TRELAWNY CO-OPERATIVE CREDIT UNION LIMITED

DATA PROTECTION POLICY

Policy #:	TCCU-DP-002
Policy Title: **DATA PROTECTION POLICY**	Signed on behalf of the Board of Directors by the Secretary of the Board:
Date of First Approval:	November 16, 2023
Previous Policy Review Date:	N/A
Current Policy Review Date:	N/A
Next Policy Review Date:	November 16, 2024
See Also:	Data Retention Policy, Authorities Schedule, ERM Policy
RESPONSIBILITY	
Responsibility for review of policy:	Data Protection Officer
Number of pages:	16

Table of Contents

1.0 Policy Objectives

This Data Protection Policy outlines how the Trelawny Co-Operative Credit Union (TCCU) handles the personal data of its employees, members, suppliers and other third parties.

This policy is intended to ensure that:

- there is compliance with the Data Protection Act, 2020 and is in keeping with considered industry good practice in protecting the personal data and sensitive personal data collected, stored and processed;
- the rights of employees, members (inclusive of all directors, committee members and other volunteers) and all business partners are protected;
- there is transparency about how individuals' data is stored and processed;
- the Credit Union is protected from the risks of a data breach.

Protecting the confidentiality and integrity of personal data is a critical responsibility of the Credit Union that is always taken seriously.

2.0 Scope

This policy applies to all personal data that is processed by the Credit Union (either directly or through an external data processor), regardless of the media on which that data is stored, or whether it relates to past or present employees, workers, members, suppliers, or any other data subject.

Anyone who works for the Credit Union, whether or not they are employees, must read, understand and comply with this policy when processing personal data. Any breach of the directives contained within this policy may result in disciplinary action.

3.0 Roles and Responsibilities

Board of Directors:

The Board of Directors has overall responsibility for ensuring compliance with the Data Protection legislation. The Board of Directors will approve, review and update this Data Protection Policy at least annually.

Supervisory Committee/ Audit Committee, Internal and External Auditors:

The Supervisory Committee and/or Audit Committee of the Board in conjunction with the Internal and External Auditors will ensure that the Credit Union's systems of internal controls are in compliance with the laws and regulations.

Management / General Manager:

The Management / General Manager will ensure that the Data Protection Policy is implemented and that controls are in place to facilitate compliance in line with the guidance of the Risk and Compliance Department and the Data Protection Officer (DPO).

Employees:

All employees of the Credit Union who collect and / or control the contents and use of personal data are responsible for compliance with the Data Protection Policy. The Credit Union will ensure that there is a program of ongoing training in the requirements under the Act.

The Data Protection Officer (DPO):

The DPO is responsible for monitoring in an independent manner, the Credit Union's compliance under the Act (Sec. 20) and will undertake a number of functions that will include, but not necessarily be limited to the following:

- Inform, advise and issue recommendations to the Credit Union regarding compliance with data protection requirements.
- Advise the Credit Union on whether or not the data protection impact assessment (DPIA) is in compliance with the Act and recommend the methodology and appropriate resources to use when conducting the DPIA. Also, to advise on any safeguards to apply to mitigate any risks to the rights and interests of the data subjects;
- Document all decisions taken by the Credit Union consistent with and contrary to advice given by the DPO; and
- Offer consultation to the Credit Union once a data breach or other incident has occurred.

4.0 Definitions

The Data Protection Act provides definitions for key terms used throughout this policy in Part 1 Preliminary Section 2 as follows:

Data controller: 'means any person or public authority, who, either alone or jointly or in common with other persons determines the purposes for which and the manner in which any personal data are, or are to be, processed, and where personal data is processed only for purposes for which they are required under any enactment to be processed, the person on whom the obligation to process the personal data is imposed by or under that enactment is for the purposes of this Act a data controller.'

Data processor: 'means any person, other than an employee of the data controller, who processes the data on behalf of the data controller.'

Data subject: 'means 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.'

Biometric data: 'means any information relating to the physical, physiological or behavioural characteristics of that individual, which allows for the unique identification of the individual, and includes:

- physical characteristics such as the photograph or other facial image, finger print, palm print, toe print, foot print, iris scan, retina scan, blood type, height, vein pattern, or eye colour, of the individual, or such other biological attribute of the individual as may be prescribed; and
- behavioural characteristics such as a person's gait, signature, keystrokes or voice.

Genetic data: 'means DNA as defined by the DNA Evidence Act, 2016.'

Personal data: 'means information (however stored) relating to a living individual, or an individual who has been deceased for less than 30 years, who can be identified from that information alone or from that information and other information in the possession of, or likely to come into the possession of, the data controller, and which includes any expression of opinion about that individual and any indication of the intentions of the data controller or any other person in respect of that individual.'

Sensitive personal data: [i]means personal data consisting of any of the following information in respect of a data subject:

- genetic data or biometric data.
- filiation, racial, or ethnic origin.
- political opinions, philosophical beliefs, religious beliefs or other beliefs of a similar nature.
- membership in any trade union.
- physical or mental health or condition.
- sex life; or
- the alleged commission of any offence by the data subject or any proceedings for any offence alleged to have been committed by the data subject.[i]

Process: 'in relation to information or personal data means obtaining, recording or storing the information or personal data, or carrying out any operation or set of operations (whether or not by automated means) on the information or data, including— (a) organisation, adaptation or alteration of the information or data; (b) retrieving, consulting or using the information or data; (c) disclosing the information or data by transmitting, disseminating or otherwise making it available; or (d) aligning, combining, blocking, erasing or destroying the information or data, or rendering the data anonymous.

5.0 Data Protection Standards

Trelawny Co-Operative Credit Union as a data controller, is committed to performing its responsibilities in accordance with the stipulated data protection standards contained in the Act in Part IV Sections 21-31 as follows:

i. ***Standard 1(Sec 22) - Fair and Lawful Processing*** – personal data must not be obtained by deception or any misleading information. There must be a legitimate reason for processing the data. The Data subject, must expressly consent to the processing of his/her data and such consent must be informed, freely given, specific, and unequivocal. The data subject must be provided with all the relevant information regarding the processing of his/her personal data which would enable the data subject to make an informed decision.

ii. ***Standard 2 (Sec 25) - Obtained only for Specified Lawful Purposes*** – personal data must not be processed in any manner incompatible with those purposes. Prior to collecting the personal data, data controllers are required to specify the purpose for obtaining the data and cannot use the data for any other purpose without first informing and, where necessary, receiving the consent of the data subject. Additionally, personal data must not be obtained for any illegal or immoral purpose.

iii. ***Standard 3 (Sec 26) - Adequate, Relevant and Limited*** - Personal data must be adequate, relevant, and where necessary must be limited to the purpose for which it is being processed. Processing of too much data may be deemed an invasion of privacy.

iv. ***Standard 4 (Sec 27) - Accurate and Up to Date*** - Personal data must be accurate and, where necessary, kept up to date. A data controller will not be in breach of this standard if the inaccurate data was provided by the data subject or a third party. However, the data controller who processes personal data is required to take reasonable steps to verify the accuracy of the data.

v. ***Standard 5 (Sec 28) - Limited Retention and Disposal Guidelines*** - Personal data must not be kept for longer than is necessary and must be disposed of in accordance with the Regulations (once passed) under the Act. Disposal is subject to any applicable retention periods prescribed by law. Data controllers are required to inform the data subject of the expected period of retention of their personal data, and this must be clearly set out in a privacy notice.

vi. ***Standard 6 (Sec 29) - Processed in accordance with the Rights of Data subjects***
Refer to Section 4.0 below.

vii. ***Standard 7 (Sec 30) - Protected by appropriate Technical and Organizational Measures to protect unauthorized or unlawful processing, accidental loss, destruction or damage to personal data and notification to the Information Commissioner of any breaches*** - Some of the technical and organisational measures include:

- conducting security audits (periodic and ad hoc).
- implementing data protection polices and privacy notices.
- proper training of employees on the handling, storage and disclosure of personal data.
- pseudonymisation and encryption of the data.
- limiting employees' access to the data.
- ensuring that any data-processing software and antivirus software used by the company are effectively maintained and kept up-to-date;

- selecting data processors who sufficiently guarantee that they have adequate security measures in place and will report security breaches;
- the ability to restore the availability of, and access to, personal data in a timely and secure manner in the event of a physical or technical incident.

viii. ***Standard 8 (Sec 31) – Processing International transfers without adequate protection of the rights of Data subjects*** - Personal data shall not be transferred to a State or territory outside of Jamaica unless that State or territory ensures an adequate level of protection for the rights and freedoms of the data subjects in relation to the processing of personal data. In determining what is considered as an 'adequate level of protection', the Information Commissioner will consider things such as:

- the nature of the data.
- the State or territory of final destination.
- the laws of the State or territory;
- the international obligations of the State or territory; and
- the security measures taken by the State or territory.

The Act, however, imposes certain limitations on this standard such as where the data subject has consented to the transfer or where the transfer is necessary for reasons of a substantial public interest or for the performance of a contract.

6.0 Rights of Data Subjects

TCCU will endeavour to uphold the rights of data subjects in accordance with the provisions of the Act as laid out in Part II Sec. 5-13 as follows:

- obtain consent from all data subjects for the processing of **personal data**. (Appendix - Consent Form).

- provide information on receipt to a request in writing from the data subject, on whether personal data is being processed by or on behalf of the Data controller, and if so, a description of the **type** of personal data that is being processed, the **purpose** for which the data is being processed and the **recipients** to whom the data is disclosed (Appendix – General Information Template)

- provide information constituting personal data and the source of that data or for transmittal of the data subjects' personal data to another data controller in a structured machine-readable format. Also, where automatic processing of personal data is for the purpose of evaluating matters relating to that individual (e.g., work performance, credit worthiness, reliability or conduct) or is likely to be the sole basis for any decision significantly affecting the individual, provide the **logic** involved in that decision making. (Appendix – Specific Data Subject Information Template). This attracts a fee based on the Fee Schedule of the Credit Union.

- obtain consent for the processing of **personal data** specifically for the purpose of **direct marketing**. The Credit Union must not approach the data subject to give consent more than once under these circumstances. Data subjects under special circumstances, have the right to issue a notice to cease or not to begin processing, in writing to the Credit Union and specific grounds cited for example if it is likely to cause substantial damage or distress to the Data subject or to another and is unwarranted for that purpose, the personal data is incomplete or irrelevant for the purpose, the personal data is prohibited under the Law for

that purpose, the personal data has been retained for longer than the period required under the Law**.**

The Credit Union shall respond within twenty-one (21) days after receiving the notice.

- provide the right of rectification by the data subject to correct inaccurate personal data concerning him held by the Credit Union.

- to be informed in the event that there is any contravention of the data processing standards or a security breach in the operations of the Credit Union. TCCU will outline the nature of the contravention or breach, measures taken or proposed to be taken to mitigate or address the adverse effects, and the name, address and contact information of the Data Protection Officer. (Sec. 21(5))

Note that the rights of the data subject are not always absolute and that the Act makes provisions under Part V – Sec.32 – 43 which covers **Exemptions to Data Protection Standards or to Disclosure to Data Subject Requirements**. These sections of the Act deal with the Minister's powers to issue exemptions on matters of National Security and further exemptions by order, published in the Gazette. It outlines exemptions in relation to taxation, statutory functions etc., regulatory activity or for special purposes.

7.0 Obligations of the Credit Union under the Act

TCCU is obligated under the Act as a data controller to carry out the following:

1. Appoint an appropriately qualified **Data Protection Officer** responsible specifically for **monitoring in an independent manner the Credit Union's compliance with the provisions of the Act.** The functions include:
    - ensuring that the Credit Union processes personal data in compliance with the eight (8) data protection standards and in compliance with the Act and good practice;
    - consulting with the Commissioner to resolve any doubt about how the provisions of the Act and any Regulations made under the Act are to be applied;
    - ensuring that any contravention of the data protection standards or any provisions of the Act by the Data controller is dealt with in accordance with Section 20 subsection (5);
    - assisting Data subjects in the exercise of their rights under the Act.

    Where the Data Protection Officer has reason to believe that the Data controller has contravened a data protection standard or any of the provisions of this Act, the Data Protection Officer shall—

    (a) forthwith in writing notify the Data controller of the contravention; and

    (b) if the Data Protection Officer is not satisfied that the data controller has rectified the contravention within a reasonable time after the notification, report the contravention to the Commissioner.

2. Register with the Office of the Information Commissioner by the stipulated date (currently November 30, 2023) by providing all the required information as set out in Sec. 16 (2) and be entered into the Register.

3. Submit **within ninety (90) days** after the end of **each calendar year** and in such form as may be prescribed by the Information Commissioner, by notice published in the Gazette, **a data protection impact assessment (DPIA) to the Information Commissioner** in respect of all personal data in the custody or control of the Credit Union. The DPIA must contain the following information:
    - a detailed description of the envisaged processing of the personal data and the purposes of the processing, specifying, where applicable, the legitimate interest pursued by the data controller.
    - an assessment of the necessity and proportionality of the processing operations in relation to the purposes;
    - an assessment of the risks to the rights and freedoms, of data subjects; and
    - the measures envisaged addressing the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the Act, taking into account the rights and legitimate interests of data subjects and other persons concerned.
4. **Report any contravention of the data standards and any security breach to the Information Commissioner** in respect of the Credit Union's operations which may affect personal data, **within 72 hours** after becoming aware of the contravention or breach. The report must set out specific information of the contravention or breach – the facts surrounding it, description of the nature of it including - category, number of Data subjects, type and number of data concerned, consequences and the name, address and contact information of the Data Protection Officer. (Sec. 21(5))

5. **Notify <u>each</u> Data subject** of the nature of the contravention or breach, measures taken or propose to be taken to mitigate or address the adverse effects, and the name, address and contact information of the Data Protection Officer.

8.0 Offences under the Act

TCCU and its officers are liable to offences under the Act. The key offences and penalties are presented in Table 1 below, subject to the passing of the Regulations.

OFFENCE	PARISH COURT	CIRCUIT COURT
Failure to comply with an enforcement notice **(Sec. 16(7))**	Fine of ≤$1million	N/A
Processing data requiring registration with the office of the Information Commissioner **(Sec. 18 (3))**	Fine of ≤$2 million **or** imprisonment ≤ 6 months	Fine **or** imprisonment ≤ 7 years
"Specified processing of data" without assessment and notification by the Information Commissioner **(Sec. 19 (5))**	Fine of ≤$5 million **or** imprisonment ≤ 5 years	Fine **or** imprisonment ≤ 10 years
Processing data in contravention of data protection standards **(Sec. 21 (2))**	Fine of ≤$2 million **or** imprisonment ≤ 2 years	Fine **or** imprisonment ≤ 7 years
Wilfully and unlawfully breaching any pseudonymisation or encryption applied to personal data **(Sec. 30 (7))**	Fine of ≤$2 million	Fine
Unlawfully obtaining or disclosing personal information **(Sec. 61 (10))**	Fine of ≤$5 million **or** imprisonment ≤ 5 years	Fine **or** imprisonment ≤ 10 years

Notwithstanding the above, a body corporate can be fined up to 4% of annual gross worldwide income for the preceding year in accordance with the Income Tax Act.

Signatures of Approval

Trelawny Co-Operative Credit Union

……... **……..…**

PRESIDENT **Date**

…… **……..…**

SECRETARY **Date**

9.0 APPENDIX

9.1 Consent Form

I, [Your Full Name], hereby give my consent for the Trelawny Co-Operative Credit Union to process my personal data as described in this consent form for the purposes outlined.

Signature: _____

Date: _____

9.2 General Information Template

Our data processing activities are carried out in accordance with the Data Protection Act 2020. We are committed to maintaining the confidentiality, integrity, and availability of your data while ensuring its lawful and fair processing.

Type of Personal Data Processed:

At the Trelawny Co-Operative Credit Union (TCCU), we may collect and process the following types of personal data, as necessary for the purposes described in this document:

- Name and/or Aliases
- Date of Birth and Place of Birth
- Gender and Nationality
- Taxpayer's Registration Number (TRN)
- National Insurance Number (NIS)
- Proof of Employment
- Contact Information (e.g., address, phone number, email)
- Identification Information (e.g., passport, driver's license)
- Financial Information (e.g., bank statements, income statements)
- Employment Status & Details
- Politically Exposed Person Status
- Financial Information

Purpose of Data Processing:

We collect and process your personal data for the following purposes:

1. **Providing and Managing Services:** We process your data to deliver our products, services, and support, as well as to manage and maintain our customer relationships.
2. **Legal and Regulatory Compliance:** We process your data to comply with legal and regulatory requirements, including but not limited to taxation, anti-money laundering, and know-your-customer checks.

3. **Communication:** We may use your data to communicate with you about our services, updates, important notices, and other relevant information.
4. **Improvement:** We analyze your data to enhance the quality of our services, identify areas for improvement, and tailor our offerings to better meet your needs.
5. **Marketing and Promotions:** If you have provided your consent, we may use your data for marketing and promotional activities, such as sending you newsletters, offers, or event invitations.

Recipients of Personal Data:

We may disclose your personal data to the following recipients, when necessary and in compliance with applicable data protection laws:

- Service Providers: We may share your data with third-party service providers who assist us in delivering our services, maintaining our IT infrastructure, and conducting business operations.
- Partners: In certain cases, we may share data with business partners or affiliates to provide joint services or offerings.
- Regulatory Authorities: We may disclose data to comply with legal and regulatory requirements or to respond to requests from government or law enforcement authorities.
- Other Third Parties: We may share data with other third parties as required by law, in the context of legal proceedings, or to protect our legal rights.

We ensure that all third parties with whom we share data are contractually bound to protect your information and use it solely for the purposes specified.

For any inquiries about your personal data, exercising your rights, or seeking more information about our data processing practices, please contact us at **dpo@jtccu.com**.

9.3 Specific Data Subject Information Template

Introduction:

This document provides specific information to you, the data subject, about how your personal data is processed by the Trelawny Co-Operative Credit Union Limited. We are committed to ensuring the privacy and security of your personal information. Please take the time to read this information carefully.

Data Controller:

Trelawny Co-Operative Credit Union Ltd

Water Square, Falmouth, Trelawny

Tel: 876-954-3253

Type of Personal Data Processed:

We currently process the following types of personal data for you, as applicable:

Types of Personal Data we have collected.	Types of Personal Data we have collected.

Purposes of Data Processing:

We may use the information we collect from you in connection with the services we provide for a range of reasons, including to:

- Process and complete transactions, and send related information, including transaction confirmations and records.
- Manage our members' use of the services, respond to enquiries and comments and provide customer service and support.

- Send alerts, updates, security notifications, and administrative communications.
- Verify your identity, creditworthiness and the accuracy of the information provided.
- Prevent criminal activity, fraud and money laundering.
- Trace debtors and recover debts.
- Investigate and prevent fraudulent activities, unauthorized access to our services, and other illegal activities; and
- For any other purposes about which we notify members and users.

Recipients of Personal Data:

We may disclose your personal data to the following recipients, when necessary and in compliance with applicable data protection laws:

- **Service Providers:** We may share your data with third-party service providers who assist us in delivering our services, maintaining our IT infrastructure, and conducting business operations.
- **Partners:** In certain cases, we may share data with business partners or affiliates to provide joint services or offerings.
- **Regulatory Authorities:** We may disclose data to comply with legal and regulatory requirements or to respond to requests from government or law enforcement authorities.
- **Other Third Parties:** We may share data with other third parties as required by law, in the context of legal proceedings, or to protect our legal rights.

Data Transfers:

In some cases, your data may be transferred to recipients located outside your country. We take appropriate measures to ensure that such transfers comply with data protection laws and that adequate safeguards are in place to protect your data.

Data Retention:

We retain your personal data only for as long as necessary to fulfill the purposes for which it was collected, unless a longer retention period is required or permitted by law.

Your Rights:

You have the following rights under data protection laws:

- **Access:** You have the right to access the personal data we hold about you.
- **Rectification:** You can request the correction of inaccurate or incomplete data.
- **Erasure:** You may request the deletion of your data in certain circumstances.
- **Restriction of Processing:** You can request the restriction of processing in specific situations.
- **Data Portability:** You have the right to receive your data in a structured, commonly used, and machine-readable format.
- **Objection:** You may object to the processing of your data for certain purposes.

Contact Information:

For any inquiries about your personal data, to exercise your rights, or for further information about our data processing practices, please contact our Data Protection Officer at **dpo@jtccu.com.**