

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 runs in the EU (Azure Sweden Central). A small set of US sub-processors operates under EU

Primary Data in Azure Sweden Central (EU)

All application compute, the PostgreSQL database, object storage, the message bus, monitoring and key management

A small set of US sub-processors under SCCs. primary personal data lives there.

A few sub-processors (for example email/SMS delivery and browser map tiles) process some personal data in the

USA. EU Standard Contractual Clauses cover those transfers. Where the recipient is certified, the EU-US Data Privacy Framework applies too.

We don't claim more than that. data never leaves the EU. 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

Stocksto is built for European B2B customers. Erasure and portability are shipped features with a signed DPA behind

Right to erasure (Art. 17)

You can have account and end-user data deleted on request. Deletion is a real, evaluated workflow in the platform, not

Right to data portability (Art. 20)

Reservation details are also erased automatically 30 days after a reservation expires.

You can export your tenant's data in a structured, machine-readable form through a dedicated export path. You can take

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 are linkable and ready to sign as part of your review.

We collect only the data needed to run the discovery and analytics product. Discovery and usage analytics carry no

consumer identity. They 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,	EU (Sweden Cen-	Within the EU: no
Microsoft Azure OpenAI Service	Monitoring and key management. Supplier to retailer outreach	EU (within the Azure	Within the EU: no
* TypeSafe AI, Inc. *	text processing, retailer business-contact data, never con- Optional automated checks and suggestions on catalogue sumer reservation data. data, business records and text submitted through forms. Structured contact fields of a person are never sent, and email	tenancy) USA	third-country trans- SCCs only: fer the Commission's Standard Contrac-
OpenAI *	address reading from public web pages, such as from the first Google keeps search results with the record and the card does. The data and text of the page goes to TypeSafe API,	USA	SCCs and the EU-US Data Pri- vacy Framework
Twilio (incl. SendGrid) *	publishes data in the USA and does not process data in the EU. (a simple to page actions and notifications) and of SMS	USA	SCCs and the EU-US Data Pri- vacy Framework
Stripe	Subscription billing and card-payment processing for paying reservations account user's phone number when they verify suppliers. Stripe acts as an independent controller for the	EU / USA	is certified SCCs, and the EU-US Data Pri- vacy Framework
Google (Google Ireland Ltd)	Sign in with Google authentication for account users who choose it. Google acts as an independent controller for the	EU / USA	is certified SCCs, and the EU-US Data Pri- vacy Framework
Mapbox	Rendering map tiles in the browser on the consumer Locator, the embeddable Widget and the Installer Portal. Receives the	USA	is certified SCCs, and the EU-US Data Pri- vacy Framework
Cloudflare, Inc. *	coarse map view and the requesting IP inherent to serving. Bot protection on the public sign-up contact and newsletter forms (Cloudflare Turnstile). The check receives the visitor's	EU / USA	is certified SCCs, and the EU-US Data Pri- vacy Framework
OpenStreetMap / Nominatim	IP address and signals from the browser, never what was typed into the form.	EU	is certified SCCs, and the EU-US Data Pri- vacy Framework
Kartverket	map coordinates during catalogue import. Server-side geocoding of Norwegian business addresses into map coordinates. © Kartverket.	Norway (EEA)	is certified SCCs, and the EU-US Data Pri- vacy Framework

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

data only

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. We drill-test the restore 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 use a shorter window and are not geo-redundant.

Recovery targets (not guarantees)

We work to internal recovery targets: 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

We drill-test point-in-time restore 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.

PROVENANCE

A store's stock answer names the retailer and the date

An answer that names the retailer who confirmed it, and when, carries more weight than one that doesn't. That's the whole claim: retailer-confirmed stock, with the date, not a certification.

The retailer, named

A store's stock answer names the specific retailer who confirmed it. It traces back to a real store, not an anonymous feed.

The date, shown

A store's stock answer carries the date it was confirmed, so the reader can judge how current it is before acting on it.

Not a certification

Naming a retailer and a date is not a certification, an audit, or a guarantee. It's a dated answer from the store itself, stated as exactly that.

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 breakdown, control by control, 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

Support and security both reach a monitored inbox.

- 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. We would rather tell you that than imply one.

WHAT WE DON'T CLAIM

The honest part of a procurement review

Buyers get burned by vendors that imply certifications they don't hold. We'd rather state the gaps up front. It's faster for your review, and it's simply true.

- 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.
- No self-serve plan carries a contractual uptime SLA. We run the service carefully and monitor it, and our targets are on the SLA page. An Enterprise agreement can set contractual terms, and it is agreed at sale rather than promised here.
- We do not claim data never leaves the EU. A small set of named US sub-processors operates under Standard Contractual Clauses. We list every one.