Data Processing Agreement

Version 1.2, 3 November 2026

This Data Processing Agreement ("**DPA**") is incorporated into and forms part of the Services Agreement (allaboard.eu/services-agreement) between All Aboard AB, company number 559214-7671, Kivra 559214-7671, 106 31 Stockholm, Sweden ("**All Aboard**") and the Agent (each as defined in the Services Agreement, together the "**Agreement**"). By entering into the Agreement, the Agent is deemed to have accepted and executed this DPA. No separate signature is required.

1. Definitions

Terms such as "personal data", "processing", "controller", "processor", "data subject", and "personal data breach" have the meanings given in Applicable Data Protection Law.

"**Applicable Data Protection Law**" means (i) the EU General Data Protection Regulation (Regulation (EU) 2016/679, "**GDPR**"); (ii) where applicable to the processing, the UK GDPR and the UK Data Protection Act 2018 (together the "**UK GDPR**"); and (iii) any other data protection law applicable to a party in connection with the Agreement. Where the UK GDPR applies to the processing, references to the GDPR include the equivalent provisions of the UK GDPR, and the competent supervisory authority for that processing is the UK Information Commissioner's Office.

"**Agent Personal Data**" means personal data that All Aboard processes as a processor on behalf of the Agent under the Agreement, as described in Annex 1, Part A. "**Sub-processor**" means a third party engaged by All Aboard to process Agent Personal Data. Capitalized terms not defined here have the meanings given in the Agreement.

2. Roles and scope

2.1 **Processor role.** This DPA applies where All Aboard processes Agent Personal Data as a processor on behalf of the Agent. The details of this processing are set out in Annex 1, Part A.

2.2 **Independent controller activities.** For the activities listed in Annex 1, Part B, including transmission of passenger data to train carriers and rail distribution partners for the issuance and servicing of tickets, payment processing, security logging, and processing required to comply with legal obligations, All Aboard acts as an independent controller and processes personal data in accordance with its Privacy Policy (allaboard.eu/privacy-policy). Those activities are outside the scope of this DPA.

2.3 **Agent as processor.** Where the Agent itself acts as a processor on behalf of its own customer (the controller), the Agent warrants that it has obtained all authorizations,

notices, consents, and documented instructions from the controller necessary for All Aboard to lawfully process the Agent Personal Data as contemplated by the Agreement, and All Aboard is engaged as a sub-processor of the Agent.

2.4 **Agent obligations.** The Agent is responsible for the lawfulness of the Agent Personal Data it submits, including having a valid legal basis and providing any required notices to data subjects. The Agent shall not submit special categories of personal data (Article 9 GDPR) or data relating to criminal convictions (Article 10 GDPR) through the services. One exception applies: disability or assistance data may be submitted where needed to book special assistance or meet accessibility requirements for a specific journey. All Aboard processes such data solely for that purpose.

3. Instructions

All Aboard shall process Agent Personal Data only on the Agent's documented instructions, including with regard to transfers to third countries, except where required by EU or Member State law or, where the UK GDPR applies, UK law. In the case of such a legal requirement, All Aboard will inform the Agent before processing, unless the law prohibits this.

The Agreement, this DPA, and the Agent's use of the API, Dashboard, and Embeds, including each order placed, constitute the Agent's complete documented instructions. Transmissions of passenger data that carriers, distribution partners, or underlying booking systems require in order to fulfill an order are made by All Aboard as an independent controller under Annex 1, Part B.

All Aboard shall notify the Agent without undue delay if it cannot comply with an instruction, and shall inform the Agent if, in its opinion, an instruction infringes the GDPR or other applicable data protection law.

4. Confidentiality

All Aboard ensures that all personnel authorized to process Agent Personal Data are bound by confidentiality obligations, whether contractual or statutory.

5. Security

All Aboard implements and maintains appropriate technical and organizational measures to protect Agent Personal Data, as required by Article 32 GDPR. These measures are summarized in Annex 2 and described in detail in the All Aboard Security & Data Protection Overview, published at allaboard.eu/security-policy. All Aboard may update its measures from time to time, provided that updates do not materially reduce the overall level of protection.

6. Sub-processors

6.1 **General authorization.** The Agent grants All Aboard a general written authorization to engage Sub-processors for the processing of Agent Personal Data. The current list of Sub-processors is maintained in section 4.4 of the Security & Data Protection Overview (allaboard.eu/security-policy) and summarized in Annex 3.

6.2 **Changes.** All Aboard will update the published list and notify the Agent at least thirty (30) days before authorizing a new Sub-processor to process Agent Personal Data. If the Agent has a reasonable, data-protection-related objection, the parties will work in good faith to resolve it. If no resolution is found, the Agent may terminate the affected services in accordance with the Agreement.

6.3 **Flow-down.** All Aboard imposes on each Sub-processor data protection obligations materially equivalent to those in this DPA and remains fully liable to the Agent for the performance of its Sub-processors.

7. Data subject rights

Taking into account the nature of the processing, All Aboard shall assist the Agent through appropriate technical and organizational measures, insofar as possible, in fulfilling the Agent's obligation to respond to data subject requests under Chapter III of the GDPR. If All Aboard receives such a request directly and can identify that it relates to the Agent, it will forward the request to the Agent without undue delay and will not respond to it except on the Agent's instruction or where required by law.

8. Personal data breaches

All Aboard shall notify the Agent without undue delay after becoming aware of a personal data breach affecting Agent Personal Data. The notification shall include, to the extent available, the information described in Article 33(3) GDPR. All Aboard shall provide reasonable cooperation and assistance in connection with the Agent's own notification obligations.

9. Assistance

Taking into account the nature of the processing and the information available to it, All Aboard shall provide reasonable assistance to the Agent in ensuring compliance with the Agent's obligations under Articles 32 to 36 GDPR (security, breach notification, data protection impact assessments, and prior consultations). All Aboard may charge a reasonable fee for assistance that exceeds what applicable data protection law requires of a processor.

10. Deletion and return

Upon termination or expiry of the Agreement, All Aboard shall, at the Agent's choice, return the Agent Personal Data in a structured, commonly used format and/or delete or anonymize it, in each case within ninety (90) days. If the Agent does not state a choice within thirty (30) days of termination, All Aboard deletes or anonymizes the data. This does not apply to personal data that All Aboard is legally required to retain (for example under the Swedish Accounting Act) or that All Aboard retains as an independent controller for the purposes listed in Annex 1, Part B, such as resolving disputes, handling chargebacks and refunds, and preventing fraud. Retained data is kept only as long as necessary for those purposes, remains protected under this DPA or All Aboard's Privacy Policy as applicable, and is deleted once the retention period or purpose expires.

11. Audits and information

All Aboard maintains adequate records of its processing and shall, upon written request, make available to the Agent the information reasonably necessary to demonstrate compliance with this DPA and Article 28 GDPR. This includes the Security & Data Protection Overview, relevant policies and security descriptions, responses to reasonable written security questionnaires, and summaries of relevant third-party assessments (such as penetration test reports).

If this information is reasonably insufficient to demonstrate compliance, the Agent, or an independent auditor mandated by the Agent that is not a competitor of All Aboard, may audit All Aboard's compliance with this DPA, including by inspection. Audits may take place at most once per twelve (12) months, require at least thirty (30) days' prior written notice, and are conducted during business hours, under confidentiality undertakings, with reasonable scope limitations, and without disrupting All Aboard's operations. The Agent bears the costs of an audit unless it reveals material non-compliance. These limits do not apply where an audit is required by Applicable Data Protection Law or a competent supervisory authority, or follows a personal data breach affecting Agent Personal Data.

12. International transfers

All Aboard stores Agent Personal Data within the EU, as described in section 5.2 of the Security & Data Protection Overview. All Aboard shall not transfer Agent Personal Data outside the EU/EEA (or, where the UK GDPR applies, outside the UK) unless the transfer is subject to a valid transfer mechanism under Chapter V of the GDPR or the UK GDPR, such as an adequacy decision, the EU Standard Contractual Clauses, the EU-US Data Privacy Framework, or the corresponding UK mechanisms. The Agent authorizes All Aboard to conclude such transfer mechanisms with Sub-processors in its own name where required.

13. Liability

The liability of each party under this DPA is subject to the exclusions and limitations of liability set out in the Agreement.

14. Term, precedence, and governing law

This DPA applies for as long as All Aboard processes Agent Personal Data and, with respect to retained data, until deletion under section 10 is complete. In the event of a conflict between this DPA and the Agreement concerning the processing of personal data, this DPA prevails. This DPA is governed by Swedish law, and the courts of Stockholm have exclusive jurisdiction, as set out in the Agreement.

Annex 1: Details of processing

Part A: Processing as processor (in scope of this DPA)

- **Subject matter:** Provision of the All Aboard services (API, Embeds, Dashboard) for planning, booking, and servicing rail and bus travel.
- **Duration:** The term of the Agreement, plus the retention period in section 10.
- **Nature and purpose:** Receiving, storing, and transmitting booking and passenger data submitted by the Agent in order to create, fulfill, modify, refund, and support orders; providing the Agent access to its bookings; travel-related communications where instructed.
- **Categories of data subjects:** The Agent's customers and travelers; the Agent's personnel using the services.
- **Categories of personal data:** Name, email address and phone number, date of birth where a fare or pass depends on it, discount or loyalty card numbers, passport number on rare occasions where required by a carrier, itineraries and ticketing details, and booking history. Special categories of personal data are not processed, except disability or assistance data where explicitly submitted by the Agent to book special assistance or fulfill accessibility requirements (see section 2.4).

Part B: Processing as independent controller (outside the scope of this DPA)

- Transmission of passenger data to train and bus carriers and to rail distribution partners as necessary to issue and service tickets; these parties receive the data as independent controllers.

- Payment processing through Stripe, using anonymized payment tokens, and reconciliation of incoming bank transfers for purchases of All Aboard Credits (payer name, account details, amount, and payment reference).
- Retention of booking and transaction records to comply with legal obligations (including the Swedish Accounting Act) and to resolve disputes, handle chargebacks and refunds, and prevent fraud.
- Security logging, fraud prevention, and service monitoring.
- Processing of the Agent's business contact details for account management, authentication, and billing.

Annex 2: Technical and organizational measures (summary)

Full details are maintained in the Security & Data Protection Overview at allaboard.eu/security-policy. In summary:

- Systems and production database hosted within the EU (UpCloud, Frankfurt, Germany), under EU jurisdiction.
- Encryption in transit (TLS 1.2 or higher) for all traffic and encryption at rest for the production database, backups, and logs.
- Full segregation of production, staging, and test environments; production data is not used in test environments.
- Least-privilege production access limited to designated engineers, reviewed on team changes and twice per year; multi-factor authentication enforced internally; credentials stored in secure password managers.
- Secure development lifecycle: mandatory code review, branch protection, signed commits, secrets scanning, automated and manual dependency management.
- Annual penetration testing by an independent external security firm (from 2026).
- Logging and monitoring; documented incident response process with breach notification commitments.
- Daily encrypted backups stored in the EU, with periodically tested restores.
- Personnel measures: confidentiality agreements, security awareness training, full-disk encryption on all work devices.

Annex 3: Sub-processors

All Aboard's current Sub-processors, including their roles and locations, are listed in section 4.4 of the Security & Data Protection Overview at allaboard.eu/security-policy, which constitutes the canonical list for the purposes of section 6 of this DPA. At the date

of this DPA, the Sub-processors are: UpCloud Oy (production hosting, Frankfurt, Germany); Cloudflare, Inc. (CDN and edge; US entity; personal data is processed transiently at edge locations and not stored there); Kinde Australia Pty Ltd (authentication; data stored in the EU); HODL s.r.o. (DBA Better Stack) (logging; data stored in the EU); Anthropic Ireland, Limited (AI assistants used by our staff; data may be processed outside the EU); and Intercom R&D Unlimited Company (customer support conversations; data stored in the US). Transfers to, or access from, outside the EU by any Sub-processor are safeguarded under the transfer mechanisms in section 12.

Train and bus carriers and rail distribution partners act as independent controllers when receiving personal data necessary to issue and service tickets, and are therefore not Sub-processors under this DPA. Stripe processes payments as described in Annex 1, Part B.