Security & Data Protection Overview

Version 1.8, 4 November 2026

Contact: security@allaboard.eu

Responsible for security & data protection: Patrik Stenmark, patrik@allaboard.eu, All Aboard AB

1. Introduction

This document supports external security and data protection evaluations of All Aboard. Commercial terms are covered separately in our Services Agreement (allaboard.eu/services-agreement), and current service status is available at status.allaboard.eu.

We review this document and our security policies at least once a year.

All Aboard provides ticket-booking services for trains and buses across Europe, serving end consumers, business customers, and travel agents. Our three core services are an API, embeddable booking widgets, and a booking dashboard.

2. Company overview

2.1 Legal entity and ownership

- Legal entity: All Aboard AB, org. no. 559214-7671
- Company address: Kivra 559214-7671, 106 31 Stockholm, Sweden
- Ownership: Privately held by founders and investors. Majority ownership and control by founders Anton Trollbäck and Carl Törnqvist.

2.2 Office and workspace

- Our office is located at Bohusgatan 27, 116 67 Stockholm, Sweden.
- Work takes place in Sweden and Germany.
- We allow remote work, but exclusively within the EU/EEA.

3. Compliance

3.1 Certifications and standards

All Aboard does not currently hold formal certifications such as ISO 27001 or SOC 2. Our security program is guided by the principles of these frameworks, and this document describes our practices transparently so that customers can evaluate them directly.

The infrastructure providers we build on hold recognized certifications:

- **UpCloud** (production hosting) is ISO 27001 certified and adheres to the CISPE Code of Conduct for cloud data protection in Europe.
- **Cloudflare** (edge network and CDN) is ISO 27001 certified and SOC 2 Type II audited.
- **Stripe** (payment processing) is a PCI DSS Level 1 certified service provider.

3.2 GDPR roles and data processing agreements

All Aboard processes personal data in accordance with the EU General Data Protection Regulation (GDPR). Depending on the service flow, we act either as an independent data controller (for example, for bookings made directly with us, payment processing, and the records the law requires us to keep) or as a data processor on behalf of our business customers.

Where we act as processor, our Data Processing Agreement (DPA) applies. It is published at allaboard.eu/dpa and is incorporated into our Services Agreement, so no separate signature is required. Questions and requests for countersigned copies can be sent to security@allaboard.eu.

3.3 Payment card data (PCI DSS)

All card payments are processed by Stripe (legal entity in section 4.4). Card details are entered directly into Stripe's hosted, PCI DSS compliant payment fields and are never stored on, or transmitted through, All Aboard's systems. We handle only pseudonymized payment tokens issued by Stripe, which keeps our own PCI DSS scope to a minimum.

3.4 Insurance

All Aboard carries cyber liability insurance with Länsförsäkringar Stockholm. A certificate of insurance is available on request from security@allaboard.eu.

4. Infrastructure

4.1 Architecture overview

Our infrastructure is divided into three technical parts to support our core services:

1. **The Internal API.** Responsibilities include the core booking flow, connections to databases and third-party payment systems, and our back-office system. Written in Elixir.
2. **The Gateway API.** Responsibilities include our public API endpoints that are documented for third-party use. Written in Node.js.
3. **The Frontends.** This includes our own website, our logged-in agent dashboard, and our embeddable booking widgets.

4.2 Hosting locations

- Our Internal API and production database are hosted with **UpCloud**, a European-owned cloud provider (legal entity in section 4.4), in the Frankfurt, Germany data center (DE-FRA1). Our systems and production database are in the EU, under EU jurisdiction. The cases where personal data is stored or processed outside the EU are listed in section 5.2.
- Our Gateway API and the Frontends run on **Cloudflare Workers**, in the Cloudflare data center closest to each user. They do not run only in the EU. Traffic, including personal data, passes through them transiently and is encrypted end to end. Cloudflare stores personal data in two cases only: sign-in sessions, kept in Cloudflare Workers KV for up to 90 days, and limited request logs that Cloudflare keeps for security and troubleshooting. Apart from these and the cases listed in section 5.2, personal data is stored in the EU. Cloudflare additionally provides network-level protection, including a firewall, DDoS mitigation and traffic filtering, in front of all our services.

4.3 Data flow

For the booking widgets, API, website, and dashboard:

Client → Cloudflare CDN → Frontends (Cloudflare Workers) → Internal API (UpCloud, Frankfurt) → Third-party rail providers → Train operators

4.4 Third-party providers and sub-processors

All Aboard relies on third-party providers for functions such as authentication, timetables, and ticket booking. Some receive passenger data and may pass it on to the train operators. Every provider with access to any personal data is listed below, together with its role:

- **UpCloud Oy** (Aleksanterinkatu 15 B, 7th floor, 00100 Helsinki, Finland): production hosting, Frankfurt (DE) data center.
- **Cloudflare, Inc.** (101 Townsend St, San Francisco, CA 94107, USA): CDN and edge computing. Our Workers run in the Cloudflare data center closest to each user, which

may be outside the EU. Personal data is stored only as sign-in sessions, for up to 90 days, and limited request logs kept for security.

- **Stripe Payments Europe, Limited** (One Wilton Park, Wilton Place, Dublin 2, D02 FX04, Ireland): payment processing. Data is transferred to Stripe, LLC in the US under the EU-US Data Privacy Framework and standard contractual clauses.
- **Kinde Australia Pty Ltd** (Suite 2, Level 5, 6-10 O'Connell Street, Sydney, Australia): authentication; data stored in the EU (AWS Dublin).
- **HODL s.r.o. (DBA Better Stack)** (Rybná 716/24, 110 00 Prague, Czech Republic): logging; data stored in the EU (AWS Frankfurt).
- **Anthropic Ireland, Limited** (6th Floor, South Bank House, Barrow Street, Dublin 4, D04 TR29, Ireland): AI assistants used by our staff (section 5.6); data may be processed outside the EU.
- **Plausible Insights OÜ** (Västriku tn 2, 50403 Tartu, Estonia): privacy-friendly, cookie-less web analytics across our services; no passenger or booking data; data stored in the EU (Falkenstein, Germany).
- **ActiveCampaign, LLC (DBA Postmark)** (1 North Dearborn Street, 5th floor, Chicago, IL 60602, USA): emails with tickets, booking confirmations and journey updates, containing contact and travel details. Data stored in the US (Deft data center near Chicago, and AWS), with email content kept for 45 days. Transfers under the standard contractual clauses in Postmark's DPA.
- **Astrodon Corporation (DBA Loops)** (450 SW Gemini Dr PMB 22902, Beaverton, OR 97008, USA): newsletter emails. Email address and first name only, no passenger or booking data. Data stored in the US, transfers under the EU-US Data Privacy Framework.
- **Intercom R&D Unlimited Company** (124 St Stephen's Green, Dublin 2, D02 C628, Ireland): customer support conversations, including the chat on our websites, in the dashboard and on agents' booking sites where it is turned on. Holds the name and email address of signed-in users and of people booking, and the messages they send. Data stored in the US (AWS N. Virginia), transfers under the EU-US Data Privacy Framework and standard contractual clauses.

Train operators described in section 4.5, act as independent data controllers when receiving passenger data in order to issue and service tickets. Where a provider or its parent company is established outside the EU/EEA, transfers of personal data are safeguarded through EU Standard Contractual Clauses and/or the EU-US Data Privacy Framework, as applicable. The current list is kept at allaboard.eu/trust/subprocessors. We notify agents at least 30 days before a new sub-processor starts processing their data (DPA section 6.2).

4.5 Train operators

Booking a ticket requires exchanging passenger data with the operator in question. We book tickets from hundreds of train and bus operators, including the incumbent state-

owned operators in each EU country and many private operators across Europe. We do not list them here; a current overview is available at allaboard.eu/inventory.

4.6 Physical security

All production systems run in professionally operated third-party data centers with industry-standard physical protections, including controlled access, surveillance, and redundant power and cooling. Our office does not host any production systems or customer data; the only company data on site resides on employee devices, which are protected as described in section 7.3.

5. Data handling

5.1 Categories and purposes

- **Personal data.** Including: name, email, phone, date of birth where a fare or pass depends on it, discount or loyalty card numbers, and on rare occasions passport number. Purpose: required by the operators for issuing tickets and for travel communications. We also store the name and email of our business clients for billing and for authentication with our provided services.
- **Travel data.** Including: itineraries and ticketing details. Purpose: ticket bookings and customer support.
- **Assistance needs.** Including: wheelchair space or other assistance requested for a journey. Purpose: passed to the operators on the route so that they can provide the assistance, and kept to handle related claims (section 5.4). Used for nothing else.
- **Payment data.** Including: pseudonymized tokens provided by our payment partner Stripe. Purpose: processing payments from our end customers (section 3.3). For business customers buying All Aboard Credits by bank transfer, we also process the transfer details visible to us as the recipient (payer name, account number, amount, and payment reference). Purpose: crediting the correct account and bookkeeping.
- **Logging data.** Including: IP address, user actions, and statistics. Purpose: security and debugging.

5.2 Storage locations

- Our Postgres production database is hosted with UpCloud in the Frankfurt, Germany (DE-FRA1) data center.
- Our logging data is stored and managed by Better Stack in the AWS Frankfurt data center.
- Our authentication partner Kinde stores and manages data in the AWS Dublin data center.

- Our analytics partner Plausible stores and manages data in its data center in Falkenstein, Germany.
- Our booking email provider Postmark stores the emails it sends in the US for 45 days.
- Our newsletter provider Loops stores subscribers' email addresses and first names in the US.
- Our customer support provider Intercom stores support conversations, and the names and email addresses of the people writing to us, in the US.
- Our payment provider Stripe transfers payment data to Stripe, LLC in the US.
- Our edge provider Cloudflare keeps sign-in sessions for up to 90 days, and limited request logs for security and troubleshooting, on its global network.

Our systems and production database are in the EU. Apart from the US providers listed above, personal data leaves the EU only in these cases: Cloudflare handles traffic in the data center closest to each user and keeps sign-in sessions and limited logs on its global network (section 4.2), our AI provider may process data outside the EU (section 5.6), and operators outside the EU/EEA receive passenger details when a journey goes there. Transfers are safeguarded as described in section 4.4.

5.3 Encryption

- All traffic is encrypted in transit using TLS 1.2 or higher: between clients and our edge, between the edge and our Internal API, and between our systems and third-party providers.
- Personal data is encrypted at rest, including the production database, database backups, and log storage.

5.4 Retention and deletion

- Accounting records (booking reference, passenger names, what was bought, amounts, dates and payment details) are retained for seven years after the end of the calendar year in which the booking was made, as required by the Swedish Accounting Act (Bokföringslagen), after which they are deleted.
- Date of birth, passport or ID numbers, discount card numbers and assistance needs are deleted 12 months after the last travel date.
- Support conversations are retained for 24 months after the matter is closed.
- Logging data is retained for 12 months.
- When a business customer relationship ends, the customer's data is deleted or anonymized within 90 days, except for records we are legally required to retain (see above).

5.5 Data subject rights

We support the rights of data subjects under GDPR, including access, rectification, and erasure. Erasure requests are honored except where we are legally required to retain the data (see 5.4), in which case the data is deleted once the retention period expires. Requests about bookings made through an agent are forwarded to that agent, which decides on them as controller (DPA section 7). Requests can be sent to security@allaboard.eu and are handled without undue delay.

5.6 AI and machine learning

We do not use customer or passenger data to train AI or machine learning models, and our AI provider (legal entity in section 4.4) is contractually barred from using the data we send it to train its models.

Our staff use AI assistants in two areas:

- **Software development.** AI assistants help our engineers write and review code. They work with our source code and with development databases that hold anonymized data.
- **Operations and customer support.** AI assistants help our staff investigate bookings, failed orders, refunds and support cases. They read booking records, including passenger personal data, through an internal interface that requires the employee's own login and administrator rights. Every record they read is logged in our audit trail under that employee's name.

AI does not make decisions that have legal or similarly significant effects on individuals. Any change in how we use AI with personal data is announced through our sub-processor notification process before it takes effect.

6. Application security

6.1 Environment separation

Our three technical parts (Frontends, Gateway API, and Internal API) are fully segregated, including at network level. Our staging, testing, and production environments are also fully isolated, and we do not use production data in staging or test environments.

6.2 Authentication

- **Dashboard and widget users** are authenticated through our authentication provider Kinde using passwordless login: one-time codes delivered by email. We do not support passwords as a login method, which eliminates entire categories of password-related attacks such as credential stuffing and password reuse. For business customers, we also support enterprise single sign-on (SSO/SAML), provided via Kinde.
- **API customers** are authenticated using OAuth 2.0, and each API client has its own credentials.

6.3 Secure development and vulnerability management

- Our code is hosted on GitHub with branch protection, signed commits, and secrets scanning that keeps credentials out of the codebase. All code changes are reviewed by someone other than their author before they are merged, so no one ships a change on their own.
- Dependencies are monitored continuously. Security patches are applied through automated pull requests, complemented by manual dependency reviews every two weeks.
- Beginning in 2026, we commission annual penetration tests of our services by an independent external security firm.
- We welcome responsible disclosure of suspected vulnerabilities at security@allaboard.eu and commit to acknowledging reports promptly.

6.4 Logging and monitoring

- Our systems' logs are stored centrally with Better Stack (section 5.2), apart from the systems that produce them, and kept for 12 months (section 5.4).
- System clocks are synchronized, so timestamps line up across our systems and logs.
- Our systems raise alerts, and we have routines for reviewing logs and alerts.
- We monitor resource usage and add capacity before our systems run short.

7. Access control and personnel security

7.1 Employee access

Production access is limited to designated engineers on a least-privilege basis. They reach production systems over encrypted SSH connections, authenticated with SSH keys. Third parties, such as our providers' support staff, get access to our systems only when it is needed and for as long as it is needed, and their access is monitored. Access rights are reviewed whenever a team member joins or leaves the working group, and through recurring access reviews twice per year.

7.2 Logins and credentials

Everyone at All Aboard has their own personal accounts, and no one shares an account. We enforce multi-factor authentication across all company systems. Any shared keys and credentials are stored exclusively in secure password managers. Default passwords and other vendor-supplied credentials are changed before a system is put into use.

7.3 Personnel practices

- All employees sign confidentiality agreements (NDAs).
- All work devices use full-disk encryption.
- All work devices have malware protection, kept up to date.
- Work devices are returned when someone leaves, and are wiped securely before they are reused or disposed of.
- Employees receive security awareness training.

8. Incident response and breach notification

We maintain an incident response process covering detection, assessment, containment, remediation, and post-incident review.

If a personal data breach affects data we hold as controller, we notify the Swedish Authority for Privacy Protection (IMY) within 72 hours where required under GDPR. Where the UK GDPR applies to the affected processing, we notify the UK Information Commissioner's Office (ICO) within the same 72-hour window. We also inform affected customers without undue delay.

If a breach affects data we process for an agent as processor, we notify the agent without undue delay and no later than 48 hours after becoming aware of it, as set out in section 8 of our DPA, so that the agent can notify its supervisory authority.

Our notifications include the nature of the incident, the data concerned, and the measures taken.

9. Backups and continuity

- Our production database is backed up automatically every day. Backups are encrypted and stored within the EU.
- We test restoring from backups twice a year.
- Our frontends and Gateway API run on Cloudflare's globally distributed edge network, and our Internal API runs on redundant infrastructure at UpCloud, limiting the impact of individual server failures.