

ReadyFlyLog Data Processing Agreement

Version	1.0
Status	Final contract ready English
Effective date	11 September 2026
Last reviewed	11 September 2026

This Data Processing Agreement forms part of the agreement under which Sándor Levente Szabó e.v., trading through ReadyFlyLog, provides the ReadyFlyLog Service to the Customer identified in that agreement. It governs ReadyFlyLog's processing of Workspace Personal Data on the Customer's behalf and records the terms required by Article 28 of the GDPR.

The Customer is the controller of Workspace Personal Data and ReadyFlyLog is its processor, except where ReadyFlyLog processes separate Controller Data for account, contract, billing, security, support, or legal purposes. Annex 1 describes the processing, Annex 2 describes the current technical and organizational measures, and Annex 3 explains the provider chain and change procedure.

1 Parties and Effect

The Processor is Sándor Levente Szabó e.v., registered at 9400 Sopron, Semmelweis utca 10., Hungary, individual entrepreneur registration number 61070435, registered with NAV in the Individual Entrepreneurs Register, Hungarian tax number 91404451-1-28, EU VAT number HU91404451, email readyflylog@gmail.com.

The Controller is the Customer identified in the Terms, order, subscription record, or other agreement for the relevant Workspace. This DPA takes effect on the Effective Date stated above or, if later, when the Customer accepts or enters the Agreement and ReadyFlyLog first processes Workspace Personal Data for that Customer. It continues while ReadyFlyLog processes such data.

2 Definitions

- Agreement means the Terms and Conditions, subscription or order record, and any other binding terms between the parties for the Service, including this DPA.
- Customer Personal Data means Personal Data processed by ReadyFlyLog on the Customer's behalf in the Service, including Workspace Personal Data described in Annex 1.
- Data Protection Laws means the GDPR and other data-protection or privacy law applicable to the processing under this DPA.
- GDPR means Regulation (EU) 2016/679.
- Security Incident means a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data processed by ReadyFlyLog.
- Subprocessor means a processor engaged by ReadyFlyLog to process Customer Personal Data for the Customer. It does not include the Customer's own personnel or a third party that the Customer or an authorized user independently directs or authorizes, such as the connected Google Drive account described in Annex 3.
- Terms means the ReadyFlyLog Terms and Conditions, Version 1.0, as updated in accordance with those Terms.

Controller, Processor, Data Subject, Personal Data, Processing, Supervisory Authority, and Special Categories of Personal Data have the meanings given in the GDPR. A capitalized term not defined here has the meaning given in the Agreement.

3 Scope and Allocation of Roles

The Customer acts as Controller and ReadyFlyLog acts as Processor for Customer Personal Data. The Customer determines the purposes of the Workspace processing, which data are entered, which users may act, and the applicable legal basis. ReadyFlyLog processes Customer Personal Data only to provide, secure, support, and administer the Service in accordance with documented Customer instructions.

ReadyFlyLog acts as an independent Controller for account creation, authentication and platform administration; its contract, subscription, billing and tax records; Terms acceptance evidence; fraud, abuse and security records; support administration; Master Admin, commercial, and capacity administration; and compliance with legal obligations. Those activities are governed by the Privacy Policy and are outside this DPA, even if some identifiers also appear in Customer Personal Data.

4 Documented Instructions

The Customer instructs ReadyFlyLog to process Customer Personal Data as needed to provide the Service features the Customer and its authorized users choose, maintain security and access controls, provide support, make available exports, and perform the other processing described in Annex 1. The Agreement, this DPA, configured settings, authorized user actions, and written requests from an authorized Customer Administrator together constitute documented instructions.

ReadyFlyLog will process Customer Personal Data only on those instructions unless Union or Member State law requires other processing. If legally permitted, ReadyFlyLog will inform the Customer of that requirement before processing. ReadyFlyLog will promptly inform the Customer if, in its reasonable opinion, an instruction infringes Data Protection Laws and may suspend the affected processing while the parties address the issue.

The Customer may give additional instructions by emailing readyflylog@gmail.com. An instruction that materially changes the Service, creates disproportionate cost or risk, or falls outside the agreed processing requires written agreement on scope, timing, and any reasonable fee before it becomes binding.

5 Customer Responsibilities

The Customer is responsible for the lawfulness, fairness, and transparency of its processing; the accuracy and necessity of Customer Personal Data; its legal basis; required notices and consents; Data Subject requests; access and role administration; and the legality of its instructions. The Customer must ensure that authorized users do not submit prohibited or excessive data.

The aircraft document feature is limited to aircraft-related documents. The Customer must not intentionally use it for medical or health records, pilot licence files, personal pilot documents, or unrelated storage. ReadyFlyLog does not provide medical, training-progress, qualification, rating, or currency-tracking functionality and does not intend to process Special Categories of Personal Data.

The Customer controls its Google account, Google Drive storage, sharing permissions, retention, and deletion. It must ensure it has authority to connect the account and to make each selected file available to ReadyFlyLog.

6 Processor Obligations

ReadyFlyLog will:

- process Customer Personal Data only on documented instructions and only for the duration and purposes described in this DPA;
- ensure that persons authorized to process Customer Personal Data are bound by confidentiality or an appropriate statutory duty;
- implement and maintain the measures described in Annex 2, taking account of the state of the art, implementation cost, processing context, and risks;
- assist the Customer with Data Subject requests, security obligations, breach notifications, data protection impact assessments, and prior consultation as described below;
- maintain records and information sufficient to demonstrate compliance with this DPA;
- apply the return and deletion procedure in section 15; and
- notify the Customer if ReadyFlyLog can no longer meet a material obligation under this DPA and work in good faith on an appropriate remedy.

7 Confidentiality and Access

ReadyFlyLog restricts access to Customer Personal Data to persons and service providers that need access for the instructed processing, support, security, or legal compliance. Authorized persons must keep the data confidential and follow applicable access and security procedures.

ReadyFlyLog maintains one platform-owner Master Admin account for limited platform, commercial, capacity, and support administration. It uses the ordinary authenticated account system. A reason is required before impersonation or switching into a Customer context, and the action is recorded in an append-only audit trail. This access does not change the Customer's controller role.

8 Security

ReadyFlyLog will implement appropriate technical and organizational measures under Article 32 of the GDPR. The current measures are described in Annex 2. ReadyFlyLog may update the measures to address changes in technology, risk, providers, or the Service, provided the overall level of protection is not materially reduced.

The Customer acknowledges that no service can guarantee absolute security or availability. ReadyFlyLog does not commit to a specific backup frequency, backup-retention period, recovery point, recovery time, point-in-time recovery capability, selective-restoration capability, or certification unless the parties expressly agree that commitment in writing.

9 Data Subject Requests

Taking account of the nature of the processing, ReadyFlyLog will assist the Customer through appropriate technical and organizational measures, insofar as possible, to respond to requests under Chapter III of the GDPR. If a Data Subject submits a request directly to ReadyFlyLog concerning Customer Personal Data, ReadyFlyLog will forward or redirect it to the Customer unless law prohibits that step. ReadyFlyLog will not decide the request for the Customer.

The Customer must identify the Workspace, Data Subject, requested action, and authorized requester. ReadyFlyLog may request reasonable verification and may charge a reasonable fee or require a separate statement of work for assistance that is unusually burdensome or outside standard Service functionality, to the extent permitted by law and the Agreement.

10 Security Incidents

ReadyFlyLog will notify the Customer without undue delay after becoming aware of a Security Incident affecting that Customer's Personal Data. Notice will be sent to the Customer Administrator contact available in the Service or another contact the Customer has designated.

As information becomes available, the notice will describe the nature of the incident, affected categories and approximate scope where known, likely consequences, measures taken or proposed, and a contact point. ReadyFlyLog may provide information in phases. Notification is not an admission of fault or liability.

ReadyFlyLog will take reasonable steps to contain, investigate, mitigate, and remediate the incident and will provide information reasonably needed for the Customer's assessment and notification duties. The Customer remains responsible for deciding whether and how to notify a Supervisory Authority or Data Subjects.

11 Assistance with Risk Assessments

Taking account of the nature of the processing and information available to it, ReadyFlyLog will provide reasonable assistance with the Customer's obligations under Articles 32 to 36 of the GDPR, including data protection impact assessments and prior consultation. The Customer must provide sufficient context and remains responsible for the assessment and decisions. Assistance beyond standard documentation or Service functionality may require agreement on reasonable cost and timing.

12 Subprocessors

The Customer gives ReadyFlyLog general written authorization to use Subprocessors. The current direct Subprocessors and the distinction between those Subprocessors, Lovable-managed onward providers, Customer-directed Google services, and controller-side providers are described in Annex 3 and the public ReadyFlyLog Subprocessor and Service Provider Information document.

ReadyFlyLog will require each Subprocessor to protect Customer Personal Data through a written agreement that imposes data-protection obligations appropriate to the processing and materially equivalent to the relevant requirements of this DPA. ReadyFlyLog remains responsible to the Customer for the Subprocessor's performance to the extent required by Data Protection Laws.

ReadyFlyLog will update the public provider information and email affected Customer Administrators at least 30 calendar days before an intended new or replacement Subprocessor begins processing, where reasonably practicable. A Customer may object during that period by emailing readyflylog@gmail.com and explaining reasonable data-protection grounds. For an urgent change required to maintain security, availability, legal compliance, or essential service continuity, ReadyFlyLog may shorten or omit advance notice and will give notice as soon as reasonably practicable.

The parties will try in good faith to resolve a valid objection, including through a reasonable configuration or alternative where available. If no reasonable resolution is available, ReadyFlyLog may stop the affected feature or the Customer may terminate the affected Service or Subscription in accordance with the Agreement. An objection does not require ReadyFlyLog to provide a technically or commercially unreasonable alternative.

13 International Transfers

ReadyFlyLog will not transfer Customer Personal Data outside the EEA except on documented Customer instructions, through an authorized provider needed for the Service, or where law requires it. If the GDPR requires a transfer mechanism, ReadyFlyLog will use an adequacy decision, the European Commission's Standard Contractual Clauses under Implementing Decision 2021/914, or another lawful mechanism. Modules Two or Three will apply to a provider relationship as appropriate to the parties' roles.

The current ReadyFlyLog deployment's primary application data region is reported and verified as Ireland in the European Union. This does not mean that all support, email, security, or onward-provider processing occurs only in the EEA. Relevant locations and safeguards are summarized in Annex 3 and the public provider information.

14 Information and Audits

ReadyFlyLog will make available information reasonably necessary to demonstrate compliance with Article 28 of the GDPR and this DPA. The Customer should first use current policies, provider documents, security descriptions, and written responses supplied by ReadyFlyLog.

If that information is insufficient, the Customer may request a reasonable audit no more than once in any 12-month period, unless a Security Incident, Supervisory Authority request, or credible evidence of material non-compliance justifies an additional audit. Audits must be scheduled on reasonable notice, occur during normal business hours, avoid disruption, protect other customers and security-sensitive information, and be conducted by the Customer or an independent auditor bound by confidentiality. The Customer bears its audit costs and ReadyFlyLog may charge reasonable costs for material assistance, except where an audit establishes ReadyFlyLog's material breach of this DPA.

15 Return and Deletion

The Customer may request return, deletion, or both by emailing readyflylog@gmail.com from an authorized Customer contact. ReadyFlyLog will verify the requester's identity and authority, identify the Workspace and scope, and confirm whether the Customer wants an available export before deletion. Supported Workspace exports and per-pilot flight exports may be used; available formats can change as the Service develops.

After termination, ReadyFlyLog may provide approximately 30 days of read-only access or other retrieval assistance where technically, legally, and securely appropriate. This period is for return and transition and does not promise an automatic destructive purge on a particular day. The Customer remains responsible for downloading required exports and its Google Drive files.

Unless the Customer gives a different lawful instruction, the Customer's standing instruction at the end of the retrieval period is for ReadyFlyLog to delete or anonymize Customer Personal Data from active ReadyFlyLog systems through a controlled manual process. ReadyFlyLog will carry out a verified instruction without undue delay and may retain only data that law requires or that ReadyFlyLog needs as an independent Controller for security, fraud prevention, legal claims, contract evidence, or tax and billing compliance. Retained data will be isolated from ordinary product use and deleted when the reason ends.

Residual copies in provider backups or disaster-recovery media may remain until the provider's normal protected rotation or deletion process completes. They will not be restored to ordinary use except for continuity or security recovery. Deleting ReadyFlyLog metadata or a file reference does not delete the underlying file from the Customer's Google Drive. ReadyFlyLog will confirm completion of an active-system deletion on reasonable request.

16 Liability and Order of Precedence

The liability terms and limitations in the Agreement apply to this DPA to the extent permitted by law. Nothing in this DPA limits a right or liability that Data Protection Laws do not permit the parties to limit.

If this DPA conflicts with the Agreement on processing Customer Personal Data, this DPA prevails to the extent of the conflict. The Standard Contractual Clauses prevail over this DPA where they apply and conflict. This DPA does not amend the controller terms in the Privacy Policy for Controller Data.

17 Notices and Contact

Notices to ReadyFlyLog under this DPA, including additional instructions, deletion requests, and Subprocessor objections, must be sent to readyflylog@gmail.com. ReadyFlyLog may send notices to the Customer Administrator email recorded for the affected Workspace. The Customer must keep that contact current.

Annex 1 Processing Details

Subject Matter and Purpose

ReadyFlyLog processes Customer Personal Data to provide the Customer-controlled Workspace features of the ReadyFlyLog flight-logging and aircraft-management Service. Processing supports authorized access, flight and aircraft records, maintenance and expense records, internal Pilot Balance entries, aircraft-document references, exports, security, support, and optional Customer-directed Google integration.

Duration and Frequency

Processing is continuous or event-driven while the Customer and its authorized users use the Service, followed by the return, retrieval, and deletion process in section 15. Particular records are processed whenever an authorized user creates, views, changes, exports, archives, or deletes them, or when the Service performs an instructed background or security operation.

Nature of Processing

- collection, recording, organization, structuring, storage, consultation, display, and retrieval;
- calculation and update of operational counters, costs, discounts, and internal Pilot Balance entries;
- role-based disclosure to authorized Workspace users and access restriction;
- generation of structured Workspace and per-pilot flight exports and, where supported, saving an export to Google Drive;
- creation and management of metadata and references for aircraft files that remain in Customer-controlled Google Drive;
- support, troubleshooting, security monitoring, audit logging, correction, archiving, deletion, and anonymization; and
- transmission to authorized Subprocessors or Customer-directed services described in Annex 3.

Categories of Data Subjects

- Customer owners, administrators, members, invited users, and account contacts;
- pilots, pilots in command, instructors, students, crew members, and other persons identified in flight records;
- maintenance personnel, vendors, or expense contacts identified in operational records;
- persons identified in aircraft-document metadata, audit records, or support material submitted by the Customer; and
- other individuals whose limited data the Customer lawfully includes in Workspace records.

Categories of Personal Data

Category	Included data
Identity and contact	Name, email address, phone number if provided, internal user and authentication identifiers
Membership and role	Workspace membership, role, invitation, access status, actor identifiers
Flight operations	Date, time, landings, route, remarks, PIC, instructor or student designation, cost, discount, corrections
Aircraft and maintenance	Aircraft identifiers and details, status, maintenance records, counters, expenses, audit history
Internal financial records	Pilot Balance top-ups, debits, discounts, cost entries, and related audit data; no payment-card or wallet service

Category	Included data
Aircraft document reference	File name, type, size, Drive file and folder identifiers, aircraft association, uploader, timestamps, and related metadata
Google connection	Connected email and account identifier, scope, root folder reference, protected credentials or tokens, and connection actions
Technical and audit	Timestamps, IP address, user agent, role changes, access context, errors, security events, and protected administrative actions
Support and export	Support content supplied for the Workspace and data included in requested exports

Special Categories and Criminal Data

No Special Categories of Personal Data or personal data relating to criminal convictions and offences are intentionally required or supported. The Customer must not use the aircraft-document feature for medical or health records and must avoid placing sensitive personal data in free-text remarks or support material unless the parties first document a lawful, necessary instruction and suitable safeguards. If such data are submitted without authorization, ReadyFlyLog may restrict access and assist the Customer with removal.

Annex 2 Technical and Organizational Measures

The measures below describe the current control framework for the Service. Their operation depends in part on managed infrastructure and on the Customer's own access, Google Drive, endpoint, and export practices.

Control area	Current measures
Governance and minimization	Controller and processor roles are documented; features and data fields are reviewed against the current product; excluded medical, pilot-document, training-progress, qualification, rating, and currency functions are not supported.
Authentication and authorization	Managed authentication, authenticated sessions, Workspace membership checks, role-based authorization, and a single authenticated Master Admin account for limited platform administration.
Workspace isolation	Row-level security and Workspace-scoped access controls restrict ordinary queries and actions to authorized records. Privileged server or database functions are used for protected operations.
Administrative access	Master Admin impersonation or context switching requires a reason and creates an append-only audit record. Commercial, capacity, role, and other sensitive actions are audited.
Transmission and storage	HTTPS and TLS protect data in transit. Managed providers supply encryption for stored data at the infrastructure level. Application secrets are kept server-side rather than exposed to the browser.
Financial integrity	Protected server-side or database writes, role checks, immutable EUR price snapshots for capacity requests, and audit trails reduce unauthorized alteration of commercial and Pilot Balance records.
Google Drive access	The drive.file scope limits access to specific files used with the application. ReadyFlyLog stores metadata and references, not aircraft-document file bytes, and keeps connection credentials in managed protected storage.
File handling	The application validates supported file type and size before creating an aircraft-document reference. The control is technical and does not promise semantic inspection of document content.
Logging and monitoring	Authentication, error, security, role, commercial, capacity, and protected administrative events may be logged with limited context needed to investigate faults and misuse.
Availability and recovery	The Service uses managed cloud infrastructure and operational response procedures. Read-only access may support retrieval after trial expiry or termination. Specific backup frequency, retention, recovery objectives, point-in-time recovery, and selective restoration are not promised.
Incident management	ReadyFlyLog investigates reported or detected security events, limits access where appropriate, coordinates with providers, documents material facts, and follows the notification process in section 10.
Supplier management	ReadyFlyLog reviews applicable provider terms, DPAs, transfer mechanisms, and public Subprocessor information and maintains a process for notice and objection.
Return and deletion	Verified Customer instructions, available exports, a controlled manual deletion or anonymization process, separation of ReadyFlyLog metadata from Customer-owned Drive files, and isolation of lawfully retained Controller records.
Customer controls	The Customer manages user roles, invitations, Google Drive access and retention, endpoints, lawful data entry, exports, and removal of prohibited or excessive content.

Annex 3 Providers and Change Procedure

Direct Subprocessors

Provider	Service and data	Location and safeguard
Lovable Labs Incorporated	Application hosting and managed cloud services, database, authentication, server functions, security, and error reporting. May process Workspace records, account identifiers, service logs, error traces, and limited support context.	Primary application data region for the current deployment is Ireland in the EU. Lovable and onward providers may process elsewhere. Lovable DPA and applicable Standard Contractual Clauses.
Plus Five Five, Inc. operating Resend	Transactional authentication, invitation, and service email. Processes recipient email, name where supplied, message content, and delivery metadata. ReadyFlyLog does not use Resend for newsletters or marketing tracking.	United States and other provider locations as applicable. Resend DPA, applicable Standard Contractual Clauses, and other lawful transfer mechanisms.

Managed Onward Provider Chain

Lovable uses managed infrastructure and onward providers, including Supabase-based database and authentication components for the current deployment. These providers sit within Lovable's provider chain unless ReadyFlyLog separately contracts with them. The current Lovable list is maintained through Lovable's Trust Center. ReadyFlyLog reviews and archives the applicable chain rather than freezing a potentially outdated onward-provider list in this DPA.

Customer Directed Google Services

Google Drive and other supported Google APIs are Customer-directed third-party services rather than ordinary ReadyFlyLog Subprocessors. The Customer or authorized user chooses whether to connect Google, selects the account and relevant files, and retains control of the underlying Drive storage. ReadyFlyLog processes connection data, metadata, references, and user-initiated API input under the Customer's instructions. Google processes data under the user's or Customer's Google relationship and applicable Google terms.

Controller Side Provider

KBOSS.hu Kft., operating Számlázz.hu, may process billing identity, address, tax or VAT details, invoice content, and invoice administration data when ReadyFlyLog uses the service manually outside the application. ReadyFlyLog uses it in its Controller role. It is not part of the Workspace processor chain unless the parties later document a different use.

Change Notice and Objection

1. ReadyFlyLog records the intended provider change, affected processing, location, and safeguard.
2. Where reasonably practicable, ReadyFlyLog updates the public provider information and emails affected Customer Administrators at least 30 calendar days before the new or replacement Subprocessor begins processing.
3. The Customer may object within that notice period at readyflylog@gmail.com on reasonable data-protection grounds and must explain the concern.
4. The parties assess a reasonable alternative, configuration, safeguard, or discontinuation of the affected feature.

5. If no reasonable resolution is available, the affected Service or Subscription may be terminated in accordance with section 12 and the Agreement.
6. For urgent security, legal, or continuity changes, ReadyFlyLog gives notice as soon as reasonably practicable after the necessary change.

Public provider terms and lists include the [Lovable Data Processing Agreement](#), the [Lovable Subprocessor information](#), the [Resend Data Processing Addendum](#), and the [Resend Subprocessor List](#).