CENTRAL AFRICA BUILDING SOCIETY 'CABS'

DATA PROTECTION POLICY

Policy Owner

Head of Compliance

Contact

Head of Compliance

Version/Date

Version 2/April 2024

Effective Date

This Policy was approved by the 16 April 2021. It is effective from 1 July 2021.

Responsible	Date
Policy prepared by CABS Compliance	January 2021
Reviewed by Head of Compliance	April 2021
Reviewed by CABS Risk	April 2021
Approved by Exco	April 2021
Approved by Board Risk and Compliance	April 2021
Approved by Board	April 2021
Policy became operational on:	1 July 2021
Next review date:	April 2022
This policy shall be reviewed at least annually.	
Reviewed by Head of Compliance	April 2024
Reviewed by CABS Risk	April 2024
Approved by Exco	2024
Approved by Board Risk and Compliance	2024
Approved by Board	2024
Next review date:	April 2025

1. INTRODUCTION

CABS needs to gather and use information about its customers, suppliers, business contacts, employees, outsourced partners and third parties that the Society has a relationship with or may need to contact. This policy describes how once this information has been collected, has to be handled, processed and stored to meet the Society's data protection standards and to comply with the law.

2. KEY TERMS

Data controller or controller: (a) Any natural person or legal person who is licensable by the Authority; (b) includes public bodies and any other person who determines the purpose and means of processing data.

Data controller's representative: Any natural person or legal person who performs the functions of the data controller in compliance with obligations set forth.

Data processor: A natural person or legal person, who processes data for and on behalf of the controller and under the controller's instruction, except for the persons who, under the direct employment or similar authority of the controller, are authorised to process the data.

Data: Any representation of facts, concepts, information, whether in text, audio, video, images, machine-readable code or instructions, in a form suitable for communications, interpretation or processing in a computer device, computer system, database, electronic communications network or related devices and includes a computer programme and traffic data.

Data protection officer: Any individual appointed by the data controller and is charged with ensuring, in an independent manner, compliance with the obligations provided for by the law.

Data subject: An individual who is an identifiable person and the subject of data.

Personal information: Information relating to a data subject, and includes—

(a) the person's name, address or telephone number;
(b) the person's race, national or ethnic origin, colour, religious or political beliefs or associations;
(c) the person's age, sex, sexual orientation, marital status or family status;
(d) an identifying number, symbol or other particulars assigned to that person;
(e) fingerprints, blood type or inheritable characteristics;
(f) information about a person's health care history, including a physical or mental disability;
(g) information about educational, financial, criminal or employment history;
(h) opinions expressed about an identifiable person
(i) personal correspondence pertaining to home and family life;

Processing: Any operation or set of operations which are performed upon data, whether or not by automatic means, such as obtaining recording or holding the data or carrying out any operation or set of operations on data, including—

(a) organisation, adaptation or alteration of the data;
(b) retrieval, consultation or use of the data;
(c) alignment, combination, blocking, erasure or destruction of the data;

3. WHY THIS POLICY EXISTS

This Data Protection policy ensures that CABS:

- Complies with data protection laws and follows good practice;
- Protects the rights of customers, staff and any third parties that it does business with;
- Practices transparency with regards to how it stores and processes personal data; and
- Protects itself from the risks of a data breach.

4. DATA PROTECTION LAW

The Data Protection Act, EU General Data Protection Regulation, the Reserve Bank of Zimbabwe Consumer Protection Framework and Consumer Protection Act prescribe how organisations including the Society must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other mediums.

To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully.

These laws and regulations are underpinned by six important principles which indicate that data must:

(i) Be processed fairly, lawfully and in a transparent manner with the consent of the data subject;
(ii) Be obtained only for specific, lawful purposes and used only for the purpose for which it was sought;
(iii) Be adequate, relevant and not excessive (data minimisation);
(iv) Be accurate and kept up to date and there should be provision for erasure of inaccurate data or rectification without delay;
(v) Not be held for any longer than necessary;
(vi) Be processed and stored in a manner that ensures appropriate security ('integrity and confidentiality') and in accordance with the rights of data subjects.

5. POLICY SCOPE

This Policy is applicable to CABS (also referred to as the Society), all its subsidiaries where CABS as the ultimate shareholder has management control and all third parties including external service providers to the Society. In instances where CABS as a shareholder does not have effective management control, this Policy will apply insofar it has been agreed with the other shareholders. No subsidiary is out of scope of this Policy unless it is expressly indicated.

The Policy applies to all personal data that the Society holds relating to identifiable individuals. Personal data is defined as anything that one could conceivably use to identify a person within a larger group and personal data is looked at singularly as well as combined.

Unless required to do so by law; or where explicit consent is given by the data subject; or where processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent the collection and/or processing of data that reveals any of the following shall not be permissible.

Personal data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

6. DATA PROTECTION RISKS

This policy helps to protect CABS from data security risks, such as **Breaches of confidentiality** (information being given out inappropriately) and Reputational damage.

7. RESPONSIBILITIES

All employees, outsourced partners and third parties contracted by the Society have a 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.

However, the following persons have key areas of responsibility which are detailed below;

(a) Board of Directors

The **board of directors** is ultimately responsible for ensuring that CABS meets its legal obligations.

(b) Data Protection Officer

The CABS Head of Compliance shall be the Data Protection Officer.

Contacts details for the Data Protection Officer are:

CABS Head Office
Northridge Park
Northend Close
Highlands
Harare
Tel: 0242 883823-60 Ext 1110
Email address: FarirayiMachawira@cabs.co.zw

This office is responsible for the following;

- Keeping the Board updated about data protection responsibilities, risks and issues;
- Reviewing all data protection procedures and related policies, in line with an agreed schedule;
- Working with the Data Protection Authority (POTRAZ) in relation to the performance of its functions in relation to the data controller.
- Arranging data protection training and advice for the people covered by this policy;
- Handling data protection questions from staff and anyone else covered by this policy;
- Dealing with requests from customers to see the data that the Society holds about them (also called 'subject access requests'); and
- Checking and approving any contracts or agreements with third parties that may handle the company's sensitive data.

(c) ICT

This office is responsible for the following

- Ensuring all systems, services and equipment used for storing data meet acceptable security standards. This includes ensuring that all servers and computers containing data are protected by approved security software and a firewall.
- Performing regular checks and scans to ensure security hardware and software is functioning properly.
- Evaluating any third-party services, the company is considering using to store or process data.
- Ensure that data is backed up frequently. Those backups should be tested regularly, in line with the Society's standard backup procedures.

(d) Marketing

This office is responsible for:

- Approving any data protection statements attached to communications such as emails and letters.
- Addressing any data protection queries from journalists or media outlets like newspapers.
- Where necessary, working with other staff to ensure marketing initiatives abide by data protection principles.
- Ensuring that marketing databases are checked against customer T24 files every six months such that communication is sent to the customer's current contact details.

8. CABS DATA PROTECTION PRINCIPLES

(a) Lawful, fair and transparent processing

To ensure its processing of data is lawful, fair and transparent, CABS shall maintain a Register of Systems. The Register of Systems shall be reviewed at least annually. Individuals have the right to access their personal data and any such requests made to the Society shall be dealt with in a timely manner.

The Society must seek consent from data subjects where personal data is sought. In all terms and conditions, requests for consent must be in plain language, must be explicit i.e. it must not be buried in other terms and conditions.

Consent must be clearly sought from customers for automated profiling and background checks that will be done using the customer's personal information. Clear consent must also be sought where the Society requests for information on any of the following categories: Race; Ethnic origin; Political opinions; Religious or philosophical beliefs; Trade Union membership; Genetics; Biometrics; Health and Sex life.

(b) Lawful purposes

All data processed by the Society must be done on one of the following lawful bases: consent, contract, legal obligation, vital interests, public task or legitimate interests. The Society shall note the appropriate lawful basis in the Register of Systems.
Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Society's systems. All personal data in the custody of the Society should be used only for the sole purpose for which it was sought or requested for.

(c) Data minimisation

The Society shall ensure that personal data that is requested from customers is adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed. In addition, the Society should not amass large volumes of personal data that are not relevant for the purpose for which they are intended to be processed. Personal data must be adequate to ensure that the Society can fulfil the purpose for which it was intended to be processed.

(d) Accuracy

The Society shall take reasonable steps to ensure personal data is accurate. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.

It is the responsibility of all employees who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible. Data should be held in **as few places as necessary** and employees should not create any unnecessary additional data sets.

The Society will make it **easy for data subjects to update the information it holds** about them. Data should be **updated as inaccuracies are discovered**.

(e) Accessible

The Society shall take all appropriate measures to ensure that data processed shall be accessible regardless of the technology used and ensure that the evolution of technology shall not be an obstacle to the access or processing of such data.

(f) Disclosure

The Society shall provide the data subject with at least the information set out below when recording the data or considering communication to a third party, unless it is established that the data subject is in receipt of such information

(i) the name and address of the Society and its representative,
(ii) the purposes of the processing;
(iii) whether compliance with the request for information is compulsory or not, as well as what the consequences of the failure to comply are;
(iv) the existence of the right to object, by request and free of charge, to the intended processing of data relating to him or her, if it is obtained for the purposes of direct marketing; in which case, the data subject shall be informed prior to the first disclosure of the data to a third party or prior to the first use of the data for the purposes of direct marketing on behalf of third parties;
(v) the existence of the right to access and rectify the data relating to him/her, unless such additional information, taking into account the specific circumstances in which the data is provided, is not necessary to guarantee fair processing.

(g) Archiving / removal

The Society has in place a Records Management Policy that speaks to archiving and retention periods of personal data. It ensures that personal data is kept for no longer than necessary as it consider what data should/must be retained, for how long, and why.

(h) Security

To safeguard the security, integrity and confidentiality of data, the Society, shall take the appropriate

technical and organisational measures necessary to protect data from negligent or unauthorised destruction, negligent loss, unauthorised alteration or access and any other unauthorised processing of the data.
Access to personal data shall be limited to personnel who need access and appropriate security should be in place to avoid unauthorised sharing of information. When personal data is deleted this should be done safely such that the data is irrecoverable. Appropriate back-up and disaster recovery solutions shall be in place.
The Society shall appoint a data processor who shall provide sufficient guarantees regarding the technical and organisational security measures employed to protect data and ensure strict adherence to such measures.

9. GENERAL DATA PROTECTION OBLIGATIONS FOR EMPLOYEES AND OUTSOURCED PARTNERS

(i) The only people able to access data covered by this policy should be those who **need it for their work**.
(ii) Data **should not be shared informally**. When access to confidential information is required, employees can request it through their line managers.
(iii) The Society will provide training to all employees to help them understand their responsibilities when handling data.
(iv) Employees should keep all data secure, by taking sensible precautions and following the guidelines below.
(v) In particular, **strong passwords must be used,** and they should never be shared.
(vi) Personal data **should not be disclosed** to unauthorised people, either within the company or externally.
(vii) Data should be **regularly reviewed and updated** if it is found to be out of date. If no longer required, it should be deleted and disposed of as per the Records Management Policy.
(viii) Employees **should request help** from their line manager or the data protection officer if they are unsure about any aspect of data protection.
(ix) Use of data: Data printouts should be shredded and disposed of securely when no longer required. Data should only be stored on designated drives and servers and should only be uploaded to an approved cloud computing services. Employees should not save copies of personal data to their own computers. Always access and update the central copy of any data.

10. ERASURE AND RECTIFICATION

CABS must put in place a procedure to handle data deletion or data processing restriction requests from data subjects.

The Society may however refuse a request for erasure where the personal data is processed for the following reasons:

- to exercise the right of freedom of expression and information;
- to comply with a legal obligation or for the performance of a public interest task or exercise of official authority;

Where CABS had processed the personal data of children, special attention needs to be paid to requests of erasure (regardless of age at the time of the request).

The Society is required to inform third parties about the erasure of a persons' personal data, unless it is impossible or involves disproportionate effort to do so.

This clause shall not apply to the extent that processing is necessary for compliance with a legal obligation which requires processing by law or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; or for the establishment, exercise or defence of legal claims.

The data subject shall have the right to obtain from the Society without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account, the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

11. SUBJECT ACCESS REQUESTS

All individuals who are the subject of personal data held by CABS are entitled to:

- Ask **what information** the company holds about them and why;
- Ask **how to gain access** to it;
- Be informed **how to keep it up to date;**
- Be informed how the company is **meeting its data protection obligations**.

If a customer contacts the Society requesting this information, this is called a subject access request. Subject access requests from individuals should be made by email, addressed to the Centralised Operations Manager (Data Controller) at DataControl@cabs.co.zw. This email group will include the Information Protection Officer (this role is currently fulfilled by the CABS Head of Operations) and Centralised Operations Manager. The Data Controller can supply a standard request form, to be completed for subject access request.

The data controller will always verify the identity of anyone making a subject access request before handing over any information.

Data subjects have a right to data portability. Thus, the Society must put in place a procedure for when data subjects request the Society to submit their information in the Society's custody to another entity/person.

Where it is a third party requesting for a customer's information, they should attach documentary evidence of the data subject's consent to the requestor's access.

12. DISCLOSING DATA FOR OTHER REASONS

In certain circumstances, the law allows personal data to be disclosed to law enforcement agencies without the consent of the data subject.

Under these circumstances, CABS will disclose requested data. However, the data controller will ensure the request is legitimate, seeking assistance from the data protection officer and from the company's legal advisors where necessary.

13. DUTY TO PROVIDE INFORMATION

The Society aims to ensure that data subjects are aware that their data is being processed, and that they understand:

- How the data is being used; and
- How to exercise their rights.

To these ends, the Society has a privacy statement, setting out how data relating to individuals is used by the Society. A version of this statement is also available on the Society's mobile application and website.

14. BREACH

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Society shall promptly assess the risk to customer's rights and freedoms and if appropriate report this breach to the data protection officer within 24 hours of the breach having taken place. The Data Protection Officer shall notify the Postal and Telecommunications Regulatory Authority, the Reserve Bank of Zimbabwe and other relevant authorities within 24 hours of receiving this notification. If the breach is sufficiently serious to warrant notification to the public, the Society through its Marketing Executive must do so without undue delay.

In cases where the Society uses a data processor, and this processor suffers a breach, then this processor must inform the Society without undue delay as soon as it becomes aware. The requirements on breach reporting should be detailed in contracts between the Society and the processor.

A breach notification must include the following;

- a description of the nature of the personal data breach including, where possible:
- the categories and approximate number of individuals concerned; and
- the categories and approximate number of personal data records concerned;
- a description of the likely consequences of the personal data breach; and
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach, including, where appropriate, the measures taken to mitigate any possible adverse effects.