



CRYSTALLINE

INFORMATION SECURITY POLICY

Data Protection Policy

Crystalline Logistics Platform

Crystalline Supply Chain Solutions Ltd

Registered in Scotland · Company No. SC900213

Summit House, 4-5 Mitchell Street, Edinburgh EH6 7BD

Document ref: CRYSPOL-DP-01

Version 0.1 · Draft

Issued: 27 August 2026

Owner: Lewis · Lewis@crystalline-solutions.com

This policy defines how client data held within the Crystalline Logistics platform is handled, protected, retained and deleted, and how data subject rights are supported where applicable.

1 Purpose & Scope

This policy applies to all client data processed through the platform, including operational logistics data and any personal data contained within it. It applies to all systems used to operate the platform and to all individuals with access to that data.

2 Principles

Client data is handled in line with the following principles:

- **Lawfulness and purpose** — data is processed only for the purpose of operating the logistics service for the client.
- **Minimisation** — only the data required to deliver the service is held.
- **Accuracy** — data is kept accurate and corrected where errors are identified.
- **Storage limitation** — data is retained only as long as required (see Retention).
- **Integrity and confidentiality** — data is protected against unauthorised access, loss or damage.

3 Data Categories

CATEGORY	EXAMPLES
Operational data	Equipment, movements, manifests, load lists, dispatch records
Contact data	Names and business contact details of client personnel
Account data	User identities and access records for the platform

The platform is not designed to hold special-category personal data, and clients are asked not to enter such data into it.

4 Storage & Location

- Client data is held within the platform's data and storage layers, which run on established cloud infrastructure providers.
- Where a client requires data to reside within their own systems, the platform can interface with the client's own storage or environment as agreed.
- Generated documents are stored in a controlled storage location with access restricted to authorised users.

5 Access & Protection

- Access to client data is restricted to authorised users on a least-privilege basis, as set out in the Access Management Policy.
- Individual accounts are protected by multi-factor authentication.
- Data in transit between systems is protected using encryption provided by the underlying platforms.
- Automated integrations authenticate using scoped API tokens, stored securely and rotated periodically.

6 Retention

Client data is retained for the duration of the service engagement and for an agreed period thereafter, after which it is deleted or returned to the client as agreed.

DATA	RETENTION
Active operational data	Retained for the duration of the engagement
Data after engagement ends	Retained for an agreed period, then deleted or returned as agreed with the client
Backups	Retained on a rolling basis and overwritten in the normal backup cycle

Specific retention periods are agreed with each client and recorded in the relevant service agreement, where they differ from the defaults above.

7 Data Subject Rights

Where the platform holds personal data, the following rights are supported in cooperation with the client as data controller:

- Access to the personal data held
- Correction of inaccurate data
- Deletion of data where there is no continuing requirement to retain it

Requests received directly are referred to the relevant client, who is ordinarily the data controller for the data held on their behalf.

8 Deletion

- On request or at the end of the agreed retention period, data is deleted from the active platform.
- Residual copies in backups are removed in the normal backup overwrite cycle.
- Deletion is confirmed to the client where requested.

9 Responsibilities & Review

The Administrator is responsible for applying this policy. All users are responsible for handling client data in line with it. This policy is reviewed at least annually, or sooner following any significant change to the platform or applicable law.



Client data is held only for as long as required, protected against unauthorised access, and deleted or returned at the end of the engagement.

Crystalline Supply Chain Solutions Ltd
Registered in Scotland · Company No. SC900213
Lewis@crystalline-solutions.com
Document ref: CRY-S-POL-DP-01 · v0.1