

StarboardLog Data Processing Agreement

Version 1.0 | Effective Date: 26 September 2026

This Agreement governs StarboardLog processing of Customer Personal Data under Article 28 GDPR. It sets documented instructions, security, Subprocessor, assistance and exit rules. Annexes describe the processing, measures and provider categories.

1 Parties and effect

The Processor is Sándor Levente Szabó e.v., 9400 Sopron, Semmelweis utca 10., Hungary; individual entrepreneur registration number 61070435; Hungarian tax number 91404451-1-28; EU VAT number HU91404451. Contact: starboardlog@gmail.com. The Controller is the Customer identified in the applicable Terms or Order for the Workspace. This DPA forms part of the StarboardLog agreement and applies when the Processor first handles Workspace Personal Data on the Controller's behalf, no earlier than the Effective Date above, and remains in effect while that processing continues.

2 Definitions

Agreement means the Terms, the relevant Order and this DPA. Customer Personal Data means the data processed on the Customer's behalf in its Workspace under Annex 1. Security Incident means a personal data breach affecting that data. Subprocessor means a provider engaged by StarboardLog for Customer processing. Customer-directed Google Drive, authorized by the Customer or User and controlled through the connected Google account, is treated separately from direct Subprocessors in Annex 3. GDPR terms have their statutory meanings.

3 Roles and instructions

The Customer is Controller for its selected Workspace processing and determines the purposes, legal basis, subjects, data, authorized Users and Guest Access. StarboardLog is Processor for that data. The Provider independently controls Account, contract, subscription, billing, security, proportionate support administration and legal-compliance data as described in its Privacy Policy. The same identifier may have different roles for different purposes.

The Agreement, DPA, configured settings, authorized Admin or User actions and verified written Customer requests are documented instructions. The Processor acts only on such instructions unless Union or Member State law requires otherwise, in which case it informs the Customer in advance if legally permitted. It promptly informs the Customer if it believes an instruction infringes applicable data-protection law. Materially different instructions require agreement on feasibility, timing and reasonable costs.

4 Customer responsibilities

The Customer establishes lawful purposes and bases; provides notices and handles data-subject requests; ensures accuracy, minimization and permission to submit Documents; manages Users, Customers, Guest links, owners and Workspace access; and decides what is guest-visible. It does not submit special-category or criminal-offence data without a separately documented lawful, necessary instruction and safeguards. It controls its Google account, underlying files and sharing to the extent the integration uses Customer-owned Drive.

5 Processor duties

The Processor processes only as instructed; binds authorized personnel to confidentiality; maintains Article 32 measures appropriate to risk; assists with rights requests, incidents, DPIAs and prior consultation; makes available information needed to demonstrate compliance; ensures lawful Subprocessor engagements; and returns or deletes Customer Personal Data at the end of services as described below. It will inform the Customer if it can no longer materially meet these duties and work toward an appropriate remedy.

6 Access and security

Access is limited to authorized personnel and providers who need it for instructed processing, support, security or law. Annex 2 describes the measures. Master Admin Workspace access and impersonation require an identified reason and append-only audit evidence. Measures may evolve without materially reducing protection. No particular backup frequency, retention, selective restore, recovery point or recovery time is promised without a separate accepted SLA.

7 Data-subject requests

The Processor assists the Customer, taking account of the nature of processing and information available, so the Customer can answer Chapter III GDPR requests. Requests received directly about Customer Personal Data are forwarded or redirected unless law prevents this. The Customer identifies the Workspace, person, action and authorized requester. Unusually burdensome out-of-scope assistance may require a reasonable agreed charge to the extent law permits.

8 Security incidents

The Processor notifies the Customer without undue delay after becoming aware of a Security Incident affecting its Customer Personal Data. It provides known facts about nature, categories, approximate scope, likely effects, actions and a contact, with later updates when necessary. It reasonably contains, investigates and helps the Customer assess notification duties. The Customer decides notifications to authorities and individuals as Controller. Notice is not an admission of liability.

9 Impact assessments

Taking account of the nature of processing and information available, the Processor provides reasonable assistance with Articles 32 to 36 GDPR, including DPIAs and prior consultation. The Customer remains responsible for decisions and context. Assistance beyond standard features or documentation may require agreement on timing and cost.

10 Subprocessors

The Customer gives general written authorization for direct Subprocessors listed in Annex 3 and the current public provider information. The Processor binds direct Subprocessors to Article 28 obligations appropriate to their work and remains liable for their performance as required by law. Where reasonably practicable it publishes an update and emails affected Admin contacts at least 30 calendar days before a new or replacement direct Subprocessor starts. A Customer may object in that period on reasonable data-protection grounds. The parties assess safeguards, alternatives or affected-feature termination. An urgent security, legal or continuity change may be implemented first with notice as soon as practicable.

11 International transfers

Transfers outside the EEA occur on documented instruction, through authorized providers necessary for the Service or under law. Where required, the parties use an adequacy decision, the European Commission Standard Contractual Clauses under Implementing Decision 2021/914 with the appropriate module, or another lawful mechanism and supplementary safeguards. The shared managed infrastructure uses Ireland as its primary application data region, with possible limited processing elsewhere by providers and onward providers.

12 Information and audits

The Processor makes available information necessary to show Article 28 compliance and permits and contributes to audits by the Customer or an authorized independent auditor. Existing documents and written answers should be used first. An audit is arranged on reasonable notice and in a manner protecting security, other customers and confidentiality. Once per 12 months is the ordinary frequency, unless an incident, regulator request or credible material noncompliance warrants more; this operational schedule does not restrict mandatory Article 28 audit rights. Reasonable assistance costs may be charged except where material breach is established.

13 Return and deletion

The authorized Customer contact may request return, deletion or both at starboardlog@gmail.com. The Processor verifies authority and scope and makes supported exports available. It normally offers approximately 30 days of Read-Only retrieval where technically, legally and securely appropriate. Unless the Customer gives a different lawful instruction, the standing instruction afterward is deletion or anonymization from active systems without undue delay. Separate controller records may be retained for law, security or claims and residual provider backups may remain until protected rotation. Underlying Drive files remain controlled by the connected account; deleting a StarboardLog reference does not delete the file. The Processor confirms active-system deletion on reasonable request.

14 Liability and precedence

Agreement liability limits apply insofar as lawful; nothing limits an unlimitable GDPR right or liability. This DPA prevails over the Terms concerning processing of Customer Personal Data; applicable Standard Contractual Clauses prevail over inconsistent DPA provisions. The Privacy Policy continues to govern the Provider's distinct Controller Data.

15 Notices

DPA instructions, objections and deletion requests should be sent to starboardlog@gmail.com. Notices to the Customer use the recorded Admin contact or an agreed contact. The Customer keeps contact details current.

Annex 1 Processing description

Subject matter: provision of a Customer-controlled StarboardLog vessel-management Workspace. Duration: continuous or event-based during use and the return/deletion period. Nature: collection, organization, storage, display, calculation, disclosure under configured roles, issue workflows, maintenance and usage tracking, expenses and currency-specific allocation, exports, support, security, correction and deletion.

Purposes: administer vessels, bookings and availability; manage Customer records and booking-linked Guest Access; record usage and counters; maintain components, requirements, events and issues; track ownership shares, expenses, balances and settlements; manage Documents, optional Drive workflows, timeline and Vessel Record Pack. Data subjects: Customer owners and contacts, Admins, Crew, Maintenance-tagged members, vessel owners, charter or rental customers, Guests, service personnel, vendors and people identified in submitted records.

Data categories: identity and contact; membership, roles and invitation status; vessel and booking context; Guest link and issue-report information; usage, counters, issues, components and maintenance; ownership shares, expenses, split methods, settlement entries and currencies; Document data or metadata, Google connection identifiers and protected authorization data; audit and support context. Financial records do not establish legal title and the Service does not move funds or automatically exchange currency. Special-category and criminal-offence data are not intentionally required; accidental submissions are handled under the Customer's lawful instructions.

Annex 2 Technical and organizational measures

The current control framework includes managed authentication and sessions, Workspace-scoped role and row-level authorization, protected server-side operations, transport encryption, provider-managed encrypted storage, restricted secrets, limited access and confidentiality, issue and maintenance attribution, operational and administrative audit records, incident response, supplier review and controlled deletion. Guest Access must remain booking-scoped and revocable and must exclude owner finance, private Documents, Google Drive and unrelated bookings. Drive access should be limited to the authorization actually granted by its user.

The controls include managed authentication and sessions; Workspace-scoped row-level and role authorization; protected server and database operations; reason-logged elevated access; TLS and provider-level storage encryption; server-side secrets; protected financial entries; limited drive.file access; audit and incident procedures; supplier review; and controlled manual return and deletion. The Customer manages invitations, Guest links, connected Drive and its own independent copies. No specific backup frequency or certification is promised.

Annex 3 Providers and change procedure

Direct Subprocessors are Lovable Labs Incorporated for managed hosting, database, authentication, server functions and security, and Plus Five Five, Inc. operating Resend for transactional email. Lovable and Resend manage their own onward-provider chains. Customer-directed Google Drive is a separate optional integration rather than a direct StarboardLog Subprocessor for the Customer-selected account and files. Számlázz.hu supports the Provider's independent invoicing as a controller-side recipient.

Lovable Labs Incorporated supplies the shared managed infrastructure, with Ireland as the primary application data region and authorized onward providers. Plus Five Five, Inc. operating Resend provides transactional application email. Their applicable DPAs, provider lists and lawful transfer safeguards govern their processing. Customer-directed Google Drive is a separate optional account integration, with drive.file permission for selected vessel files. KBOSS.hu Kft. operating Számlázz.hu supports the Provider's manual billing as a controller-side recipient. Changes follow Section 10 and the standalone Subprocessor and Service Provider Information document.