



Freight Services

Risk Management Process

Data Protection & Privacy Policy

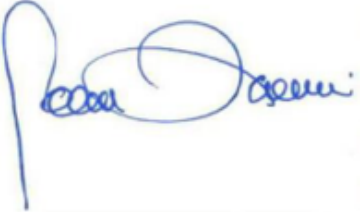
Document Ref: SOP-RMGDPP-01

Version Control

First Approved:	30-07-22	Authorization: Managing Director
Current Version:	SOP-RMGDPP-01	
Past Revisions:	None	Queries: Finance & Admin Manager
Review Cycle:	Quarterly (3 Months)	
Effective Date:	30-07-22	

Approved By:

Managing Director



30th July, 2022

Table of Contents

1.0 Overview	4
1.1 What is our Data Protection Procedure all about?	4
1.2 What Data is covered	4
2.0: Data Protection Procedure	5
2.1 Owners of Data (Interested Parties)	5
2.2 Methods of Obtaining Data.....	5
2.3 Purposes for Obtaining, Using, Retaining or Disclosing Data	5
2.4 Methods of retaining/recording data and location.....	6
2.5 Review and update of personal information:.....	6
2.5 Retention period and Destruction.....	7
2.6 Providing data (Notice, choice and consent)	7
2.7 Protection of Data.....	8
2.8 Transmittal of Data	9
2.9 Distribution to 3 rd Parties.....	9
3.1 Complaints and Disputes	11
3.2 Applicable Systems	11
3.3 Data Storage Security Procedures	12
3.4 Data Storage Security Process.....	12
COPYRIGHT NOTICE	13
All rights reserved.....	13

1.0 Overview

Freight Services (Fiji) PTE Limited values the privacy values the privacy of every individual and is committed to the protection of personal data. This Data Protection and Privacy Procedure ('Procedure') outlines how the Organization ('us', 'our' or 'we'):

1.1 What is our Data Protection Procedure all about?

The FSF data protection procedure (DPP) follows our security process and is part of our Administration Policy. It is dedicated to standardizing the use, monitoring, and management of data. The main goal of this procedure is to protect and secure all data consumed, managed, and stored by FSF. It is a requirement of us as an organization to comply with FIDI standards and regulations.

1.2 What Data is covered

Data protection policies should cover all data stored by core infrastructure of the organization, including on-premise storage equipment, offsite locations, and cloud services. It should help the organization ensure the security and integrity of all data—both data-at-rest and data-in-transit.

Data protection policies can demonstrate the organization's commitment to ensuring the protection and privacy of consumer data. If the organization is subject to compliance audits, or experiences a data breach, the data protection policy can be presented as evidence demonstrating the organization's commitment to data protection principles.

This data protection procedure covers the following aspects:

- The scope of required data protection
- Data protection techniques and policies applied by relevant parties such as individuals, departments, devices, and IT environments
- Any applicable legal or compliance requirements for data protection

- The roles and responsibilities related to data protection, including data custodians and roles specifically responsible for data protection activities

2.0: Data Protection Procedure

All personal information covered by the law and recorded either in writing or on electromagnetic media (hard disks (server or PCs), CDs, tapes, back up media etc.) is subject to this procedure which per indications which personal data is managed, where it comes from and with whom it has been shared.

2.1 Owners of Data (Interested Parties)

Owners of data are:

- ✓ **Direct FSF employee** and management personnel; and
- ✓ **Customer / Client** (the information such as passport details, tax id, address, phone number, email)
- ✓ **Agents and third parties** operating on FSF's behalf

2.2 Methods of Obtaining Data

Data is obtained orally and in writing. Data is collected orally during the course of conducting business telephonically or in person (office visits) (e.g. requests for information, requests for quotation etc.). Written data is collected during conduct of business through normal correspondence or using electronic means (e-mail, transfer applications – drop box, we transfer, CD's, tapes, etc.)

2.3 Purposes for Obtaining, Using, Retaining or Disclosing Data

- **Employees** - Data on employees is necessary to comply with the formalities required by law, regulations and Community legislation concerning the administration of employees, such data will be processed

on paper and/or magnetic, electronic, and similar media, and in any case using instruments that guarantee security and confidentiality.

□ **Customer/Client** - Client's data is required and used exclusively for the following purposes:

- the establishment or continuation of a business contractual relationship;
- to comply with proper administrative procedures, civil, fiscal and other requirements of law;
- commercial and marketing statistics;
- to answer questions;
- to maintain and update a most frequently asked questions, proposals and communications database
- for eventual subscription to our newsletter whenever available;

2.4 Methods of retaining/recording data and location.

It's important to maintain accurate, complete and relevant personal information. FSF records data both in written (physical) and electronic form.

Written data is found in personnel files, customer service files, accounting files, reports and other documentation required by law, regulation, community legislation or governmental entities. Data obtained orally is normally reduced to written form subsequently placed in the above-mentioned files.

Electronic form of data is retained on the server or on individual PCs.

2.5 Review and update of personal information:

Review and update of personal information is not allowed nor from private customer nor from corporate account since it used for single move only and shall be requested for each individual business transaction regardless of whether the data is already in our possession.

2.5 Retention period and Destruction

Employee and management personal data is maintained for the duration of employment or appointment and destroyed upon termination of employment or cessation of the appointment.

Customer/client personal data is maintained for the period of 10 years and then destroyed.

All documents are destroyed in a manner to render impossible any subsequent restoration of the personal data or sensitive data. This is accomplished using means such as paper shredders or incinerators but in no way, trash cans unless the documents are reduced to a form that impedes the reconstruction of the information that they initially contained.

Data stored on electromagnetic media shall be destroyed through permanent cancellation from the local network (G Drive). Back up data will likewise be deprived of availability of all personal data previously destroyed/cancelled.

2.6 Providing data (Notice, choice and consent)

The interested party/owner of the data shall be provided an express choice concerning the consent or otherwise to the collection and use of data, to include disclosure.

This is done by re-directing the client to our website (www.fsf.com.fj) where he / she can consult both our Privacy Protection Policy and our ABC charter.

These enclosures include a consent choice for completion by the data owner. The enclosures also inform the owner of the consequences, if consent is not given directly, in the absence of particular comments or requests regarding data protection FSF will operate on an implicit consent basis, taking for granted

that the customer has read the information regarding data protection provided in the documents.

Whenever possible and practicable in conducting business orally, FSF staff informs the client of the consent choice and that if consent is not given or in case of failures in providing the specifically requested data, even partially, places FSF in the impossibility to fulfil their requests as we cannot complete required processes and laws.

2.7 Protection of Data

All physical forms of data shall be kept in appropriate types of filing media to the maximum extent possible and kept solely in designated areas that are constantly surveilled during normal operating hours. After duty hours these areas are subject to both electronic anti intrusion surveillance and detection supported by random intrusion detection patrols.

Areas where personal data is maintained will so be indicated with appropriate cautionary signs.

Custody of this data is the responsibility of personnel assigned to perform the related duties and those located in the vicinity of the storage location. Personnel other than those charged with administrative or management duties will be challenged as to their need-to-know personal data before they can access files or systems where personal data is kept.

Sensitive data will be kept under key and in the custody of the person responsible for the function. Access or disclosure of these sensitive data will only be permitted to management personnel and personnel with a verified need to know and necessary to perform specifically assigned duties/responsibilities.

Data stored on electronic media is protected from unauthorized access and disclosure through use of credential authenticating application (password) which permit passing an access screening procedure.

Sensitive data is further protected by being kept in directory folders that have a second authenticating control which permits access only to designated personnel maintained by the systems manager. Sensitive data will not be kept in electronic form in generic directory folders that do not have the secondary authenticating control.

Access to the warehouse where forwarding/storage data is evident requires authorized entry. Unescorted entry is authorized for FSF employees and certain suppliers strictly for performance of assigned duties and services respectively. The Warehouse Manager will maintain a list of authorized personnel for unescorted entry. All other personnel require escorted entry by the warehouse man or other authorized employee.

In case of violation of above procedure, it's FSF's responsibility to inform the Local Police (for digital unauthorized access) or for physical unauthorized access for further investigation and actions taking as per applicable laws and regulations

2.8 Transmittal of Data

All e-mails and other correspondence with or transmitting data will include an appropriate statement concerning the confidentiality, restricted use to the intended addressee and notification concerning misdirection of the correspondence and warning against any type of further unintended processing of the contents.

2.9 Distribution to 3rd Parties

Some personal data may have to be distributed to those third parties involved in the process of the move such as local origin agents, customs agents or

destination agents. Most commonly this happens through the sending of the documents required by each party to perform their service (eg. Copy of the passport and of the Fiji local fiscal code will be sent to the customs agent so as to allow preparation the documents for an FCL shipment).

In no case will any data other than that specifically required be distributed to any person or party involved.

FSF forbids and prevents its members from distributing or seeking any data other than that they duly came into possession.

Should personal data be requested through official channels by the police forces or other law enforcement agencies, FSF will second the request in compliance with the law in force.

3.0: Monitoring and Review Process

Monitoring and enforcement of the Privacy policy and procedure of FSF is the responsibility of all personnel, but in particular the administrative personnel that as part of their duties obtain, use and maintain files with personal data.

Agents and third parties operating on FSF behalf have been chosen also taking into account their respect for Privacy. Therefore, when data is disclosed, such parties are required and expected to operate following the specifications of our policies or similar policies, edited on the basis of Fiji laws and of the laws in force in the subject country for services abroad.

During internal audits/inspections the applicability of this procedure shall be verified and reported to management. The verification process shall include examination of files for correspondence to the requirement herein established as well as electronic systems access/security.

The Privacy policy and procedure of this document shall be reviewed at least annually and updated as necessary. It shall also be reiterated to dependent personnel once a year.

3.1 Complaints and Disputes

All complaints involving personal data will be directed/addressed to and handled by the Finance & Admin Manager of FSF.

Any resulting disputes will be processed in accordance with applicable laws relating to data privacy.

3.2 Applicable Systems

PC's, Operating Software (Cargowise) and Servers (Local Network)

3.3 Data Storage Security Procedures

The administration for FSF business is done by a computer network based on one Server station and different workstations.

- ❑ The hardware can be of different suppliers.
- ❑ The software is based on Microsoft Windows applications for which licenses are available.
- ❑ Some independent programs are also available for which no license is required.

3.4 Data Storage Security Process

- ❑ Copy of all data is stored on 3 external hard disks, these 3 hard disks are interchanged on a weekly basis by our IT Manager
- ❑ 1 hard disk remains in server room, one remains in Admin office, the other is taken home for physical security by the Admin staff in case of data backup emergencies.
- ❑ Not all data is accessible by all staff – each staff can only access the data they have been given access to. Changes are done via our server operations. - All programs are authorized for all the users except for bookkeeping programs, salary registrations etc. which are only accessible by the administration department. –
- ❑ Antivirus program (MacAfee) is used and one firewall (Grand Stream Firewall) – entry and exit through server.

COPYRIGHT NOTICE

All rights reserved.

The contents of this manual are strictly and solely intended for the Staffs, Directors, and Office bearers of Freight Services (FSF) and may contain confidential and legally privileged information. If you are not the intended recipient of this manual, you are notified that any dissemination, distribution or copying of the contents thereof (whether in full or in part) is strictly prohibited. No part of this Manual shall be reproduced in any form or incorporated in any information retrieval system, electronics or mechanical, without the express written approval of the Managing Director or any other legally authorized officer of Freight Services.

To the bona-fide, intended recipients, for the reason that this manual may contain confidential and legally privileged information, you are to ensure that it is always kept in a secure and safe custody where it cannot be accessed by any unauthorized parties. Any breaches, whether intended or unintentional, and failure to comply with the above requirements may result in disciplinary proceedings understanding instructions of the Organization and/or redress through legal proceedings for retribution with fines and penalties to the full extent as permissible by Law. The Copyright in this work is vested in FSF and the document is issued in confidence for the purpose only for which it is supplied.

GET IN TOUCH

FIJI



Freight Services
P.O.Box 14998, Suva
24-26 Edinburgh Drive, Suva, Fiji Islands



t.+679 3309603
m.+679 5200



e. info@fsf.com.fj

PAPUA NEW GUINEA



Freight Services
Office 1, Allotment 33 Section 73,
Henao Drive, Gordon



t.+675 3251069
m.+675 72744355



e. info@fsf.com.fj

www.fsf.com.fj