MFS | MANAGEMENT FINANCIAL SERVICES

TAX | ACCOUNTING | PAYROLL

Data Protection Policy

Introduction

MFS Management Financial Services CC, herein known as MFS, is an Accounting Services Firm that provides accounting, tax and payroll advice and services to its clients.

MFS acknowledges that our clients, suppliers, and our employees care about how their personal information is used and shared. This policy describes the types of personal information that we may collect, the purposes for which we use the information, the circumstances in which we may share the information, and the steps that we take to safeguard the information and privacy of those persons and entities we deal with.

Rationale

This policy stipulates MFS's commitment to ensuring that any personal data which MFS processes, is carried out in compliance with The Protection of Personal Information Act 4 of 2013 (or POPIA Act).

Scope

This policy applies to all personal data processed by MFS and is part of MFS's approach to comply with data protection law. All MFS employees are expected to comply with this policy and failure to comply may lead to disciplinary action for misconduct, or dismissal.

Personal Information

The information we collect may include, but is not limited to, the following:

Employees and payroll - Banking details, identity documents, personal contact details, client's employee's details and salary details.

Clients - Banking details, identity documents, FICA documents, proof of address, personal contact information, company information, SARS required information, tax certificates, CIPC required information, payroll details, bank statements, invoices, credit notes, quotes and supporting documents as well as access to clients accounting systems.

Personal information about children

We do not knowingly collect personal information from children (under 18 years of age) without the permission of their parent or guardian.

Method of data collection

We collect personal information directly from the client by way of face-to-face meetings, telephone conversations, emails, use of drop box, client memory sticks, manual file drop offs and from third parties for example private bankers etc.

What do we do with personal information collected from you?

Our small staff team has access to all client information provided to us and we use all personal information collected in order to provide accounting, tax and payroll services to our clients.

If you apply for employment with us, we use the personal information you supply to process your job application, draw up the employee contracts and for payroll purposes. Only MFS members have access to this data.

Other than what is set out in this privacy policy, we will not share your personal information unless we are required to do so by law.

Protection of the Company and others

We will only release personal information when we believe that such a release is appropriate to comply with the law; enforce or apply our mandate or other agreements; or protect the rights, property, or safety of the Company. This includes exchanging information with other companies and organizations for fraud protection and credit risk reduction. However, this does not include selling, sharing, or otherwise disclosing personally identifiable information from insured persons, or entities for commercial purposes in a way that is contrary to the commitments made in this privacy policy.

With the consent of the relevant party, and other than as set out above, such party will receive notice when information about them might go to third parties, and you will have an opportunity to choose not to share the information.

How secure is the information held by us?

We maintain appropriate physical, electronic and procedural safeguards in connection with the collection, storage, and disclosure of personally identifiable information.

Some of the physical safeguards implemented by MFS include but are not limited to the following:

- All hard copies of information are kept in our locked and access-controlled premises, which have been fitted with burglar guards, trellidoors and alarm systems;
- Only limited employees have keys to the office and each person has their own alarm code. On entry and exit of the office, the main member is sent a SMS detailing which employee accessed the offices and at what times;
- Only management and members know the challenge code to the alarm system;
- Our computer server room is locked at all times and can only be accessed by the main member and the designated IT consultant;
- Our file archive room remains locked at all times on our premises, with only one employee having the key to access this room. A list of all information in archives is kept and constantly updated;
- Each employee has their own lockable filing cabinet;
- We have a "clean desk" policy in place with all employees;
- All hard copy data returned to our clients is to be signed out by the client as proof of receipt;
- There is only one designated member who receives drop box files and retrieves data off of client's memory sticks;
- On the odd occasion employees need to remove a client's hard copy file from the office, a register is kept, and all employees are required to sign the information in and out of the office.

Some of the electronic safeguards implemented by MFS include but are not limited to the following:

- Our server has multiple fire walls, as well as ESET Anti-virus software;
- MFS makes use of Microsoft 365, which is only available for use in the office, thus no one has access to global email passwords and therefore emails cannot be accessed from any other devices;
- Each employee has their own username and password to access his/her computer and the company system;
- Each clients accounting files are password protected;
- Due to Covid, remote access has been given to certain employees, which allows them to access their work stations remotely. This is controlled via a password protected VPN access and each employee can only access their own work station;
- Only members have the WIFI password.
- Backups of all our information are run daily and stored on external hard drives. Weekly offsite backups are also kept.

MFS ensures that good data protection practice is imbedded in the culture of our employees and our organization. Each MFS employee is required to sign our Electronic Communications and Information Security Policy as well as our Confidential Information Agreement on start of their employment. When an MFS employee leaves, all physical and electronic access is terminated immediately, and their email addresses are deleted within one month.

Storage of data

We retain your personal data only for the period necessary for the purposes set out in this policy, or in accordance with the provisions of any applicable legislation.

As specified by SARS, all client information is kept in our archives for a period of 10 years. Thereafter, the client is given the option to collect their information, otherwise this information is shredded and recycled.

Clients who are no longer clients of MFS are required to collect all their hard copy data and sign for it as proof of receipt.

Clients' details kept on file are updated as soon as we are made aware of any changes, otherwise every few years an email is sent to clients requesting them to reconfirm their details to ensure SARS and CIPC have our clients most up to date information.

Breach of Data

Should any breach of personal data occur, the incident is required to be reported immediately to the designated Information Officer, whereafter an incident report form is required to be completed.

If required, the client will be contacted by the Information Officer to inform them of any breach that may have occurred and the effects thereof. Steps to rectify the situation will also be put in to place as soon as possible and any incident will be treated as a top priority by MFS.

Designated Information Officer

MFS has appointed Gail Kimble as the designated Information Officer responsible for all data protection and monitoring.

What choices do I have?

You have the right to request a copy of the personal information we hold about you or to object to the processing of personal information held about you. You also have the right to ask us to update, correct or delete your personal information. To do this, contact our Information Officer and specify what information you would like and any changes to be made. We will take all reasonable steps to confirm your identity before providing details of your personal information, or before making changes to personal information we may hold about you. However, as we are a small firm and know most of our clients personally, we need not perform identity checks on those clients we have a relationship with and who request information from us directly.

Please note that we may amend this policy from time to time.

Notices and Revisions

If you have any concern about privacy at the Company, please e-mail us a thorough description and we will try to resolve the issue for you. Unless stated otherwise, our current privacy policy applies to all information that we have on record. However, we stand behind the promises we make and will never materially change our policies and practices to make them less protective of personal information collected in the past, without the consent of affected persons.

Questions, comments, and requests regarding this privacy policy are welcomed and should be addressed to the Information Officer.

Contact Details

Address:	70 Adelaide Tambo Drive, Durban North, KwaZulu Natal, 4051
Tel:	031 564 7812
Information Officer's email:	info@manfs.co.za
Website:	www.manfs.co.za

Monitoring and review

This policy was last updated on the 17th of June 2021 and shall be regularly monitored and reviewed, at least every third year.

Other data policies in place at MFS

- Electronic Communications and Information Security Policy
- Confidential Information Agreement