Security

Version: 4 November 2026

Atlas Pickup Points is built and operated with a focus on data minimisation, European Union data residency and defence-in-depth security. This page summarises the technical and organisational measures we apply to protect merchants and their buyers, and links to the binding commitments in our Terms of Service, Entrustment Agreement (DPA) and Privacy Policy.

Infrastructure and EU data residency

- European Union hosting: The application and its databases are hosted in data centres located within the European Union.
- Managed cloud infrastructure: Production workloads run on managed cloud infrastructure in the European Union, hosted in data centres certified under ISO/IEC 27001 and SOC 2.
- Subprocessors: Every third party that processes personal data on our instructions is listed at https://atlaspickuppoints.com/legal/subprocessors, together with the service provided, place of processing and GDPR Chapter V transfer basis. Merchants receive at least 7 days' advance notice by email before any new subprocessor is engaged.

Encryption and authentication

- Encryption in transit: All traffic between buyers' browsers, merchants' devices, Shopify and our infrastructure is encrypted in transit using TLS.
- No standalone credentials or cookies: The application runs exclusively inside the Shopify ecosystem and does not maintain separate user passwords or install cookies of its own. Access in the Shopify administrative console is authenticated on every session using short-lived session tokens issued by Shopify. The only information kept in the browser is the merchant's selected interface language, in local storage, and the identifier of an error-triggered session recording, in session storage, which is discarded when the tab is closed.
- Payment security: Subscription billing is handled entirely by Shopify. Atlas Pickup Points never collects, processes or stores payment card details.

Access control

- Least privilege: Access to production systems and personal data is restricted to personnel for whom it is necessary to provide and support the service, is granted individually and requires strong authentication.
- Merchant store access: Our support team accesses a merchant's Shopify store only with the merchant's permission – through a staff or collaborator account the merchant grants and can remove at any time in the Shopify administrative console (§ 5 Section 14 of the Terms of Service). To investigate a support request, authorised support personnel can also open the App as the merchant's store, within the access the merchant approved when installing the App.
- Confidentiality: All personnel authorised to process personal data are bound by confidentiality obligations (§ 3 Section 2 of the Entrustment Agreement).

Privacy by design and error diagnostics

- No third-party analytics or advertising trackers: We do not use third-party analytics or advertising trackers, and we do not profile merchants or buyers. Technical and diagnostic logs are recorded first-party on our own EU servers to operate and secure the application.
- Masked error diagnostics: To diagnose technical faults in the administration interface, an error report and an error-triggered session recording are captured only when an error occurs, with the content of form fields masked. Nothing is recorded during error-free sessions, and diagnostic data are retained for a maximum of 30 days.
- Google Maps: The pickup-point map displayed in the application is provided by Google Maps under the merchant's own Google Maps API key and is governed by the agreement between the merchant and Google.

AI governance

- No training on merchant or buyer data: We contractually warrant (§ 5 Section 18 of the Terms of Service) that merchant and buyer data are never used to create or train any AI systems.
- Human oversight: AI-based tools are used under the oversight of our personnel to assist with and respond to technical support inquiries, while all binding decisions remain with a human.

Data retention, portability and deletion

- 30-day post-termination deletion: When a merchant uninstalls the application or terminates the Service Agreement, all entrusted personal data and merchant data are deleted within a maximum of 30 days (§ 5 Section 19 of the Terms of Service and § 7 of the Entrustment Agreement), unless retention is required by mandatory law.
- Data export: During the 30-day window following termination, merchants may request an export of their data in a structured, commonly used and machine-readable format.

Incident response and breach notification

- 24-hour breach notification: In the event of a personal data breach affecting entrusted data, we notify the affected merchant without undue delay and no later than within 24 hours of discovering the breach (§ 3 Section 4 point 1 of the Entrustment Agreement).
- Compliance and audit rights: We provide merchants with documentation necessary to demonstrate GDPR Article 28 compliance within 14 days of a request and support merchant audits in accordance with § 3 Sections 6–10 of the Entrustment Agreement.

Reporting a security issue

If you discover a potential security vulnerability or have a question about how Atlas Pickup Points protects data, please contact us at security@atlaspickuppoints.com.

This page describes our technical and organisational measures for information purposes. The binding commitments are those set out in our Terms of Service, the Entrustment Agreement (Appendix No. 1 to the Terms of Service) and our Privacy Policy; in the event of any inconsistency, those documents prevail.