Jamaica Social Investment Fund

(JSIF)

Enterprise Data Privacy Policy

TABLE OF CONTENTS

GLOSSARY

Business Unit: Individual branches and sections within JSIF that perform specific business functions.

Confidentiality: The ethical and legal principle or obligation that ensures sensitive information or data shared by an individual or entity is kept private and protected from unauthorized access or disclosure.

Data Controller: A person or public authority such as JSIF who, alone or jointly determines the purpose for which and manner in which any Personal Data are, or are to be, processed.

Data Controller Representative: A person or other entity appointed by the Data Controller for the purposes of representing JSIF in front of the authority.

Data Privacy Impact Assessment (DPIA): A process that focuses on reducing privacy risks associated with the processing of Personal Data in an organization. A DPIA will identify risks and suggest measures to reduce these risks.

Data Privacy Program: The set of policies, procedures, and actions that the JSIF engages in to protect the Personal Data of stakeholders.

Data Processor: In relation to Personal Data, means any person who processes data on behalf of the Data Controller who is not an employee of the data controller.

Data Protection Act of Jamaica (DPA): The Data Protection Act came into effect Dec 1, 2023, providing greater safeguards for the handling of personal information of Jamaicans held in physical or electronic form.

Data Subjects: A named or otherwise identifiable individual who is the subject of Personal Data, and in determining whether an individual is identifiable account shall be taken of all means used or reasonably likely to be used by the data controller or any other person to identify the individual, such as reference to an identification number or other identifying characteristics (whether physical, social or otherwise) which are reasonably likely to lead to the identification of the individual e.g. a JSIF stakeholder, employee, and/or authorized agent.

Data Subject Request (DSR): Request by a natural person for information or specific action related to their Personal Data which may have been collected, processed, shared and/or maintained by JSIF. See Data Subject Rights Procedures.

Employee: Any full-time, part-time, and temporary employees, trainees, volunteers and others whose work performance is under the direct control of JSIF. Employee does not include any Third Party or any Employee, agent or subcontractor of a Third Party.

Information Classification: The grouping of records based on its value, legal requirements, regulatory compliance, sensitivity, criticality, and risk of loss or compromise.

Jamaica Social Investment Fund: JSIF.

Permissible Purpose: A reasonable business purpose related to the reason why JSIF is processing Personal Data from Data Subjects.

Personal Data: Any information (however stored) relating to a living individual, or an individual who has been deceased for less than thirty years, who can be identified from that information. This includes other information in the possession of JSIF, or information JSIF is likely to come into the possession of.

Privacy Impact Assessment: A process which assists organizations in identifying and managing the privacy risks arising from new (or changes to existing) projects, processes, or systems.

Privacy Notice and/or Notice: A statement made to a Data Subject that describes how an organization collects, uses, retains, and discloses Personal Data.

Privacy RACI matrix: A tool used to clarify roles and responsibilities related to privacy and data protection within. RACI stands for Responsible, Accountable, Consulted, and Informed, which are the four key roles that can be assigned to individuals or teams in relation to specific tasks or processes.

Processing and/or Processed: Actions that result in the collection, creation, use, storage, transfer, handling, distribution, disposal of, or otherwise interaction with Personal Data.

Record of Processing Activity (RoPA): The RoPA documents all Personal Data processing activities carried out by the Business Units within JSIF.

Sensitive Personal Data: Individually identifiable information concerning race or ethnic origin, health, criminal history, trade union membership, religion or philosophical beliefs, sex life or sexual orientation, or political opinions as well as genetic data and biometric data which allows or confirms the unique identification of an individual, such as fingerprints or facial geometry.

Targeted Advertising: Displaying to a Data Subject an advertisement that is selected based on Personal Data obtained or inferred over time from the Data Subject's activities across nonaffiliated websites, applications, or online services to predict the Data Subject's preferences or interests.

The Program: JSIF's Privacy Program.

Third Party: Any entity (individual or fund) that is providing products or services to JSIF.

1. ENTERPRISE DATA PRIVACY POLICY

1.1 Policy Statement

The Jamaica Social Investment Fund (JSIF) prioritizes data privacy for its stakeholders and is committed to ensuring that Personal Data collected and processed in the course of business is carried out in compliance with the Data Protection Act, 2020 (DPA). JSIF is dedicated to upholding the principles of the Data Protection Act (DPA), including data minimization, transparency, fairness, lawfulness, and accuracy, while also committing to data protection by design and by default.

1.2 Scope

The Enterprise Data Privacy Policy applies to all employees, agents, entities or individuals who collect, create, use, store, handle, distribute, dispose of, or otherwise interact with (process) personal data, whether in hard copy or electronic format on behalf of JSIF. The type of personal data processed includes biographic, biometric, demographic, financial, transactional, sensitive, social media, account, education-related and employment-related personal data.

1.3 Purpose and Objectives

This Policy establishes the requirements necessary to protect stakeholder and employee personal data demonstrating JSIF's commitment to data protection. This JSIF Enterprise Data Privacy Policy (the Policy) has the following objectives:

1. Describe JSIF's responsible use of Personal Data and to secure the organization's information assets.
2. Demonstrate compliance with the DPA through the documentation of controls in place for data protection, relating to collection, creation, retention, use, disclosure, sharing, and disposal within JSIF's processing environment.
3. Encourage effective and ethical use of systems that manage Personal Data.

1.4 Policy Governance

JSIF is committed to preserving the privacy of its stakeholders including investors, beneficiaries and JSIF employees (collectively, Data Subjects). JSIF prioritizes processing personal data in compliance with regulatory obligations under the DPA, as well as conforming to international best practices and requirements of our Funding Agencies. This Policy is owned and maintained by the Head of Privacy. This individual provides guidance to JSIF Business Units when implementing new processes, systems, software, or third-party agreements to ensure that appropriate privacy safeguards are in place and to establish the appropriate handling of Data Subjects' Personal Data.

1.5 Roles and Responsibilities and Definitions

These roles and responsibilities are specific to this Policy and are described at a high level. These roles and responsibilities are further defined in the Privacy RACI matrix.

Role	Responsibilities
Head of Privacy	Implement operational privacy policies and procedures, update when necessary; Oversee completion of Data Subject Requests (DSRs), Privacy Impact Assessment (PIAs), Data Protection Impact Assessment (DPIAs), Record of Processing Activities (RoPAs), and Privacy Notices; Train and educate staff on data protection regulations, privacy policies, and best practices for handling personal data to ensure compliance and mitigate risks.
Privacy Committee	Provide advisory support for JSIF's privacy process. This multidisciplinary committee will have stakeholders from different Business Units to offer comprehensive input into organizational privacy-related policies and procedures.
Legal	Provide advice around JSIF's privacy obligations; Monitor applicable privacy laws and policies (local and in other jurisdictions) that impact JSIF.
Document Owner/Approver	Review, update, and validate this Policy annually.
Employees	Comply with this Policy and associated standards and procedures to prevent unauthorized access or disclosure of JSIF data including Personal Data.
Business Unit Leaders	Keep the RoPA updated; Trigger PIA whenever they are necessary; Understand the full life cycle of the Personal Data processing activities; Assist the privacy office with DSRs; Identify privacy risk management requirements and controls including cases where 3rd parties are involved.
DPO	Monitor in an independent manner, JSIF's compliance with the provisions of the DPA (in accordance with section 20 of the DPA); Train and educate staff on data protection regulations, privacy policies, and best practices for handling personal data to ensure compliance and mitigate risks.
Third Parties	Implement security measures, conduct data processing activities with due care, and ensure compliance with privacy regulations when processing or handling personal data on behalf of JSIF.
Data Subjects	Provide accurate personal data; Validate their identity with JSIF upon request in order to exercise their rights under the DPA (e.g., access, rectification, erasure).

2. POLICY REQUIREMENTS

In today's digital landscape, safeguarding personal data is essential for organizations committed to upholding individuals' privacy rights. A comprehensive Data Privacy Program includes having Data Protection and Privacy Policies, a clear Privacy Notice, and carrying out Privacy Impact Assessments (PIAs) and Data Protection Impact Assessments (DPIAs) to identify and mitigate privacy risks. Additionally, maintaining Records of Processing Activities (RoPA) helps track data flows, while managing Data Subject Rights Requests ensures individuals can exercise their rights regarding personal information. Together, these elements create a proactive approach to data privacy and protection.

2.1 Data Privacy Program

Oversight for privacy compliance is governed by the Data Privacy Program (Program). The Program establishes processes that support compliance with the DPA by JSIF Business Units. The Program's privacy management framework lists leading practices regarding data protection and how JSIF meets those requirements. These practices involve:

- **Data Privacy Governance:** Define governance processes to manage privacy risks throughout the data lifecycle, along with other risks unique to JSIF. This includes management of privacy risks relating to records containing Personal Data.
- **Individual Rights**: Rights of the Data Subjects regarding their Personal Data, including individual rights such as, objection to processing, right of access, right to erasure, right to rectification.
- **Notice & Consent:** Implement appropriate measures to communicate the required information to individuals before collecting Personal Data.
- **Third Party Relationships:** Define a vendor management program with agile assessment tools and contractual mechanisms to comply with DPA requirements. Use of industry leading practices, technological solutions, and contractual measures to maintain effective privacy-compliant vendor relationships.
- **Security for Personal Data**: Enablement of data security measures implemented to help JSIF understand the different levels of data sensitivity and the industry specific security threats that inform JSIF's security posture.
- **Privacy Impact Assessments (PIAs)**: PIAs should be completed prior to processing personal information. The JSIF has defined a PIA template including privacy risk considerations and mitigation.
- **Cross Border Transfers:** Document and secure transfer of Personal Data across country borders when applicable.
- **Records Retention**: Define a sustainable data retention and destruction program adapted to our industry specific needs. The program helps overcome roadblocks and facilitate the effective execution of retention schedules and data destruction processes.
- **Record of Processing Activities (RoPAs):** Identify and document data flows to see how Personal Data moves throughout the internal systems of the organization to and from third-party operations. The data retention policy is effectively implemented and reviewed on a regular basis, as well as a data inventory that is regularly updated.
- **Personal Data Processing**: Legal justification for processing Personal Data must exist to evaluate defensibility from a compliance standpoint. Business Units are expected to collaborate among themselves to properly define reasons for processing Personal Data.

2.2 Data Protection and Privacy Policies

Policies with privacy requirements, including this Policy, must be reviewed annually, or as needed to reflect changes in business operations, the regulatory landscape, or due to contractual obligations.

This Policy applies to all JSIF employees in all Business Units. The terms of this Policy are strictly enforced. Any violations of this Policy will result in appropriate disciplinary action in accordance with the JSIF's Human Resources policies and procedures up to and including termination of employment. Any requests for an exception to this Policy must be directed to the Privacy Committee email (dataprotection@jsif.org).

2.3 Privacy Notice

When applicable, before collecting personal data, JSIF will provide a Privacy Notice (Notice) that describes JSIF's data processing practices. A Notice will be delivered by JSIF at the time Personal Data is collected by JSIF. Notices outline the following key points: the types of Personal Data collected, how it is used, the legitimate business purposes for processing, how Personal Data is disclosed and protected, Data Subject Rights, and any other relevant information as determined by Legal. Legal is responsible for creating and maintaining these Notices, and Business Units must notify Legal of any changes to the collection, use, storage, or processing of Personal Data to keep all Notices current. Additionally, JSIF may need to provide other notices as mandated by law.

2.4 Privacy Impact Assessment (PIA)

JSIF complies with various data privacy and protection obligations to effectively manage privacy risk. This includes mitigating risks by conducting Privacy Impact Assessments (PIA). A PIA is a process that identifies and assesses the potential privacy risks arising from business processes, systems, processes, strategies, changes, new projects, and business relationships. The process analyzes how Personal Data is collected, processed, shared, maintained, and disposed of. Refer to the Privacy Impact Assessment Procedure document for more information.

2.5 Data Protection Impact Assessment (DPIA)

JSIF is mandated to conduct a Data Protection Impact Assessment (DPIA) annually within ninety (90) days after the end of each calendar year. Based on the guidelines from the Office of the Information Commissioner, a DPIA template shall be maintained. The DPIA shall use the current Records of Processing Activities (RoPA) as well as completed PIAs as inputs. The Head of Privacy is required to conduct the DPIA exercise, in collaboration with relevant stakeholders and Business Units, as applicable.

While the DPIA and PIA are similar in nature, there are several key differences. The DPIA focuses on reducing privacy risks associated with the processing of Personal Data in an organization, whereas the PIA focuses on privacy by design, ensuring that the privacy risks of new processes or systems are sufficiently documented and addressed prior to implementation.

2.6 Records of Processing Activities (RoPA)

JSIF is required to maintain Records of Processing Activities (RoPA). The RoPA documents all Personal Data processing activities carried out by the Business Units within JSIF. The RoPA must be updated whenever new processing activities are undertaken by JSIF, or existing processes change, leveraging PIAs as inputs. Each Business Unit must complete a RoPA for each process involving Personal Data, in execution of its function. The Head of Privacy is responsible for maintaining and storing this document and should provide guidance to all stakeholders who process Personal Data in completing it. JSIF has developed a RoPA Template & Response Inventory.

2.7 Data Subject Rights Requests

The DPA grants Data Subjects a range of specific rights concerning their Personal Data, including:

1. Request for access
2. Request for rectification
3. Request to opt-out of data processing

4. Request in relation to automated decision-taking

In keeping with the rights of Data Subjects, JSIF has established a DSR Procedure which is to be followed when handling Data Subject Requests.

3. LIMITATIONS ON THE COLLECTION, USE, RETENTION, AND DISCLOSURE OF PERSONAL DATA

3.1 Standards for Processing Personal Data

The JSIF has adopted the following privacy standards outlined in the DPA when processing Personal Data. These principles are as follows:

1. Fair and Lawful Processing: Data may only be processed if the subject consents to the processing of data, and this consent has not been withdrawn. For the processing of sensitive data, this consent must be in writing.
2. Obtained Only for Specified Lawful Purposes: Data should be collected only for specified and lawful purposes and shall not be processed in any manner that is incompatible with those purposes.
3. Data Quality: Personal Data collected must be adequate, relevant, and necessary, relative to the purpose for which the data is processed.
4. Accurate and Up to Date: The data must be accurate and kept up to date when necessary.
5. Limited Retention: The data shall not be kept for longer than is necessary and will need to be disposed of in accordance with regulations.
6. Processed in Accordance with the Rights of Data Subjects: The Act outlines the rights of access to Personal Data, processing data for direct marketing, failure to comply with a notice.
7. Protected by Appropriate Technical and Organizational Measures: Additional technical and organizational measures are requisites, as is a data controller.
8. International Transfers: Transfer of data outside of Jamaica is prohibited unless an adequate level of protection can be ensured.

3.2 Data Sharing and Transfer

JSIF may share Personal Data with business partners, third parties, and specific service providers in line with the requirements set forth in this Policy and associated Standards. This Personal Data may be used for Processing transactions, fulfilling Data Subject's requests, responding to inquiries, and marketing.

All Personal Data sharing must be for Permissible Purposes and in compliance with regulatory and contractual obligations. Any third parties that are provided with or have access to Personal Data and sensitive Personal Data are required to implement appropriate organizational and technical safeguards consistent with the requirements of the DPA. The Business Unit leading the relationship with a Third Party is responsible for ensuring that the Third Party has the necessary controls as well as data sharing agreements, not only at the beginning of the relationship but for the entire lifecycle of the relationship. This obligation is written into the contract with the Third Party.

3.3 Procurement

JSIF requires that all Employees refer to the Third-Party Management Guidelines document when exploring business with a Third Party.

4. INFORMATION CLASSIFICATION

4.1 Data Classification Handling Guidelines.

Personal Data must be processed in conformance with best practices.

5. COMPLIANCE WITH LOCAL LAWS AND REGULATIONS

5.1 Consent for Marketing Campaigns

JSIF must comply with relevant laws addressing the use of Personal Data for marketing purposes, such as the DPA, and any other privacy regulations which mandate requirements on the Processing of Personal Data for marketing purposes.

JSIF may use Personal Data for marketing purposes such as for directly notifying a Data Subject of special promotions, offers, events, and/or to personalize advertisements to Data Subjects via email, direct mail, telephone, text message, push notification, and other means.

JSIF shall not process the Personal Data of a Data Subject for the purpose of direct marketing unless the Data Subject consents to the processing for that purpose, or the Data Subject is considered a customer of JSIF pursuant to the DPA section 10(4).

Business Units must always provide applicable Data Subjects with the ability to opt out of marketing campaigns such as those for email, direct mail, text message, push notification, telephone, etc. JSIF provides Data Subjects with the ability to opt out of certain marketing. Any exclusion and/or opt-out lists must be updated and operationalized.

5.2 Online Privacy

Each JSIF Business Unit that collects Personal Data online (for example, via contact forms, surveys) must develop procedures to ensure that Data Subjects have adequate Notice of JSIF's Processing practices. These policy objectives and standards apply to all websites, web portals, mobile applications, as well as other online offerings.

Business Units must engage with the Head of Privacy to ensure that the development of new online content, software, or offerings embodies the standards for processing Personal Data outlined in section 3.1.

6. TRAINING

6.1 Privacy Training and Awareness

Privacy awareness and training are integral to creating a culture of privacy compliance. Training materials must reflect key privacy requirements and be delivered to all impacted individuals based on the individual's job duties. Prior to deployment, training and awareness materials must be approved by the Head of Privacy who is knowledgeable of legal, regulatory, and contractual privacy requirements and corporate risk requirements.

7. DATA SECURITY AND INCIDENT RESPONSE

7.1 Data Security

JSIF protects the security of Personal Data it obtains and uses during its business processes. Policies and procedures are in place that are designed to safeguard Personal Data, such as acceptable use, access control, system configuration and patch management. Refer to JSIF's Information Security Policy for more information.

7.2 Incident Response

In the event of a data breach, the DPA (section 21) sets out various reporting requirements to be made by JSIF Employees. Refer to JSIF's Data Privacy Breach Procedure for more information.

8. RECORDS RETENTION

8.1 Retention of Personal Data

All Personal Data collected by JSIF will be retained in keeping with JSIF's record's management and retention practices.

8.2 Destruction of Personal Data

JSIF will promptly destroy Personal Data in accordance with the JSIF's record's management and retention practices, following consultation with Legal and a determination that a legal hold is not required or that the legal hold has been lifted.

9. COMPLIANCE AND MONITORING

The Head of Privacy is designated as the primary oversight authority, responsible for the implementation and enforcement of the Policy across all departments.

Compliance activities include regular audits, risk assessments, and training programs to educate employees on data privacy practices. Additionally, JSIF will utilize monitoring tools to track data processing activities and ensure that all data handling aligns with established privacy policies.

Continuous review and improvement processes will be in place to adapt to evolving regulations and best practices, ensuring ongoing compliance and protection of personal data.

10. VERSION CONTROL

Key Information

Title	**Enterprise Data Privacy Policy**
Prepared By	Ernst & Young Limited
Reviewed By	JSIFLegal
Owner	Legal & Governance
Approved By	
Date Effective From	
Version Number	V1.0

Review Frequency	Annually
Next Review Date	

Revision History

Version	Date	Summary Changes	Initials	Changes Marked

Approval: This document requires the following signed approvals.

Name/Title	Date	Version
Dr. Wayne Henry, Chairman, Board of Directors	Feb. 20, 2026	V1.0
Dr. Wayne Henry, Chairman, Corporate Governance and Ethics Committee	Feb 20, 2026	V1.0
Mr. Omar McFarlane-Sweeney, Managing Director	Feb. 20, 2026	V1.0

Distribution: This document has been distributed to

Name	Title/Division	Date of Issue	Version

Linked Policies/Documents
