of contracts and mandates

Categories of personal data

- identification and contact data (name, emails, phones, addresses, photo)
- identity documents (kind, number, country, expiry), date of birth, nationality, tax/VAT number
- emergency contacts
- bank data: IBAN/BIC, SEPA direct debit mandates, payment methods and bank transactions
- access cards and keys; meter readings and their photos (kept 24 months)
- contracts and electronic signatures with IP address and device data (audit trail)
- timesheets, work assignments, shifts and absences
- documents, photos and emails processed with OCR and AI; assistant and Telegram bot messages, including voice notes

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- absence records that may reveal sickness

Database location: Ireland (EU). Application servers: Paris, France (EU).

Guild

Categories of data subjects

- association members and applicants
- referees, company contacts, event attendees, speakers and sponsors
- voters in governance processes
- recipients of campaigns and visitors who contact the association

Categories of personal data

- identification and contact data, address, nationality, date of birth, photo
- professional qualifications and certificates (e.g. STCW)
- applications, dossiers and uploaded documents
- membership fees, invoices and payments
- event check-ins and governance votes
- consents and communication logs; public directory profiles

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- health data in medical fitness certificates (e.g. ENG1)
- trade union membership, where the Customer is a trade union or professional body of that kind

Database location: Frankfurt, Germany (EU). Application servers: Paris, France (EU).

Broker

Categories of data subjects

- leads, prospective buyers and charterers
- vessel sellers and owners

- broker users of the Customer
- recipients of tracked emails and visitors of landing pages

Categories of personal data

- identification and contact data
- email content and open/click tracking, when the Customer connects a mailbox
- private vessel files and inspection photos
- activity history, form submissions and landing page views
- assistant conversations

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- None expected.

Database location: Frankfurt, Germany (EU). Application servers: Paris, France (EU).

Charter

Categories of data subjects

- charter clients and guests
- yacht owners and agents
- crew and employees of the Customer
- signatories of proposals and agreements, respondents to reviews

Categories of personal data

- identification and contact data, photo
- identity documents (passport or document number and country), date of birth, nationality
- emergency contacts, check-in and preference sheet answers
- owners' bank data (IBAN/SWIFT) and payment records
- signatures and signing audit events
- crew timesheets and leave; enquiry messages

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- guests' health information and allergies
- crew absence records for sickness
- dietary preferences that may reveal religious beliefs

Database location: Ireland (EU). Application servers: Paris, France (EU).

Agent (port agency)

Categories of data subjects

- seafarers in crew changes
- principals (ship owners and managers) and their contacts
- vendors and suppliers
- agency staff and email correspondents

Categories of personal data

- identification data: name, nationality, date of birth, rank
- passport number and copies of passports and visas; immigration status
- travel and accommodation data (flights, hotels)
- tax identification and bank data; invoices and payments

- emails and messages about port calls

Special categories of personal data (only if the Controller chooses to store them; see clause 5)

- None expected.

Database location: London, United Kingdom (adequacy decision). Application servers: Paris, France (EU).

ANNEX II — TECHNICAL AND ORGANISATIONAL MEASURES

Access control

- Authentication by email and password with enforced password rules; multi-factor authentication available for all users (authenticator app, email or SMS codes, depending on the Module).
- Role-based access control scoped by organisation, vessel, marina, yard or association, and by department where the Module supports it.
- Row-level security policies in the database and server-side authorisation checks on every request that accesses a customer's records.
- Administrative access by SupaSailing staff limited to named individuals, logged where the Module supports it (impersonation and audit logs), and used only for support and security on the Controller's request or to fix incidents.

Encryption

- Encryption in transit with TLS for all connections between users, the Service and sub-processors.
- Encryption at rest of databases, file storage and backups by the hosting providers.
- Additional application-level encryption of secrets such as multi-factor authentication seeds, banking and payment-provider tokens, and signing keys.

Availability and resilience

- Managed PostgreSQL databases with daily backups retained for seven (7) days.
- Uploaded files mirrored daily to a separate object store, with displaced or deleted files kept for ninety (90) days for recovery.
- Infrastructure monitoring and health checks with automatic restart of failed services.
- Documented restoration procedures.

Logging and integrity

- Security-relevant events recorded, including authentication, access to sensitive documents, electronic signatures and administrative actions, where the Module supports it.
- Electronic signatures in the Modules that offer them are protected by an audit trail and tamper-evidence.

Organisational measures

- Confidentiality undertakings from all staff and contractors.
- Least-privilege access to production systems.
- Credentials kept out of source code, with rotation after suspected exposure.
- A personal data breach procedure consistent with clause 9.
- Selection and contractual control of sub-processors under clause 6.

Data minimisation and privacy by design

- Special category data fields are optional and shown only to authorised roles.
- Error monitoring configured to exclude personal data where used.
- Personal data is not used to train AI models.

Testing

- Regular review of access policies and dependencies.
- Security fixes applied as a priority.
- Tests run before deployment of changes to production.

ANNEX III — SUB-PROCESSORS

The following sub-processors are authorised for the Modules in the Order Form. The current list is published at https://supasailing.com/legal/subprocessors.

Sub-processor	Purpose	Modules	Location	Transfer mechanism
Hostinger International Ltd.	Application servers (virtual private server)	Fleet Management, Ferry, Merchant, Dock, Guild, Broker, Charter, Agent (port agency)	Paris, France (EU)	No transfer outside the EEA
Supabase, Inc.	Managed database, authentication and file storage (hosted on AWS)	Fleet Management, Ferry, Merchant, Dock, Guild, Broker, Charter, Agent (port agency)	Database region per Module (see Annex I); support access from the United States	Data stored in the EEA/UK; support access under SCCs (Module 3)
Cloudflare, Inc.	DNS, TLS termination, network protection and encrypted backup storage (R2)	Fleet Management, Ferry, Merchant, Dock, Guild, Broker, Charter, Agent (port agency)	Global edge network; United States	EU-US Data Privacy Framework and SCCs (Module 3)
Emailit	Transactional email delivery (notifications, codes, documents)	Fleet Management, Ferry, Merchant, Dock, Guild, Broker, Charter, Agent (port agency)	Prague, Czech Republic (EU)	No transfer outside the EEA
Twilio Ireland Limited (Twilio Inc. group)	SMS delivery for multi-factor authentication codes and notifications	Fleet Management, Ferry, Merchant, Dock, Guild, Broker, Charter, Agent (port agency)	Ireland (EU) and United States	EU-US Data Privacy Framework and SCCs (Module 3)
Stripe Payments Europe, Ltd.	Payment processing for payments collected through the Service	Fleet Management, Ferry, Merchant, Guild, Broker, Charter	Ireland (EU); Stripe group in the United States	EU-US Data Privacy Framework and SCCs
Anthropic, PBC	AI features: assistants, document and image reading, text extraction and drafting	Fleet Management, Ferry, Merchant, Dock, Broker, Charter, Agent (port agency)	United States	EU-US Data Privacy Framework and SCCs (Module 3); no training on submitted data
OpenAI Ireland Ltd (OpenAI group)	AI features: document assistant, search embeddings, speech transcription	Fleet Management, Ferry, Merchant, Charter	United States	SCCs (Module 3); no training on API data
Groq, Inc.	Speech-to-text transcription of voice messages and fast text processing	Fleet Management, Ferry, Merchant, Dock, Broker, Charter, Agent (port agency)	United States	SCCs (Module 3)
Google Ireland Limited / Google LLC (Maps Platform)	Maps and place search	Fleet Management, Ferry, Merchant, Charter	United States and global	EU-US Data Privacy Framework and SCCs

Sub-processor	Purpose	Modules	Location	Transfer mechanism
Discord Inc.	Internal operational alerts to SupaSailing staff (may include a user name and email)	Fleet Management, Ferry, Merchant, Guild, Broker, Charter, Agent (port agency)	United States	SCCs (Module 3)
Google Ireland Limited (Google Analytics)	Product usage analytics, only after consent	Fleet Management, Ferry, Merchant	United States and global	EU-US Data Privacy Framework and SCCs
BunnyWay d.o.o. (bunny.net)	Hosting of tutorial videos	Fleet Management, Ferry, Merchant	Slovenia (EU)	No transfer outside the EEA
Google Ireland Limited / Google LLC (Gemini API)	AI features: document text recognition and classification, invoice extraction	Dock	United States and global	EU-US Data Privacy Framework and SCCs
Mapbox, Inc.	Maps, geocoding and static map images	Dock, Broker, Charter	United States	SCCs (Module 3)
Functional Software, Inc. (Sentry)	Error monitoring, configured to exclude personal data	Guild, Agent (port agency)	United States	EU-US Data Privacy Framework and SCCs
Resend, Inc.	Back-up transactional email delivery	Broker	United States	SCCs (Module 3)
Slack Technologies Limited (Salesforce group)	Internal operational alerts to SupaSailing staff	Charter	Ireland (EU) and United States	EU-US Data Privacy Framework and SCCs

Controller-enabled integrations (not sub-processors; see clause 6.5):

- Telegram (bot for staff messages, voice notes and photos, when the Customer links it)
- Bank and card providers connected by the Customer (Airwallex, Centtrip, Revolut Business)
- The Customer's email accounts connected for sync (Gmail, Microsoft 365, IMAP)
- The Customer's own payment accounts (Stripe Connect, PayPal, SumUp)
- Viator channel manager (when the Customer connects it)