Protection of Personal Information Act Notice

FSP Name: Mont Blanc Financial Services
FSP Number: 8271
Date: 2026

1. Version Control

The Responsible Party undertakes to review this policy regularly.

Version number	Version date	Summary of changes made
1	05/02/2026	General 2026 update
2	30/04/2026	Addition of Employee Health Data & Cloud Services

2. Definitions

Data Subject means the person to whom personal information relates and can be a natural or legal person.

Personal Information means information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to—

- information relating to the race, gender, sex, pregnancy, marital status, national, ethnic or social origin, colour, sexual orientation, age, physical or mental health, well-being, disability, religion, conscience, belief, culture, language and birth of the person;
- information relating to the education or the medical, financial, criminal or employment history of the person;
- any identifying number, symbol, e-mail address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
- the biometric information of the person;
- the personal opinions, views or preferences of the person;
- correspondence sent by the person 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 the person; and
- the name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person;
- Personal information concerning a child.

Third Party Operator means a person (natural or legal) who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party.

Health Information means the personal information relating to a data subject's physical or mental health, including information arising from healthcare services, testing, treatment or diagnosis.

3. Introduction

The Protection of Personal Information Act 4 of 2013 requires that we keep plans and process in place on how we process, store and share personal information. We respect our clients' right to privacy and endeavour to collect and use information minimally, transparently, and for the purpose for which it was collected. This Policy and supporting documents are written in easily understandable language so that is practical in usable to a wide audience in the business.

The Responsible Party is committed to keeping information safe and secure, to provide persons with reasonable access to their information, and to give effect to the rights in terms of POPI. To this extent, we emphasise that only the necessary information is collected and used accordingly. The collection serves to protect legitimate legal interests and ensures that we are able to offer clients a service or product.

4. Application of this Policy

The obligations in this policy apply to The Responsible Party, its management, staff members, and representatives. Any Third Parties who The Responsible Party entrusts personal information to are also bound by the terms in this policy. It applies to all Personal Information gathered from Data Subjects.

5. Security Measures with regards to confidentiality of personal information

5.1 Purpose of Collection

The Responsible Party requires certain categories of information to ensure that clients receive high quality services and that client needs are met as they may require from time to time. The same goes for any partnerships, due diligence or other third party interactions where personal information is gathered. Information may be collected for explicitly defined purposes or incidental to the function, activity or service of the Responsible Party or a third party that might be our service providers.

The Responsible Party warrants that personal information will never be used for a reason that is not in line with what it was collected for. Should the purpose for which we collect information not be specified in this clause, the purpose will be communicated to you in writing and agreed to in our interactions with data subjects which might include varied and different parties.

5.2 Consent

Any information that we collect from data subjects will be with consent. The rule of thumb is if the business is collecting information from any person whether natural or legal it must obtain a signed Consent Form. Consent may be obtained from data subjects during introductory meetings, application forms, electronic media or ongoing interaction. It might also be via online website cookies or any other form of valid consent.

Where data subjects provide us with information, the need to do so willingly and voluntarily with the understanding that we require the information to pursue both our clients' legitimate interests as well as our own.

To carry on business and to protect or facilitate data subject interests, we require personal information from time to time and will treat it with utmost confidentiality. should a data subject at any time during the processing of their information object to same, they may withdraw consent by furnishing us with reasonable notice and in the prescribed form attached.

5.3 Information we Require

The Responsible Party collects different categories of information from data subjects depending on their needs and our agreements with them. We do not collect information that is unnecessary or irrelevant for the purpose specified. We strive to collect only the information that is necessary for us to deliver our service.

Please bear in mind that this is not an exhaustive list and we may at times require information that is not contained herein. We will inform data subjects as to the information we collect from them whenever practicable, whether such information is voluntary or mandatory, and what the consequences are if information (whether voluntary or mandatory) is not provided. Usually, if the information requested is not provided, we can only offer a limited service or no service at all.

5.4 Access to and Integrity of Information

The Responsible Party is committed to maintaining the integrity and accuracy of data subject information. To this extent, data subjects are reminded via consent forms that they may request access to their own information at any time and to request that we update or correct any information that may be outdated or incorrect.

We take reasonable and routine steps to ensure that the information we collect is up to date and accurate. Where information does not need to be updated to fulfil the purpose for which it was collected, such information will not be updated without the client's express request.

5.5 Security of Information and Regular Monitoring

The safety and confidentiality of Data Subject information is of paramount importance to The Responsible Party and its staff. To this extent, The Responsible Party is committed to preventing unauthorized access, damage, loss of or destruction of personal information by ensuring that industry-appropriate and adequate security measures are implemented and persistently reviewed.

The company maintains strict security and confidentiality measures for both physical and electronic health records. The processing of health information is subject to a strict duty of confidentiality and outline procedures for the secure, permanent disposal of these specific records.

We do our best to identify risks both internally and externally, and to adapt accordingly we implement security systems with due regard to generally accepted information security practices.

5.6 Holding Periods

Information we collect on data subjects will not be held for longer than necessary, or if the purpose for which said information was collected has ultimately been fulfilled, or if the collected information has become obsolete.

Where no agreements, other laws or terms in this policy apply, a record of personal information will be kept for one year after the information was finished being processed, including usage for the specific purpose for which the information was collected originally.

We will destroy Records of Personal Information as soon as reasonably practicable, unless further retention is required by the laws mentioned above or agreed to between the parties.

For more information on durations of specific records, please refer to Annexure A to view our Record Retainment Policy.

5.7 Information Erasure

The Responsible Party will endeavour that information be destroyed, where reasonable, after its retention period has lapsed as set out in Annexure A.

Data Subjects have the right to obtain the erasure of their personal data without an undue delay if:

- the information is no longer necessary for the specified purpose it was collected for; or
- where the data subject withdraws consent in terms of this policy; or
- the collected personal information is inaccurate, irrelevant, excessive or incomplete.

If data subjects prefer for The Responsible Party to cease processing their information instead of deleting it, reasonable notice may be given to this effect following which we will immediately stop processing your information.

Notice in terms of erasure must be provided in the prescribed format of forms attached to this policy.

5.8 Direct Marketing

We will never process personal information for the purpose of direct marketing (or spam) unless Data Subjects:

- have consented to such processing; or
- had not previously refused consent; and if
- contact details were obtained in the context of providing them with our services; and if
- they were given reasonable opportunity to object to the direct marketing; or
- was already a data subject.

5.9 Employee Health Data

In addition to general personal information, The Responsible Party acknowledges its specific obligations as an employer regarding the processing of employee Health Information. We strictly limit the collection and processing of employee health data to what is legally mandated and practically necessary for employment and health and safety purposes.

The specific employee Health Information we may collect includes, but is not limited to:

- Sick notes and medical certificates.

- Occupational health and safety records.
- Medical scheme or health insurance details.

This information is collected and processed solely for the following justifiable purposes:

- Fulfilling statutory and contractual leave requirements (such as administering sick leave).
- Facilitating emergency medical procedures and ensuring workplace safety.
- Administering employee benefits related to healthcare.

All employee Health Information is treated as highly confidential, subject to the strict security measures and permanent disposal procedures outlined in Section 5.5 of this policy.

6. Security measures regarding an operator or person acting under authority

6.1 Disclosure of Information

The Responsible Party staff are regularly reminded that they have a confidentiality obligation towards data subjects who hold a Right to Privacy under the Constitution, and neither The Responsible Party nor its staff will disclose data subject information to a third party unless:

- we are required to do so by law; or
- the disclosure is necessary to enable us to perform our functions as per our clients' mandates; or
- it is vital to protecting the rights of the Responsible Party

6.2 Authority

In the event that information is to be disclosed to a third party, The Responsible Party will ensure that the third party receiving personal information is as committed to protecting your privacy and information as we are. We do this via obtaining a commitment form from the third party in written form where the third party agrees to keep information confidential and maintains security measures.

7. Data Breach Management

A Data Breach incident is an event that has caused or can potentially cause damage to our organisation's assets, reputation and / or personnel which includes our customers and any other personal information we process, store or share. A Data Breach can occur when there is intrusion, compromise and misuse of information by a party that does not have lawful access rights to the information that was compromised.

An Information Security Incident includes, but is not restricted to, the following;

- The illegitimate use of our systems for the processing, storage or sharing of data by any person.
- The transfer of personal information to persons who are not entitled to receive that information.
- The loss or theft of personal and/or classified data and information via any means, for example hacking or even attempted hacking.
- Unauthorised changes to personal information via our system hardware or software.

- Unauthorised disruption or denial of service to our system.

Where there are reasonable grounds to suspect that the personal information of a data subject has been breached (accessed, acquired, deleted or damaged by an unauthorised third party), we will:

- notify the data subject of such a breach in detail, as well as
- inform the information regulator as soon as reasonably possible after the breach is discovered.

Data breach communication to the data subject can be done in one of the following methods:

- Mailed to the data subject's last known physical or postal address;
- Sent by e-mail to the data subject's last known e-mail address;
- Placed in a prominent position on the website of the responsible party;
- Published in the news media; or
- As may be directed by the Regulator.

The communication must include enough information so that the data subject can take protective measures and should include:

- A description of the possible consequences of the breach;
- A description of the measures that the responsible party intends to take or has taken to address the security breach;
- A recommendation with regard to the measures to be taken by the data subject
- To mitigate the possible adverse effects of the breach; and
- If known to the responsible party, the identity of the unauthorised person who may have accessed or acquired the personal information.

Any data breaches experienced by Third Party Operators must be reported to the Responsible Party.

8. Prohibited Data Processing and Exemptions

Due to the nature of our business we may from time to time obtain data that is prohibited to enable us to offer our services and to comply with the laws applicable to our business. As such we aim to make use of the exemptions that the POPI Act provides in instances where the information is needed. We obtain consent for this personal information and may include but not be limited to:

- The religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, sex life or biometric information of a data subject (Note: Exemptions for Health Information are governed specifically by our internal safeguards and the 2026 Health Information Regulations as outlined in Sections 5.5 and 5.9) ; or
- The criminal behaviour of a data subject to the extent that such information relates to-
    - The alleged commission by a data subject of any offence; or
    - Any proceedings in respect of any offence allegedly committed by a data subject or the disposal of such proceedings.
- Personal information concerning a child.

9. Information Officer

The Responsible Party's Information Officer is responsible for:

- Ensuring information policies are reviewed, monitored, up to date and sufficient;
- Ensuring an Impact Assessment is done
- Ensuring the PAIA Manual is developed, monitored, maintained and available as prescribed (if applicable)
- Handling complaints or requests made in terms of this policy;
- Supporting this policy with relevant documentation;
- Ensuring POPI training or awareness is conducted;
- Backing up data;
- Reporting incidents and allocating security responsibilities; and
- Any other relevant information-related duty or responsibility.

The Responsible Party's Information Officer is Kirsty Bezuidenhout, with Contact Number: 010 045 2023, and E-Mail Address: kirsty@mbfs.co.za.

10. Personal Information Transfers outside South Africa

10.1 General International Transfers and Cloud technology

Due to the pervasive and widespread use of cloud technology and the disappearance of national borders in the broader context of the digital age we live in it is accepted that Personal Information of Data Subjects will almost always be transferred internationally. It is not always possible to pinpoint exactly in which country the cloud service is hosted as this may change from time to time as data centres operate internationally in several countries. It may well be the case that Personal Information is transferred to multiple countries.

The use of these services are required to be able to operate as a business, to stay competitive and to keep up to date with new digital technological innovation. We also require the use of these services to be able to provide clients with our services.

For all Data Subjects we obtain consent to transfer their information across borders and this is to be done before we do so.

10.2 Specific Restrictions on Health Information

Notwithstanding the general provisions above, the transfer of Health Information to a third party in a foreign country is subject to heightened restriction. Mont Blanc Financial Services strictly prohibits the transfer of Health Information across borders (including storage via international cloud providers) unless the requirements of **Section 72(1) of POPIA** are fully satisfied.

Specifically, Health Information will only be transferred if:

- The recipient is subject to a law, binding corporate rules, or a binding agreement which provides an **adequate level of protection** substantially similar to the conditions for lawful processing as set out in POPIA; or
- The Data Subject explicitly consents to the transfer; or
- The transfer is necessary for the performance of a contract between the Data Subject and Mont Blanc Financial Services.

We will conduct due diligence to ensure that any cloud provider or third party handling Health Information is legally bound by data protection standards that meet these criteria.

10.3 Platforms and Reasons for Transfer

The reasons or platforms we use to transfer Personal Information across borders are:

- Cloud services for data file storage such as Dropbox, OneDrive etc.
- Cloud server services for email.
- Newsletter service providers.
- Proprietary software services and client CRM

11. Prescribed Forms Relating to the Processing of Personal Information

For Data Subjects to exercise their rights in terms of their information we need to abide by the law. In this context there are certain prescribed forms by POPI to be used when interacting with data subjects. Please see attached the forms for general use.

Form 1- Objection to the processing of personal information

Form 2 - Request for correction or deletion of personal information or destruction or deletion of record of personal information

Form 4 - Request for data subject's consent to process personal information for Direct Marketing

12. POPI Awareness

The responsible Party conducts POPI awareness sessions with all staff or other consultants or contractors via awareness sessions. All previously mentioned persons will be required to have completed the POPI awareness training.

From time to time more in-depth POPI awareness sessions may be held with the Information Officers and Deputy Information Officers.