TRUST & PROCUREMENT

Everything a procurement review needs, on one page.

The claims a Nordic B2B buyer checks — data residency, GDPR posture, sub-processors, backup and recovery, and security controls — stated exactly as they are, with links to the underlying documents and a downloadable pack for your file.

DATA RESIDENCY

Primary processing in the EU — transfers named and covered

Primary processing in the EU (Azure Sweden Central); a small set of US sub-processors under EU Standard Contractual Clauses.

Primary data in Azure Sweden Central (EU)

All application compute, the PostgreSQL database, object storage, the message bus, monitoring and key management run in Microsoft Azure's Sweden Central region. This is where all primary personal data lives.

A small set of US sub-processors, under SCCs

A limited number of sub-processors (for example email/SMS delivery and browser map tiles) process some personal data in the USA. Those transfers are covered by EU Standard Contractual Clauses, and the EU–US Data Privacy Framework where the recipient is certified.

We don't claim more than that

We deliberately avoid implying that data never leaves the EU, because a few named sub-processors sit outside it. The full list, with purpose, location and transfer basis, is in the sub-processor table below and in the DPA.

GDPR & DATA RIGHTS

Subject rights that are actually implemented, not promised

Stockisto is built for European B2B customers. Erasure and portability are shipped features with a signed DPA behind them — not roadmap items.

Right to erasure (Art. 17)

Account and end-user data can be deleted on request. Deletion is a real, evaluated workflow in the platform — not a manual promise — and consumer reservation details are additionally erased automatically 30 days after a reservation expires.

Right to data portability (Art. 20)

A tenant's data can be exported in a structured, machine-readable form through a dedicated export path, so a customer can take their data with them.

Data Processing Agreement (Art. 28)

A full DPA is authored and available — Art. 28 processor terms, Standard Contractual Clauses, and an Annex naming every sub-processor. It is linkable and ready to sign as part of your review.

Data minimisation

We collect only the data needed to run the discovery and analytics product. Discovery and usage analytics carry no consumer identity and do not store the client IP.

SUB-PROCESSORS

Every third party that touches personal data

SUB-PROCESSOR	PURPOSE	LOCATION	TRANSFER
Microsoft Azure	Cloud hosting and infrastructure — application compute, the PostgreSQL database, object storage, the message bus, monitoring and key management. This is where all primary personal data lives.	EU — Sweden Central	Within the EU — no third-country transfer
Microsoft Azure OpenAI Service *	Optional AI assistance that drafts supplier-to-retailer outreach text. It processes retailer business-contact data, never consumer reservation data.	EU (within the Azure tenancy)	Within the EU — no third-country transfer
Twilio (incl. SendGrid) *	Delivery of transactional and lifecycle email via SendGrid — invitations, confirmations and notifications — and of SMS phone-verification codes via Twilio's messaging API, which receives the account user's phone number when they verify it.	USA	SCCs, and the EU–US Data Privacy Framework where the recipient is certified
Stripe	Subscription billing and card-payment processing for paying suppliers. Stripe acts as an independent controller for the payment data it collects, under its own terms.	EU / USA	SCCs, and the EU–US Data Privacy Framework where the recipient is certified
Google (Google Ireland Ltd)	"Sign in with Google" authentication for account users who choose it. Google acts as an independent controller for the authentication data under its own terms.	EU / USA	SCCs, and the EU–US Data Privacy Framework where the recipient is certified
Mapbox	Rendering map tiles in the browser on the consumer Locator, the embeddable Widget and the Installer Portal. Receives the coarse map view and the requesting IP inherent to serving tiles — never reservation contact details.	USA	SCCs, and the EU–US Data Privacy Framework where the recipient is certified
OpenStreetMap / Nominatim	Server-side geocoding of retailer business addresses into map coordinates during catalogue import.	EU	Within the EU — business address data only

DNS is served by Cloudflare; no personal data is proxied or processed.

BACKUP & RECOVERY

Backed up in production, and the restore is actually rehearsed

In production, the database is backed up point-in-time with up to 35 days of retention, geo-redundant within the EU. Point-in-time restore is drill-tested on real infrastructure (most recent drill: July 2026).

35-day geo-redundant backups in production

The production PostgreSQL database is backed up with point-in-time restore and up to 35 days of retention, geo-redundant within the EU. Non-production environments are backed up on a shorter window and are not geo-redundant.

Recovery targets (not guarantees)

We work to internal recovery targets of at most 1 hour of data loss (RPO) and at most 4 hours to restore service (RTO). These are operational targets we design and test against, not a contractual guarantee.

Drill-tested restore

Point-in-time restore is drill-tested on real infrastructure — the most recent drill (July 2026) restored the database, confirmed row-count parity against the source, and tore the copy down cleanly.

SECURITY CONTROLS

The controls, in brief — the full list is on /security

A short summary of the controls a reviewer asks about first. The complete, per-control breakdown lives on our Security page.

- Multi-tenant isolation enforced in the data layer — a global query filter constrains every read to the calling tenant, an insert-time guard blocks tenant-less writes, and cross-tenant tests run in CI on every change.
- Short-lived (15-minute) JWT access tokens with an HttpOnly refresh cookie that rotates on every use and detects replay of a spent token.
- TLS everywhere with HSTS, a restrictive Content-Security-Policy and security headers on every response, plus per-tenant rate limiting and automatic abuse blocking.
- Encryption in transit (TLS) and at rest (managed storage encryption), with privileged tenant actions written to an audit log.

SUPPORT

A real inbox, a stated response expectation

- General support and product questions: help@stockisto.com. We reply within one business day.
- Security reports and disclosure: security@stockisto.com. We acknowledge good-faith reports and coordinate a fix.
- We do not offer a formal, contractual response-time SLA yet, and we would rather tell you that than imply one.

WHAT WE DON'T CLAIM

The honest part of a procurement review

- We are not ISO 27001 certified, and we won't imply otherwise. The concrete controls we do run are listed on our security page.
- We are not SOC 2 audited. There is no SOC 2 report to hand you today.
- We offer no contractual uptime SLA. We run the service carefully and monitor it, but we don't sell a guaranteed-uptime number we can't yet stand behind.
- We do not claim data never leaves the EU. A small set of named US sub-processors is covered by Standard Contractual Clauses, and we list every one.