

MURAJA

DATA SECURITY & HANDLING

How Muraja handles client freight information

Version 1.0 | Prepared 28 August 2026 | muraja.ae

Pre-launch security statement

Muraja is currently in its pre-launch and validation stage and is not yet incorporated as a legal entity. This document sets out the data-handling controls and workflow Muraja intends to operate when accepting client documents. It is not a security certification and does not claim ISO 27001, SOC 2 or any government security accreditation. The document will be updated when the production technology providers and legal entity are finalised.

Muraja reviews commercially sensitive freight records, including invoices, quotations, rate cards, contracts, Bills of Lading and shipment data. Our security approach is therefore based on a simple principle:

YOUR FREIGHT DATA STAYS CONTROLLED.

Security at a glance

- Start small: the initial review begins with 30 freight invoices and the corresponding quotes or rate agreements.
- Private transfer: client documents are not requested through a public website enquiry form.
- Restricted access: client files are kept in restricted business storage and are not intended to be visible to other clients.
- AI assists; people decide: technology can structure and flag data, but a material discrepancy is verified by a human before it is presented.
- Minimum necessary data: Muraja requests additional shipment evidence only where it is needed to verify a specific issue or perform the agreed analysis.
- Confidential use: client information is used only to provide the agreed Muraja service and related administrative or legal requirements.

1. The Muraja security workflow

The workflow is designed to keep the document journey clear from the moment a client shares information through to the final evidence pack.

01	02	03	04	05
Secure upload	Restricted review	AI-assisted analysis	Human verification	Evidence pack

Secure upload

Each client is provided with a private document-transfer location for the agreed files. The public website enquiry form is used for contact information and qualification, not for uploading commercially sensitive freight documents.

Restricted review

Client files are organised within restricted business cloud storage. Access is limited to authorised Muraja personnel who need the information to perform that client review. Client workspaces are kept separate so one client is not intended to see another client's files.

AI-assisted analysis

Technology can help extract, organise, compare and flag potential anomalies across large volumes of freight data. Where client information is processed by AI, Muraja intends to use commercial business environments with data-protection terms rather than public or free consumer tools.

Human verification

An AI flag is not a confirmed finding. Muraja checks the invoice, quotation, rate agreement, contract and supporting shipment evidence relevant to the issue before presenting a material discrepancy.

Evidence pack

Confirmed findings are presented with the supporting commercial evidence needed to understand the issue and, where applicable, support correction or recovery. Muraja does not simply return an unverified AI output.

2. What information is handled

Muraja is a freight spend recovery and intelligence service, not a transport-management system. The information requested is limited to the agreed review.

Muraja Recovery	Muraja Intelligence
Invoices, quotations, rate cards or contracts, and supporting shipment evidence where needed.	Shipment data, freight history, operational charge data and rate comparisons within the agreed scope.
Purpose: identify and support correction or recovery of incorrect freight charges.	Purpose: identify avoidable freight spend, recurring leakage and opportunities for better cost control.

Start with 30 invoices

The initial pilot does not require a client to hand over its entire logistics operation. Start with 30 freight invoices and the corresponding quotes or rate agreements. Additional shipment documents are requested only where they are needed to verify a finding.

3. Access and storage controls

Muraja's objective is to keep client freight information within a small, controlled set of business systems rather than spreading documents across personal devices or informal channels.

- Private client location: client documents are transferred into a private workspace or upload location provided for that engagement.
- Restricted permissions: access is limited to authorised Muraja personnel involved in the client work.
- Client separation: files are organised by client and engagement; one client does not receive access to another client's workspace.
- Business storage: production client files are intended to be kept in business cloud storage rather than personal consumer storage accounts.
- Need-to-know access: if Muraja later expands its team, access should be granted only to personnel who require the files for that engagement and removed when no longer needed.
- Controlled sharing: files should not be forwarded externally unless this is required for the agreed service, authorised by the client, or permitted by applicable law.

About encryption and technical standards

Muraja will select production service providers that offer standard business security controls for data transmission, storage and account access. Until the production providers and configurations are finalised, Muraja does not claim a particular encryption standard or security certification.

4. AI-assisted processing

AI is used as an analysis aid, not as the final authority on whether a freight charge is valid.

- AI may help extract invoice data, organise charge lines, standardise formats, compare documents, identify unusual patterns and flag possible discrepancies.
- Muraja intends to use commercial AI environments with business data protections where client information is processed.
- Client documents are not intended to be uploaded into public or free consumer AI tools for service delivery.
- A potential discrepancy is reviewed against the underlying commercial evidence before it is presented as a finding.
- AI does not make the final recovery decision and does not independently communicate claims to a carrier or freight forwarder.
- Muraja does not use client freight documents to train public AI models or for unrelated advertising.

AI Finds It. We Verify It. You Recover It.

Technology helps Muraja review large volumes of freight data efficiently. Potential findings are flagged for review, but every material discrepancy is verified by a human before it reaches the client.

5. Minimum necessary data

The safest document is often the document that does not need to be collected. Muraja therefore applies a minimum-necessary approach.

- The free initial review starts with the smallest useful dataset: 30 freight invoices plus the corresponding quotes or rate agreements.
- Bills of Lading, shipment records, contracts or other supporting documents are requested only where they are needed to verify a finding or complete the agreed analysis.
- Clients should avoid sending personal or sensitive information that is not relevant to the freight review.
- If a document contains information that is not needed, Muraja may ask the client to provide a more limited version where practical.

6. Third-party business systems

Muraja may rely on specialist third-party business services to host the website, receive email, store client files, manage workflow and support AI-assisted analysis.

- Providers are selected for a defined business purpose and should receive only the information needed to provide that service.
- Where relevant, Muraja intends to use business or enterprise service arrangements with contractual confidentiality and data-protection terms.
- Some providers may process or store information outside the UAE. International handling of personal data will be addressed in the Muraja Privacy Policy and managed in accordance with applicable data-protection requirements.
- The final production provider list will be documented once the technology stack is confirmed.

7. Retention and deletion

Client files should not remain in active systems indefinitely. Retention is linked to the purpose of the engagement.

- Free pilot files: normally deleted or returned within 90 days after the pilot is completed unless the client proceeds with an engagement or a longer period is needed to discuss or verify findings.
- Recovery engagements: information may be retained while correction, recovery, validation or dispute support remains active and for a reasonable period afterwards where needed for contractual or legal records.
- Intelligence engagements: agreed historical data may be retained while the recurring service is active and will normally be deleted or returned within 90 days after the service ends unless another period is agreed or legally required.
- Backups: information may remain for a limited additional period in normal backup-rotation processes.

8. Security incidents

If Muraja becomes aware of suspected unauthorised access, disclosure, loss or alteration of client information, the issue should be treated as a security incident.

- Contain: restrict further access or sharing and preserve relevant records.

- Assess: determine what information was involved, whose information was affected and the likely impact.
- Correct: change access, credentials or provider settings where required and take reasonable steps to prevent recurrence.
- Notify: inform affected clients and make any regulatory notification required by applicable law based on the circumstances of the incident.
- Document: retain an internal record of the incident, response and corrective actions.

9. What Muraja does not require

A Muraja review should not require a client to surrender control of its freight operation.

- No replacement of the client's freight forwarders.
- No implementation of a full transport-management system.
- No access to every internal company system as a condition of the initial 30-invoice review.
- No public website upload of commercially sensitive client freight documents.
- No acceptance of an AI output as a confirmed financial finding without human verification.

10. Client responsibilities

Security also depends on how information is supplied to Muraja. Clients should:

- use the private upload method provided by Muraja rather than sending sensitive files through public website forms;
- share only documents they are authorised to provide;
- avoid including unnecessary sensitive personal information;
- tell Muraja if a document has special handling restrictions or contains unusually sensitive information; and
- notify Muraja promptly if an upload link, account or document has been shared with the wrong person.

11. Confidential handling

Client information is used solely to provide the agreed Muraja service, manage the engagement and meet applicable administrative, contractual or legal requirements. Muraja does not sell client personal data or freight documents. Confidentiality and data-handling commitments should also be reflected in the engagement terms used with paid clients.

12. Relationship with the Privacy Policy

This Data Security & Handling statement explains how Muraja intends to protect and control client information operationally. The Muraja Privacy Policy separately explains what personal data may be collected, why it is processed, third-party providers, international transfers, retention and individual privacy rights. Where personal data is involved, Muraja intends to operate in accordance with applicable UAE data-protection requirements, including the UAE Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data where it applies.

13. Contact and updates

Data security enquiries

General enquiries: enquiries@muraja.ae

Website: muraja.ae

If you have a question about how a proposed Muraja engagement would handle your freight documents, contact us before uploading the files.

This statement will be reviewed when Muraja's legal entity, secure upload provider, cloud storage provider and production AI environment are finalised.