Charles Merrington
Executive Financial Services (Pty) Ltd

Authorised Financial Services
Provider Licence Number 12833

PROTECTION OF PERSONAL INFORMATION POLICY

1. Scope

This policy applies to everyone with access to Personal Information available to them due to their relationship with Charles Merrington Executive Financial Services (Pty) Ltd, (CMEFS).

It addresses the rights of Data Subjects, being the various categories of people whose personal information we have access to.

Personal Information broadly means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a specific natural or juristic person / Data Subject.

This policy must be read together with CMEFS's Records Management, Cyber Security and Business Continuity Policies.

2. Purpose

This Policy aims to ensure CMEFS's compliance with various laws and regulations addressing Personal Information and sets out how CMEFS handles their Data Subjects' Personal Information and additionally lists the purpose(s) said information is used for.

3. Policy

CMEFS is committed to protecting the privacy of Data Subjects and to ensuring that their Personal Information is used appropriately, transparently, securely and in accordance with applicable laws.

We subscribe to the Protection of Personal Information Act Principles and will:

1. Obtain and process information fairly.
2. Keep information only for one or more specified, explicit, and lawful purpose.
3. Use and disclose information only in ways compatible with these purposes.
4. Keep information safe and secure.
5. Keep information accurate, complete, and up to date.
6. Ensure that information is adequate, relevant, and not excessive.
7. Retain information for no longer than is necessary for the purpose or purposes.
8. Provide a copy of personal data kept to the Data Subject on request.

4. Background and definitions

4.1 Definitions

Personal Information broadly means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly to a specific natural or juristic person / Data Subject.

Data Subjects means the various categories of people whose personal information we have access to e.g., our employees and our clients.

Processing in this context mean to collect, store, and share Personal Information.

4.2 Conditions for processing

In terms of the provisions of the Protection of Personal Information Act, Personal Information may only be processed if certain conditions are met:

- When the Data Subject consents to the processing – consent is only required where the information will be used for something other than the intended use for which the information is supplied.
- When the processing is necessary.
- When processing complies with an obligation imposed by law on CMEFS.
- When processing protects the legitimate interest of the Data Subject.
- When processing is necessary for pursuing the legitimate interest of CMEFS or of a third party to whom information is supplied.

4.3 Type of Personal Information

CMEFS will generally collect some of the following personal information from our Data Subjects:

- Information relating to the race, gender, sex, pregnancy, marital status, national, ethnic, or social origin, colour, age, physical or mental health, well-being, disability, language, and birth.
- Information relating to the education, medical, financial, criminal or employment history.
- Identifying number, name, symbol, e-mail address, physical address, telephone number, location information.
- Biometric information (employees).
- Correspondence sent/received that is implicitly or explicitly of a private or confidential nature or further correspondence that would reveal the contents of the original correspondence.
- The views or opinions of another individual about our Data Subject.

4.4 Purpose of processing

We may use this information in the process of:

- Providing a product / service to a Data Subject;
- As part of employee on-boarding or any other internal human resources function;
- Conducting credit reference searches or verification;
- Confirming, verifying, and updating contact details;
- For the detection and prevention of fraud, crime, money laundering or other malpractice;
- For audit and record keeping purposes;
- In connection with legal proceedings;
- Providing our services to a Data Subject to carry out the services requested and to maintain and constantly improve the relationship;
- Providing communications in respect of CMEFS and regulatory matters that may affect Data Subjects;
- In connection with and to comply with legal and regulatory requirements or when it is otherwise allowed by law;
- To carry out the transaction(s) requested;
- For underwriting purposes;
- Assessing and processing claims;
- For purposes of claims history; and or
- Conducting market or customer satisfaction research.

5. Procedures

5.1 Collection

We will collect Personal Information directly from Data Subjects but may also supplement the information provided with information we receive from other providers to offer a more consistent and personalised experience in clients' interaction with us.

5.2 Processing

Personal Information will be processed for the same purpose as what it was collected, and we will share information with third parties for the reasons provided above.

5.2.1 General sharing of Personal Information

CMEFS has however concluded agreements with all our service providers that process information on our behalf placing an obligation on these providers to keep this information confidential and to take the necessary measures to protect it.

Additionally, CMEFS also has a process in place to determine if the parties with whom we duly share the Personal Information of our Data Subjects subscribes to the same data protection principles as what we do.

We recognise that the processing of a minor's personal Information is subject to (as a minimum) the relevant parent or guardian's implied consent.

5.2.2 Sharing Personal Information with entities in foreign countries

We may need to transfer Personal Information to another country for processing or storage. We will endeavor to ensure that anyone to whom we pass personal information is subject to the same Data protection regulations as what we are or agrees to treat Personal Information with a similar level of protection as afforded by ourselves.

5.2.3 Safeguarding Personal Information

We will adequately protect the Personal Information we hold and avoid unauthorised access and use of Personal Information. We will continuously review our security controls and processes to ensure that personal Information is secure.

When we contract with third party providers for the safekeeping of information, we will impose appropriate security, privacy, and confidentiality obligations on them to ensure that Personal Information is kept secure.

5.3 Access and correction of Personal Information

Data Subjects have the right to access the Personal Information we hold about them. Data Subjects also have the right to request us to update, correct or delete their Personal Information on reasonable grounds. Once a Data Subject objects to the processing of their Personal Information, CMEFS may no longer process said Personal Information. We will take all reasonable steps to confirm our Data Subject's identity before providing details of their Personal Information or making changes to their Personal Information. CMEFS's Information Officer will be responsible for managing this process.

5.4 Data breaches

Even though CMEFS will take every precaution to prevent a data breach, a breach may still occur.

A personal data breach is a breach of security leading to a:

- Confidentiality breach – an accidental or unauthorized disclosure of, or access to, personal data.
- Availability breach – an accidental or unauthorized loss of access to, or destruction of, personal data and/or
- Integrity breach – an accidental or unauthorized alteration of personal data.

5.4.1 Notification to the Information Regulator ("IR")

The Information Regulator must be notified of the breach if it is likely to result in a risk to the rights and freedoms of data subjects i.e., if, for example, it could result in:

- loss of control over their data
- limitation of their rights
- discrimination
- identity theft
- fraud
- damage to reputation
- financial loss
- unauthorized reversal of pseudonymization
- loss of confidentiality
- any other significant economic or social disadvantage.

Where a breach is reportable, the Company must notify the Information Regulator without undue delay and, where feasible, no later than 72 hours after becoming aware of the breach. If our report is submitted late, it must also set out the reasons for our delay.

The notification must at least include:

- a description of the nature of the breach including, where possible, the categories and approximate number of affected data subjects and the categories and approximate number of affected records;
- the name and contact details of the Information Officer;
- a description of the likely consequences of the breach; and
- a description of the measures taken, or to be taken, by the Company to address the breach and mitigate its possible adverse effects.

5.4.2. Communication to affected Data Subjects

Where the personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, CMEFS also needs to communicate the breach to the affected data subjects without undue delay, i.e., as soon as possible.

Reporting to Data Subjects may however be delayed if reporting may lead to an increased risk to the Data Subject.

In clear and plain language, CMEFS must provide affected Data Subjects with:

- a description of the nature of the breach;
- the name and contact details of CMEFS's Information Officer and CEO;
- a description of the likely consequences of the breach;
- a description of the measures taken, or to be taken, by CMEFS to address the breach and mitigate its possible adverse effects;
- practical advice on how to limit the damage, e.g., resetting their passwords; and
- Data subjects will be contacted individually, by e-mail, unless that would involve CMEFS in disproportionate effort such as where contact details have been lost as a result of the breach or were not known in the first place, in which case we will use a public communication, such as a notification on our website.

However, CMEFS is not required to report the breach to Data Subjects if:

- appropriate technical and organisational protection measures have been implemented, and those measures have been applied to the personal data affected by the breach, in particular those that render the personal data unintelligible to any person who is not authorised to access them, such as state-of-the-art encryption, or
- subsequent measures were taken to ensure that the high risk to the rights and freedoms of Data Subjects is no longer likely to materialize.

Any communication to Data Subjects with regards to Data Breaches may under no circumstances be sent or published without prior approval of CMEFS's Information Officer.

5.4.3 Data breach register

CMEFS will maintain a register of all personal data breaches, regardless of whether they are notifiable to the Information Regulator. Please see a template register in Annexure A.
5.4.4 Data breach reporting procedure
If anyone knows or suspects that a personal data breach has occurred, they must immediately both advise their line manager and contact the Deputy Information officer or Information Officer. Any evidence relating to the breach discovered and report must be retained.

The Deputy Information Officer will investigate and assess the suspected data breach in accordance with the response plan set out below and will determine who should be notified and how.

5.4.5 Response plan

The Deputy Information Officer must:

- Make an urgent preliminary assessment of what data has been lost, why and how.
- Take immediate steps to contain the breach and recover any lost data.
- Undertake a full and detailed assessment of the breach.
- Record the breach in the Company's data breach register.
- Notify the Information Regulator where the breach is likely to result in a risk to the rights and freedoms of data subjects.
- Notify affected Data Subjects where the breach is likely to result in a high risk to their rights and freedoms.
- Respond to the breach by putting in place any further measures to address it and mitigate its possible adverse effects, and to prevent future breaches.

Please see Annexure B for more information.

5.4.6 Information Officer and Deputy Information Officer

The Protection of Personal Information Act appoints the highest level of authority in an organisation as the Information Officer. The Information Officer has been tasked with ensuring compliance with data protection and privacy legislation and regulations.

The Information Officer has appointed a Deputy Information Officer to perform the required tasks. Please see Annexure C for a template Deputy Information Officer appointment letter.

The details of our Information Officer and Deputy Information Officer are as follows:

Information Officer

Name & Surname: Clive Donk
Email: it@cmefs.co.za

Information Officer Registration Number:

Deputy Information Officer

Name & Surname: Charles Merrington

ANNEXURE A: CMEFS DATA BREACH REGISTER

Date the breach occurred	Description of the breach	Breach category	Breach Reported to IR	Number of data subjects affected	Data subject impact classification	Number of records affected	Reported to data subject	Impact of the breach on CMEFS	Remedial action taken
		Confidentiality Availability Integrity	Yes No N/A		Serious Moderate None		Yes No N/A		

ANNEXURE B: DATA BREACH RESPONSE PLAN FOR CMEFS

