
# FR8 Logistics

## Data (Privacy) Protection Procedures

Doc. Version: 2.0

Date: 27 July 2026

Ref: FIDI FAIM 3.4 Framework

FIDI

# TABLE OF CONTENTS:

# 1. PURPOSE AND SCOPE

FR8 Logistics (FR8) needs to gather and use certain information about individuals to conduct its work well, efficiently, and properly. These can include customers, suppliers, business contacts, employees, and other people the organisation has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled, and stored to meet the company's data protection standards, comply with the law, and meet the FAIM Quality Standard requirements.

Scope: This policy applies to:

- FR8's Port Vila and Santo offices
- All FR8 staff (full-time, part-time, temporary, and contractors)
- All contractors, suppliers, and other people working on behalf of FR8
- All data that the company holds relating to identifiable individuals, including:
  a. Names of individuals
  b. Postal and email addresses
  c. Phone numbers
  d. Identification documents
  e. Financial information
  f. Move details and inventory
  g. Any other information relating to individuals

FAIM Reference: FD 5.1

# 2. OUR SUSTAINABILITY VISION

This data protection policy ensures FR8:

- Complies with data protection law and follows good practice
- Protects the rights of staff, customers, and partners
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

# 3. DATA PROTECTION LAW

Vanuatu's Data Protection and Privacy Act No. 13 of 2024 describes how organisations must collate, handle, and store personal information. These rules apply regardless of whether data is stored electronically, on paper, or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely, and not disclosed unlawfully.

**Six Important Rules:**

1. Personal data must be processed fairly and in a transparent manner in relation to the data subject.
2. Personal data must be processed for explicit, specified, and legitimate purposes and must not be incompatible with them.
3. Personal data must be adequate, relevant, proportional, and not excessive in relation to the purposes for which they are processed.
4. Personal data must be accurate and kept up to date; inaccurate data must be rectified or erased without delay.
5. Personal data must be preserved in a form which permits identification of data subjects for no longer than is necessary.
6. Personal data must be processed in a manner that ensures reasonable and appropriate security measures against unauthorised or unlawful processing and against accidental or unauthorised access, destruction, loss, use, modification, or disclosure.

# 4. DATA PROTECTION RISKS

This policy helps to protect FR8 from data security risks, including:

- Breaches of confidentiality: Information being given out inappropriately
- Failing to offer choice: Individuals must be free to choose how the company uses data relating to them
- Reputational damage: The company could suffer if hackers successfully gained access to sensitive data
- Legal penalties: Non-compliance with data protection laws can result in fines and legal action.

# 5. ROLES AND RESPONSIBILITIES

**5.1 Overall Responsibility**

As the sole director, Christopher Kernot is ultimately responsible for ensuring that FR8 meets its legal obligations, including that of Data Protection Officer. Responsibilities include:

- Regularly reviewing all data protection procedures and related policies
- Arranging data protection training and advice for the FR8 team
- Fielding any questions from staff and anyone else covered by this policy
- Ensuring that information is kept confidential
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data

**5.2 IT Security Management**

As FR8's IT provider, ODC manages systems and data security with the following measures:

| Security Measure | Description |
|---|---|
| Cyber Security Protocols | Multi-factor authentication on email and key systems; business-grade firewall at network perimeter; antivirus and anti-malware on all endpoints; spam and malware filtering on inbound mail. |
| Storage of Personal Information | Data is held in access-controlled, cloud-hosted systems (Microsoft 365), with access restricted on a role basis to staff who need it. Backups are taken regularly and held securely. |
| Password Protocols | Minimum length and complexity enforced; no shared or reused credentials; MFA applied on top. |
| Relevant Laws | ODC ensures FR8 is compliant with Vanuatu's Data Protection and Privacy Act No. 13 of 2024. |
| Privacy and Cyber Security Policy | ODC maintains a formal policy document ("ODC Privacy and Cyber Security Policy"). |

**5.3 All Staff Responsibilities**

Everyone who works for or with FR8 has responsibility for ensuring data is collected, stored, and handled appropriately.

Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

# 6. FAIM PRIVACY PRINCIPLES

FR8's Data (Privacy) Protection Procedure addresses the following 10 minimum privacy principles:

## PRINCIPLE 1: MANAGEMENT

Objective: To define, document, communicate, and assign accountability for privacy policies and procedures; and to create and maintain an overview of all data processing activities.

### 6.1.1 Privacy Governance

FR8 has appointed its Managing Director as the Data Protection Officer (DPO) who is responsible for:

- Overseeing the implementation and maintenance of this Data (Privacy) Protection Procedure
- Monitoring compliance with applicable privacy laws and regulations
- Serving as the primary point of contact for privacy-related queries, complaints, and regulatory authorities
- Conducting periodic privacy impact assessments

### 6.1.2 Data Processing Activity Register

FR8 maintains a Data Processing Activity Register that documents all processing activities involving personal information. This register includes:

| Element | Description |
|---|---|
| Purpose of Processing | Why the personal information is processed (e.g., to provide moving quotes, coordinate shipments, process claims). |
| Categories of Data Subjects | Who the personal information relates to (e.g., private customers, corporate account transferees, employees). |
| Categories of Personal Data | What personal information is collected (e.g., name, contact details, move dates, inventory of goods, financial information, identification documents). |
| Recipients of Personal Data | With whom the personal information is shared (e.g., destination agents, shipping companies, insurance providers, customs authorities). |
| Retention Periods | How long the personal information is retained. |
| Data Transfers | Whether personal information is transferred to third countries and the safeguards in place. |
| Security Measures | Technical and organisational measures to protect personal information. |

The Data Processing Activity Register is reviewed and updated at least annually or whenever there is a significant change in processing activities.

### 6.1.3 Communication and Accountability

This Data (Privacy) Protection Procedure is communicated to all employees, contractors, and relevant third parties.
Each department head is responsible for ensuring that staff within their department comply with this procedure.
All new employees receive training on this procedure as part of their induction, with annual refresher training thereafter.

## PRINCIPLE 2: NOTICE

Objective: To provide clear notice to individuals about the company's privacy policies and procedures, and to identify the purposes for which personal information is collected, used, retained, and disclosed.

### 6.2.1 Privacy Notice (Privacy Policy)

FR8 maintains a clear, concise, and easily accessible Privacy Notice that is provided to individuals at or before the point of data collection. The Privacy Notice includes the following minimum information:

| Element | Description |
|---|---|
| Identity of the Data Controller | FR8 Logistics and contact details of the Data Protection Officer (Christopher Kernot). |
| Purpose of Processing | To provide international moving and relocation services, including quotations, shipment coordination, customs clearance, storage, and delivery. |
| Categories of Personal Information Collected | Name, address, contact details, move details, inventory, identification documents, financial information. |
| Retention Period | How long the personal information will be retained (see Principle 5). |
| Recipients | Destination agents, shipping companies, customs authorities, insurance providers, and other service providers. |
| Data Subject Rights | Access, rectification, erasure, restriction, objection, portability. |
| Legal Basis for Processing | Performance of a contract, legitimate interests, legal obligation, consent. |
| Contact Details | How individuals can contact the Data Protection Officer to exercise their rights or raise concerns. |

**6.2.2 Provision of Privacy Notice**
The Privacy Notice is provided to individuals:

- Private customers: At the time of the initial enquiry, quote request, or survey, and is prominently displayed on the company's website.
- Corporate account transferees: Provided at the time of service booking and included in all relevant communications.
- Employees and job applicants: Provided at the time of recruitment and on the company's internal intranet.

## PRINCIPLE 3: CHOICE AND CONSENT

Objective: To describe the choices available to individuals and to obtain implicit or explicit consent with respect to the collection, use, and disclosure of personal information; and to maintain verifiable records of consent.

**6.3.1 Consent Mechanisms**
FR8 obtains consent for the collection, use, and disclosure of personal information in accordance with applicable laws.
Explicit consent is obtained for:

- Processing of sensitive personal information (e.g., health information, biometric data)
- Disclosure of personal information to third parties not directly involved in the service delivery (e.g., marketing purposes)
- International transfers of personal information to countries without adequacy decisions

Implicit consent is obtained for processing that is necessary for the performance of a contract (e.g., sharing shipment details with destination agents, customs brokers, and shipping companies).

**6.3.2 Consent Records**
Records of consent are maintained and include:

- Date and time of consent
- Method of consent (e.g., signed consent form, ticked checkbox, verbal consent recorded in the file)
- Scope of consent (what the individual consented to)
- Withdrawal of consent (when and how consent was withdrawn)

Consent records are stored within the customer's move file and are accessible for audit purposes.

**6.3.3 Withdrawal of Consent**
Individuals are informed of their right to withdraw consent at any time.
Withdrawal of consent does not affect the lawfulness of processing carried out before withdrawal.
On receipt of a withdrawal request, the Data Protection Officer is notified and the processing activity is ceased (unless another legal basis applies).

## PRINCIPLE 4: COLLECTION

Objective: To collect personal information only for the purposes identified in the notice and as necessary for the provision of international moving and relocation services.

**6.4.1 Collection Principles**
Personal information is collected only for the purposes outlined in the Privacy Notice and as necessary for:

- Providing quotations for international moving services
- Coordinating and managing shipments (origin services, shipping, customs clearance, destination services)
- Processing insurance claims
- Complying with customs and legal requirements
- Billing and invoicing
- Customer relationship management and service improvements

**6.4.2 Minimization**
FR8 collects only the personal information that is adequate, relevant, and limited to what is necessary for the purposes of processing. Unnecessary or excessive personal information is not collected.

**6.4.3 Collection Channels**
Personal information is collected through the following channels:

- Direct collection: In-person surveys, telephone calls, emails, website forms, and written correspondence
- Indirect collection: From third parties (e.g., corporate relocation companies, destination agents, shipping lines) where necessary for service delivery

## PRINCIPLE 5: USE, RETENTION, AND DISPOSAL

Objective: To limit the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent; and to retain and dispose of personal information appropriately.

**6.5.1 Use of Personal Information**

Personal information is used only for the purposes identified in the Privacy Notice and for which consent has been obtained.
Use of personal information for any new purpose requires either a new consent or a documented legal basis.
Employees are prohibited from accessing personal information for personal reasons or purposes unrelated to their job responsibilities.

**6.5.2 Retention Periods**

Personal information is retained for only as long as necessary to fulfil the stated purposes or as required by law or regulations.
Standard retention periods for international moving operations include (but are not limited to):

| Category of Personal Information | Retention Period | Basis for Retention |
|---|---|---|
| Customer move files | 7 years from final delivery | Legal (contractual claims) and operational (claims handling) |
| Quotations and estimates | 3 years from quotation date | Operational and customer service |
| Financial and billing records | 7 years from invoice date | Tax and legal requirements |
| Employee records | 7 years from employment end date | Legal and regulatory requirements |
| Insurance claims records | 7 years from claim settlement | Insurance and legal requirements |
| Marketing and consent records | Until withdrawal of consent | Consent-based processing |

**6.5.3 Disposal**

Personal information is disposed of securely when the retention period has expired.
Disposal methods include:

- Physical documents: Shredding, pulping, or confidential incineration
- Electronic records: Permanent deletion using secure data destruction software; physical destruction of storage media (e.g., hard drives) where necessary

All disposal activities are documented in the relevant file or record.

## PRINCIPLE 6: ACCESS

Objective: To provide individuals with access to their personal information for review and update.

**6.6.1 Subject Access Requests**

Individuals (private customers, corporate account transferees, employees) have the right to request access to their personal information held by FR8.
Requests for access (Subject Access Requests) must be made in writing to the Data Protection Officer (Christopher Kernot).

**6.6.2 Response to Access Requests**

FR8 responds to access requests within 30 calendar days of receipt. The response includes:

- Confirmation as to whether personal information is being processed
- A copy of the personal information held
- The purposes of the processing
- The categories of personal information concerned
- The recipients or categories of recipients to whom the personal information has been disclosed
- The retention period or criteria for determining retention
- Information about the individual's rights (rectification, erasure, restriction, objection)

Access requests are provided free of charge, except where manifestly unfounded, excessive, or repetitive, in which case a reasonable fee may be charged.

**6.6.3 Rectification**

If an individual identifies that their personal information is inaccurate or incomplete, they may request rectification.
FR8 corrects or completes the personal information without undue delay and confirms the rectification to the individual.

**6.6.4 Record Keeping**

All access requests, rectification requests, and responses are documented and retained.

## PRINCIPLE 7: DISCLOSURE TO THIRD PARTIES

Objective: To disclose personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

### 6.7.1 Third Party Disclosure

Personal information is disclosed to third parties only for the purposes identified in the Privacy Notice and as necessary for the provision of international moving services, including:

| Third Party | Purpose |
|---|---|
| Destination Agents | To coordinate delivery and destination services |
| Shipping Companies and Freight Forwarders | To arrange transportation of goods |
| Customs Brokers and Authorities | To comply with customs requirements (including customs declarations) |
| Insurance Providers | To arrange insurance coverage and process claims |
| Storage Facilities | For temporary or long-term storage of goods |
| Corporate Relocation Companies | Where the individual is a transferee of a corporate customer |
| Legal and Regulatory Authorities | Where required by law or regulation |

### 6.7.2 Third Party Agreements

Third parties processing personal information on behalf of FR8 are required to sign a Data Processing Agreement that includes:

- Obligations to process personal information only for the purposes specified
- Obligations to implement appropriate security measures
- Obligations to comply with data protection laws
- Obligations to notify FR8 of any data breach
- Obligations to return or delete personal information upon completion of services

A list of all third parties with whom personal information is shared is maintained in the Data Processing Activity Register.

### 6.7.3 International Transfers

Where personal information is transferred to third parties in other countries, FR8 ensures appropriate safeguards are in place, such as:

- Standard Contractual Clauses (SCCs) approved by the European Commission
- Transfers to countries with adequacy decisions
- Other legally permitted transfer mechanisms

Individuals are informed of international transfers in the Privacy Notice.

## PRINCIPLE 8: SECURITY FOR PRIVACY

Objective: To protect personal information against unauthorised access (both physical and digital); and to handle potential data breaches in accordance with documented procedures.

### 6.8.1 Physical Security

FR8 maintains physical security controls to protect personal information, including:

| Control | Description |
|---|---|
| Access Control | Secure access to office premises and warehouse through locked doors and restricted entry |
| Visitor Management | All visitors are signed in and escorted while on premises |
| Workstation Security | Staff are required to lock screens when away from desks; paper documents containing personal information are stored in locked cabinets when not in use |
| Transport Security | Vehicles and containers used for moving goods are secure; drivers are trained to protect personal information |
| Paper Disposal | Paper documents are disposed of via shredding or confidential waste |

**6.8.2 Digital Security**
FR8 maintains digital security controls to protect personal information, as managed by ODC:

| Control | Description |
|---|---|
| Access Controls | Multi-factor authentication; role-based access to systems and data |
| Encryption | Encryption of personal information in transit and at rest where appropriate |
| Firewalls and Antivirus | Perimeter security (firewalls, intrusion detection) and endpoint protection (antivirus, anti-malware) |
| Backup and Recovery | Regular backups of systems containing personal information, with secure storage and recovery procedures |
| Patch Management | Regular updates and patches to software and systems |
| Remote Access | Secure remote access for staff working off-site |

**6.8.3 Data Breach Procedure**
FR8 has a documented Data Breach Response Procedure that includes the following steps:

| Step | Action | Responsibility |
|---|---|---|
| 1. Detection | Identify and assess the breach (nature, scope, cause). | All Staff / IT Security |
| 2. Containment | Immediately contain the breach to prevent further exposure (e.g., isolate systems, disable access, recover data). | IT Security / DPO |
| 3. Investigation | Investigate the root cause and assess the risk to affected individuals. | DPO / IT Security |
| 4. Assessment | Determine whether the breach is likely to result in a risk to the rights and freedoms of individuals. | DPO |
| 5. Notification to Authorities | Notify the relevant data protection authority within 72 hours of becoming aware of the breach (if required). | DPO |
| 6. Notification to Individuals | Notify affected individuals without undue delay if the breach poses a high risk to their rights and freedoms. | DPO |
| 7. Documentation | Document all actions taken, including the breach description, impact assessment, notifications, and corrective actions. | DPO |
| 8. Review and Remediation | Review the root cause, implement corrective and preventive actions, and update policies and procedures. | DPO / Management |

A Data Breach Register is maintained to document all breaches, including the date, nature, cause, impact, and actions taken.

## PRINCIPLE 9: QUALITY

Objective: To maintain accurate, complete, and relevant personal information for the purposes identified in the notice.

**6.9.1 Data Accuracy and Completeness**
FR8 takes reasonable steps to ensure that personal information held is accurate, complete, and up-to-date.
Information is verified:

- At the point of collection (e.g., confirmation with the individual)
- At regular intervals (e.g., annual review of customer records, pre-move survey updates)
- On receipt of a correction request from the individual

**6.9.2 Data Review**
Personal information held is reviewed periodically to ensure it remains relevant for the purposes identified. Where personal information is found to be incorrect, incomplete, or outdated, it is corrected or updated without undue delay. Where personal information is no longer necessary for the stated purposes, it is securely disposed of in accordance with Principle 5.

**6.9.3 Data Integrity**
Personal information is maintained in a format that ensures its integrity and reliability.
Access to personal information is restricted to authorised personnel only to prevent unauthorized alteration or deletion.

**6.9.4 Staff Responsibilities**
Staff should not create any unnecessary additional data sets.
Staff should take every opportunity to ensure data is updated (e.g., confirming customer details when they call).
FR8 will make it easy for data subjects to update the information FR8 holds about them.
Data will be updated as inaccuracies are discovered.
It is all staff's responsibility to ensure databases are checked and any inaccuracies remedied.

## PRINCIPLE 10: MONITORING AND ENFORCEMENT

Objective: To monitor compliance with the company's privacy policies and procedures; and to address privacy-related complaints and disputes through an escalation procedure.

**6.10.1 Monitoring and Review**

FR8 monitors compliance with this Data (Privacy) Protection Procedure through:

| Activity | Frequency | Responsibility |
|---|---|---|
| Annual Audit | At least once a year | DPO |
| Periodic Checks | Random spot checks on move files and processing activities | DPO |
| Internal FAIM Audit | Annually (as part of FAIM requirements | DPO |

The monitoring and review process assesses:

- Whether personal information is collected, used, retained, disclosed, and disposed of in conformity with this procedure
- Whether staff are aware of and compliant with privacy policies
- Whether third parties are compliant with Data Processing Agreements
- Whether any new risks or issues have arisen

**6.10.2 Review and Update Procedure**

This Data (Privacy) Protection Procedure is reviewed and updated at least once a year, or whenever there is a significant change in operations, technology, or regulations. The annual review covers:

- Changes in applicable data protection laws and regulations
- Changes in business operations or processing activities
- Findings from monitoring, audits, and breach investigations
- Changes in best practices and industry standards

Updates are communicated to all staff through email, intranet, or training sessions.

**6.10.3 Communication to Staff**

This Data (Privacy) Protection Procedure, and any updates, are communicated to all internal personnel through:

- Induction training: All new staff receive a copy of this procedure and complete privacy awareness training
- Annual refresher training: All staff complete annual training on this procedure and privacy compliance
- Notification of updates: Staff are notified of updates via email or company intranet

Training records are maintained in the staff training register.

**6.10.4 Complaints and Escalation Procedure**

FR8 maintains a documented procedure for handling privacy-related complaints and disputes:

| Step | Action | Responsibility |
|---|---|---|
| 1. Receipt | Privacy-related complaint is received (verbal, written, or electronic). | Any Staff |
| 2. Acknowledgment | Complaint is acknowledged to the complainant within 5 working days. | DPO |
| 3. Investigation | Complaint is investigated (including review of relevant files, policies, and procedures). | DPO / Dept Head |
| 4. Response | A response is provided to the complainant within 30 working days, detailing findings and actions taken. | DPO |
| 5. Escalation | If the complainant is dissatisfied, the matter is escalated to the Managing Director. | DPO |
| 6. External Escalation | If the matter is not resolved, the complainant is informed of their right to lodge a complaint with the relevant data protection authority. | DPO |

## 7. DATA STORAGE

These rules describe how and where data should be safely stored.
Questions about storing data safely can be directed to the IT manager or data controller.

**7.1 Paper Storage**
When data is stored on paper:
- It should be kept in a secure place where unauthorised people cannot see it
- When not required, the paper or files should be kept in a locked drawer or filing cabinet
- Employees should make sure paper and printouts are not left where unauthorised people could see them (e.g., on a printer)
- Data printouts should be disposed of securely when no longer required

**7.2 Electronic Storage**
- Employees should ensure the screens of their computers are always locked when left unattended
- Personal data should never be transferred outside the European Economic Area without authorisation
- Employees should not save copies of personal data to their own computers
- Always access and update the central copy of any data

## 8. DATA USE

Personal data is of no value to FR8 unless the business can make use of it. However, it is when personal data is accessed and used that it can be at the greatest risk of loss, corruption, or theft. When working with personal data, employees should ensure:
- Screens of their computers are always locked when left unattended
- Personal data is not transferred outside the European Economic Area without authorisation
- Copies of personal data are not saved to their own computers
- They always access and update the central copy of any data

## 9. DATA ACCURACY

The law requires FR8 to take reasonable steps to ensure data is kept accurate and up to date.
Staff Responsibilities:
- Staff should not create any unnecessary additional data sets
- Staff should take every opportunity to ensure data is updated (e.g., confirming a customer's details when they call)
- FR8 will make it easy for data subjects to update the information FR8 holds about them
- Data will be updated as inaccuracies are discovered
- It is all staff's responsibility to ensure marketing databases are checked and any inaccuracies remedied

## 10. SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by FR8 are entitled to ask what information the company holds about them and why; how to gain access to it; and how to keep it up to date. They may do so by logging a subject access request.
Procedure:
- Requests must be made in writing to the Data Protection Officer
- FR8 responds within 30 calendar days

The response includes a copy of the personal information held, the purposes of processing, categories of data, recipients, retention period, and information about rights

Requests are provided free of charge unless manifestly unfounded, excessive, or repetitive

## 11. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, Privacy Laws allow personal data to be disclosed to law enforcement agencies without the consent of the data subject after ensuring the request is legitimate, and only with the authority of the Managing Director.

## 12. DATA PROCESSING AGREEMENTS

FR8 requires all third parties processing personal information on its behalf to sign a Data Processing Agreement. This agreement includes:

- Obligations to process personal information only for the purposes specified
- Obligations to implement appropriate security measures
- Obligations to comply with data protection laws
- Obligations to notify FR8 of any data breach
- Obligations to return or delete personal information upon completion of services

## 13. RELATED DOCUMENTS

| Document | Reference |
|---|---|
| Social Responsibility Policy / Code of Conduct | FR8-HR-001 |
| ODC Privacy and Cyber Security Policy (v1.0) | |
| Employment Contract | FR8-HR-002 |
| Training Register | FR8-HR-003 |
| Quality Manual | FR8-OP-002 |
| Non-Conformity, Corrective and Preventive Actions Procedure | FR8-OP-005 |

## 14. DECLARATION OF COMPLIANCE

**Company Name: FR8 Logistics**

I, Christopher Kernot, in my capacity as Managing Director, hereby declare that I have reviewed and approved this Data (Privacy) Protection Procedure, and confirm that FR8 Logistics is committed to compliance with the FAIM minimum requirements for data protection and privacy.

Date: _____

Signature: _____

Company Seal / Logo

**Document Control**

| Version | Date | Author | Approved By | Description of Changes |
|---|---|---|---|---|
| - | - | FR8 | - | Initial version prior to FAIM 3.4 Compliance. |
| 2.0 | 27-07-2026 | FR8 | Christopher Kernot | Various & numerous content additions |
| | | | | |

## END OF DOCUMENT