Date: 25/10/2021
Revision No: 00

fischer
South Africa

POPIA Privacy Policy

1 Jakaranda Street
Hennopspark Ext. 7 | P.O. Box 7466
Centurion 0046 | South Africa

Phone +27 87 148 4960
fischer@fischersa.com
www.fischersa.com

Directors:
Hans-Peter Fischer (German)
E.H.G. Kotzenmacher (Austrian)
M.E. Kotzemacher (Managing)

Date: 25/10/2021
Revision No: 00

FISCHER SOUTH AFRICA
(Hereinafter referred to as "The Company")

Comprising of:
fischer Stainless Steel Tubing S.A. (Pty) Ltd.
fischer Tube E.C. (Pty) Ltd.
fischer Tube Technik (Pty) Ltd.
fischer South Africa Facilities (Pty) Ltd.

POPIA PRIVACY POLICY

FOREWORD

Policies and procedures are cornerstones for success in any organization. They guide implementation as well as set the parameters and standards for corporate ethics; they stimulate productivity by eliminating uncertainty as well as ensuring predictability. Without a policy, upon which to base standards and procedures, decisions are likely to be inconsistent and security lapses will be present and able to be exploited by both internal and external persons. The threat posed by the lack of consistency in a policy by an institution, carries unbearable consequences.

All concerned employees, volunteers, contractors, suppliers, and any other persons acting on behalf of the organisation are to familiarize themselves with the contents of this document. Employees are, as an integral part of their employment contracts, governed by this policy in line with The Company's corporate values and other relevant codes of conduct.

The content of this policy is binding on all employees. Non-compliance of this policy is subject to disciplinary procedures, which could result in a warning, immediate dismissal, or even civil/criminal lawsuits.

1 Jakaranda Street
Hennopspark Ext. 7 | P.O. Box 7466
Centurion 0046 | South Africa

Phone +27 87 148 4960
fischer@fischersa.com
www.fischersa.com

Directors:
Hans-Peter Fischer (German)
E.H.G. Kotzenmacher (Austrian)
M.E. Kotzemacher (Managing)

fischer South Africa

TABLE OF CONTENTS

1 Jakaranda Street
Hennopspark Ext. 7 | P.O. Box 7466
Centurion 0046 | South Africa

Phone +27 87 148 4960
fischer@fischersa.com
www.fischersa.com

Directors:
Hans-Peter Fischer (German)
E.H.G. Kotzenmacher (Austrian)
M.E. Kotzemacher (Managing)

1. INTRODUCTION

- The right to privacy is an integral human right recognized and protected in the South African Constitution and in the Protection of Personal Information Act 4 of 2013 ("POPIA").

- POPIA aims to promote the protection of privacy through providing guiding principles that are intended to be applied to the processing of personal information in a context-sensitive manner.

- Through the provision of quality goods and services, the Company is necessarily involved in the collection, use and disclosure of certain aspects of the personal information of clients, customers, employees, and other stakeholders.

- A person's right to privacy entails having control over his or her personal information and being able to conduct his or her affairs relatively free from unwanted intrusions.

- Given the importance of privacy, the Company is committed to effectively managing personal information in accordance with POPIA's provisions.

2. DEFINITIONS

2.1 Personal Information

- Personal information is any information that can be used to reveal a person's identity.

- Personal information relates to an identifiable, living, natural person or, where applicable, an identifiable existing juristic person.

- Personal information does not include information that does not identify you (including in instances where that information has been de-identified so that it does not identify a person).

- The personal information that we collect about you may differ on the basis of your engagement with us or the products and/or services that you receive from or provide to us.

2.2 Special personal information

- Special personal information refers to details about your religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric information or information about your criminal offences or convictions.

- The processing of Special Personal Information requires higher levels of protection. We need to have further justifications for processing Special Personal Information. We implemented appropriate policies and safeguards, which we are required by law to maintain, to process Special Personal Information.

2.3 Data Subject

- This refers to the natural or juristic person to whom personal information relates, such as an individual client, customer or a company that supplies the Company with products or other goods.

2.4 Responsible Party

- The responsible party is the entity that needs the personal information for a particular reason and determines the purpose of and means for processing the personal information. In this case, the Company is the responsible party.

2.5 Operator

- An operator means a person who processes personal information for a responsible party in terms of a contract or mandate, without coming under the direct authority of that party. For example, a third-party service provider that has contracted with the Company to shred documents containing personal information. When dealing with an operator, it is considered good practice for a responsible party to include an indemnity clause.

2.6 Information Officer

- The Information Officer is responsible for ensuring the Company's compliance with POPIA.

- Where no Information Officer is appointed, the head of the Company will be responsible for performing the Information Officer's duties.

- Once appointed, the Information Officer must be registered with the South African Information Regulator established under POPIA prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.

2.7 Processing

- The act of processing information includes any activity or any set of operations, whether or not by automatic means, concerning personal information and includes:

    - the collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
    - dissemination by means of transmission, distribution or making available in any other form; or
    - merging, linking, as well as any restriction, degradation, erasure, or destruction of information.

2.8 Record

- Means any recorded information, regardless of form or medium, including:

    - Writing on any material;
    - Information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored;
    - Label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means;
    - Book, map, plan, graph, or drawing;
    - Photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced.

2.9 Filing System

- Means any structured set of personal information, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria.

2.10 Unique Identifier

- Means any identifier that is assigned to a data subject and is used by a responsible party for the purposes of the operations of that responsible party and that uniquely identifies that data subject in relation to that responsible party.

2.11 De-Identify

- This means to delete any information that identifies a data subject, or which can be used by a reasonably foreseeable method to identify, or when linked to other information, that identifies the data subject.

2.12 Re-Identify

- In relation to personal information of a data subject, means to resurrect any information that has been de-identified that identifies the data subject, or can be used or manipulated by a reasonably foreseeable method to identify the data subject.

2.13 Consent

- Means any voluntary, specific, and informed expression of will in terms of which permission is given for the processing of personal information.

2.14 Direct Marketing

- Means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
-
    - Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
    - Requesting the data subject to make a donation of any kind for any reason.

2.15 Biometrics

- Means a technique of personal identification that is based on physical, physiological, or behavioural characterisation including blood typing, fingerprinting, DNA analysis, retinal scanning, and voice recognition.

3. POLICY PURPOSE

- The purpose of this policy is to protect the organisation from the compliance risks associated with the protection of personal information which includes:

    - Breaches of confidentiality. For instance, the organisation could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
    - Failing to offer choice. For instance, all data subjects should be free to choose how and for what purpose the organisation uses information relating to them.
    - Reputational damage. For instance, the organisation could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by the organisation.

- This policy demonstrates the Company's commitment to protecting the privacy rights of data subjects in the following manner:

    - Through stating desired behaviour and directing compliance with the provisions of POPIA and best practice.
    - By cultivating an organisational culture that recognises privacy as a valuable human right.
    - By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
    - By creating business practices that will provide reasonable assurance that the rights of data subjects are protected and balanced with the legitimate business needs of the organisation.
    - By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information Officers in order to protect the interests of the organisation and data subjects.
    - By raising awareness through training and providing guidance to individuals who process personal information so that they can act confidently and consistently.

4. POLICY APPLICATION

- This Privacy Policy applies to the processing by us or on our behalf, and our successors-in-title, of the Personal Information relating to you, being a user who accesses and/or uses our website or our products and services, or a provider of products and services to us, clients, suppliers, former employees, prospective employees, and other data subjects that engage with us.

- This Privacy Policy applies regardless of the device which you use to access our website (*if any)* or to engage with us, which device is capable of using, or enabled to use, the Website including, but not limited to, internet-connected mobile devices and tablets ("**Access Device**").

- This Privacy Policy does not apply to the processing of Personal Information by other third parties relating to or by means of other parties' websites, products, or services, such as websites linked to, from or advertised on the Website or through our products and services, or sites which link to or advertise the Website or our products and services.

5. TYPES OF PERSONAL INFORMATION

- We may process various types of Personal Information about you, as follows:

    - **Identity Information**, which includes information concerning your name, username or similar identifier, marital status, title, occupation, interests, date of birth, gender, race, and legal status, as well as copies of your identity documents, photographs, identity number, registration number and your qualifications.
    - **Contact Information**, which includes your billing addresses, delivery addresses, e-mail addresses and telephone numbers;
    - **Financial Information**, which includes bank account details; details of funds which we invest and hold on your behalf for a matter, insurance information, financial statements, tax clearance certificates and VAT registration numbers.
    - **Transaction Information**, which includes details about payments made to or received from you and company information, which may consist of financial activity;
    - **Technical Information**, which includes your internet protocol (IP) address, your login data, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform, and other technology on the devices you use to access the Website or to use our products and services or engage with us;
    - **Usage Information**, which includes information as to your access to and use of the Website, products, and services, such as what links you went to, what content you accessed, the amount of content viewed and the order of that content, as well as the amount of time spent on the specific content and what products and services you access and use when engaging with us;
    - **Location Information**, which includes geographical information from your Access Device (which is usually based on the GPS or IP location); and
    - **Marketing and Communications Information**, which includes your preferences in respect of receiving marketing information from us and our third parties, and your communication preferences.

- We may also process, collect, store and/or use aggregated data, which may include historical or statistical data ("**Aggregated Data**") for any purpose, including for know-how and research purposes.

- Aggregated Data may be derived from your Personal Information but is not always considered Personal Information, as this data does not directly or indirectly reveal your identity. However, if we combine or connect Aggregated Data with your Personal Information in a manner that has the result that it can directly or indirectly identify you, we will treat the combined data as Personal Information, which will be managed in accordance with this Privacy Policy.

6. WHEN WILL WE PROCESS SPECIAL PERSONAL INFORMATION?

- We will generally not process particularly Special Personal Information about you unless it is necessary for establishing, exercising, or defending a right or obligation in law, or where we have obtained your consent to do so.

- On rare occasions, there may be other reasons for processing your Special Personal Information, such as where the information has been deliberately made public by you.

- The situations in which we may process your Special Personal Information include the following:

    - racial and ethnic information may be processed by us through CCTV cameras installed at our premises for safety and security reasons;
    - as part of the recruitment and hiring process, we may process information relating to your criminal behaviour;
    - we may process information pertaining to your political persuasion as part of the know your client (KYC) processes and customer due diligence (CDD) checks;
    - we may process information relating to your health as part of our screening processes when accessing our premises, in order to comply with Covid-19 regulations and protocols; and
    - we may process information which indicates your religious beliefs (for example, when you attend events organised by us, we may ask you for your dietary requirements, and this may indicate your religious beliefs).

7. HOW WE COLLECT YOUR PERSONAL INFORMATION

- We collect your Personal Information in the following ways:

    - through direct or active interactions with you;
    - through automated or passive interactions with you;
    - from third parties and public sources; and
    - CCTV *(where applicable)*.

- **Direct or active collection from you**

- We may require that you submit certain information:

    - to enable you to access portions of the Website;
    - to subscribe to our publications;
    - to request marketing or information about our events to be sent to you;
    - to apply for job opportunities;
    - to make contact with our partners, directors, managers, and employees;
    - to grant you access to our premises;
    - to enable you to facilitate the conclusion of an agreement with us; and
    - that is necessary for our fulfilment of our statutory or regulatory obligations.

- We also collect Personal Information directly from you when you communicate directly with us, for example when you complete certain application forms, via e-mail, telephone calls, feedback forms, giving us your business card, site comments or forums.

- If you contact us, we reserve the right to retain a record of that correspondence in accordance with applicable data protection legislation, which may include Personal Information.

- The Personal Information that we actively collect from you may include any of the Personal Information listed in this Privacy Policy and, in some instances, certain Special Personal Information listed in this Privacy Policy.

- **Passive collection from your Access Device when browsing our website**

- We may passively collect certain of your Personal Information from the Access Device that you use to access and navigate the Website, by way of various technological applications, for instance, using server logs to collect and maintain log information.

- We may also use cookies and anonymous identifiers which enable our computer system to recognise you when you next visit the Website to distinguish you from other users and to improve our service to you, and which can be used to enhance the content of the Website and make it more user-friendly, as well as to give you a more personalised experience.

- A cookie is a small piece of data (an alphanumeric identifier) which our computer system transfers to your Access Device through your web browser when you visit the Website, and which is stored in your web browser. When you visit the Website again, the cookie allows the site to recognise your browser. Cookies may store user preferences and other information.

- You may disable the use of cookies by configuring your browser to refuse all cookies or to indicate when a cookie is being sent. However, please note that some parts of the Website will not function properly if you refuse cookies, and you may not be able to enjoy all of the features and functionality of the Website.

- The Personal Information that we passively collect from your Access Device may include your Identity Information, your Contact Information, your Technical Information, your Profile Information, your Usage Information, your Location Information and your Marketing and Communications Information, or any other Personal Information which you permit us, from time to time, to passively collect from your Access Device.

- **Collection from third parties and public sources**

- We may receive Personal Information and Special Personal Information about you from various third parties, including recruitment agencies, suppliers of background checks services and publicly available sources.

- **CCTV**

- We may collect Personal Information and Special Personal Information about you through CCTV cameras installed at our premises for safety and security reasons.

8. HOW WE USE YOUR PERSONAL INFORMATION

- We use your Personal Information for the following purposes:
    - to comply with our regulatory reporting obligations;
    - to comply with our statutory obligations, including screening clients and visitors' health when accessing our premises to comply with Covid-19 regulations and protocols;
    - to conduct the recruitment and hiring processes, which includes conducting criminal record and credit checks (where appropriate), the capturing of a job applicant's details and providing status updates to job applicants;
    - in relation to supplier information, to create supplier profiles on our systems, pay suppliers, and for general supplier administration;
    - to maintain and improve the Website and to improve the experience of our website users, including by requesting feedback from our website users on our products and services and to facilitate the procurement of our products and services.
    - to retain and make information available to you on the Website;
    - to maintain and update our client, or potential client databases;
    - to maintain and update our supplier database;
    - to establish and verify your identity on the Website;

- to operate, administer, secure, and develop the Website and the performance and functionality of the Website;
- to detect, prevent or manage actual or alleged fraud, security breaches or the abuse, misuse or unauthorised use of our systems and files, the Website and/or contraventions of this Privacy Policy and/or the Terms and/or the Agreements;
- to inform you about any changes to the Website, this Privacy Policy or other changes that are relevant to you;
- to create user profiles, compile and use statistical information (including non-personal information) about you and other users and their access to the Website and to analyse and compare how you and other users make use of the Website, including (without limitation) their browsing habits, click-patterns, preferences, frequency and times of use, trends and demographic information including recommendations to users and tailoring information and content for users;
- to conduct market research surveys;
- to offer you information and content which is more appropriately tailored for you as far as reasonably possible;
- to provide you with the latest information about our products and services or events provided that you have agreed to receive such information;
- for security, administrative and legal purposes;
- for client relations purposes, which may include storage of clients' marital status and birthdates;
- pitching, opportunity tracking and reporting;
- campaign tracking and reporting;
- to communicate with you and retain a record of our communications with you and your communications with us;
- to fulfil any contractual obligations that we may have to you or any third party;
- to analyse and compare the types of Access Devices that you and other users make use of and your physical location; and
- for other activities and/or purposes which are lawful, reasonable, and adequate, relevant, and not excessive in relation to the provision of our services and/or the use of the Website, our business activities, or such other purpose for which it was collected.

- We will obtain your permission before collecting or using your Personal Information and/or Special Personal Information for any other purpose.

9. COMPULSORY PERSONAL INFORMATION AND CONSEQUENCES OF NOT SHARING IT WITH US

- The following information is compulsory Personal Information:
    - your name and surname;
    - your contact details, such as your email address and/or your telephone number.
- Depending on the nature of your engagement or relationship with us, other types of Personal Information may be necessary, including:
    - financial (including bank account details, tax information);
    - names and registration numbers as contained in documents issued by the Companies and Intellectual Property Commission and the South African Revenue Service; and
    - information which may be necessary to ensure our compliance with the Financial Intelligence Centre Act, 38 of 2001.
- All other Personal Information is optional. If you do not agree to share the above-mentioned compulsory Personal Information with us, then you might not be able to engage with us fully, be paid for your products and services or receive complete and accurate products and services from us or enjoy all the features and functionality on the Website, including certain content and products and services.

10. SHARING OF YOUR PERSONAL INFORMATION

- We will not intentionally disclose your Personal Information, whether for commercial gain or otherwise, other than with your permission, as permitted by applicable law or in the manner as set out in this Privacy Policy.
- You agree and give permission for us to share your Personal Information under the following circumstances:
    - with our agents, advisers and suppliers that have agreed to be bound by applicable data protection legislation and this Privacy Policy or similar terms, which offer the same level of protection as this Privacy Policy;

- with our employees, suppliers, consultants, contractors and agents if and to the extent that they require such Personal Information in order to process it for us and/or in the provision of services for or to us, which include know-how and research, pitching to other clients to obtain further instructions; reporting purposes (e.g. the South African Revenue Service); hosting, development and administration, technical support and other support services relating to the Website or the operation of our business. We will authorize any Personal Information processing done by a third party on our behalf, amongst other things by entering into written agreements with those third parties governing our relationship with them and containing confidentiality; non-disclosure and data protection provisions. Such persons may be disciplined, their contracts terminated, or other appropriate action taken if they fail to meet their obligations;
- to enable us to enforce or apply our Terms and/or any Agreement you have with us;
- to enable us to monitor web traffic: web servers serving the website automatically collect information about pages you visit. This information is used for internal review, to tailor information to individual visitors and for traffic audits;
- for statistics purposes: we may perform statistical analyses in order to measure interest in the various areas of the Website (for product development purposes);
- to protect our rights, property, or safety or that of our clients, employees, contractors, suppliers, agents and any other third party;
- with governmental agencies and other regulatory or self-regulatory bodies, if required to do so by law or when we reasonably believe that such action is necessary to:
    - comply with the law or with any legal process;
    - protect and defend the rights, property or safety of the company, or our clients, employees, contractors, suppliers, agents or any third party;
    - detect, prevent, or manage actual or alleged fraud, security breaches, technical issues, or the abuse, misuse, or unauthorized use of the Website and/or contraventions of this Privacy Policy; and/or
    - protect the rights, property, or safety of members of the public (if you provide false or deceptive information or misrepresent yourself, we may proactively disclose such information to the appropriate regulatory bodies and/or commercial entities).

- We will get your permission before disclosing your Personal Information to any third party for any other purpose, if we are required by law to do so.

11. STORAGE AND TRANSFER OF YOUR PERSONAL INFORMATION

- We store your Personal Information on:
    - our premises, in the form of hard copies;
    - the premises of third-party service providers such as document storage service providers;
    - our servers; or
    - on the servers of our third-party service providers, such as IT systems or hosting service providers.

- In the event of the scenarios contemplated in clauses above, we will ensure that we have entered into written agreements with those third-party service providers governing our relationship with them that require them to secure the integrity and confidentiality of Personal Information in their possession by taking appropriate, reasonable technical and organizational measures.

- From time to time, we and our service providers may need to transfer to and/or store your Personal Information on servers in a jurisdiction other than where it was collected (i.e. outside of South Africa) and we hereby notify you that such jurisdiction may not have comparable data protection legislation.

- If the location to which Personal Information is transferred and/or is stored does not have substantially similar laws to those of South Africa, which provide for the protection of Personal Information, we will take reasonably practicable steps, including the imposition of appropriate contractual terms to ensure that your Personal Information is adequately protected in that jurisdiction.

- Please contact us if you require further information as to the specific mechanisms used by us when transferring your Personal Information outside of South Africa or to a jurisdiction that is different to the one in which we collected your Personal Information.

12. SECURITY

- We take reasonable technical and organizational measures to secure the integrity of your Personal Information and using accepted technological standards to prevent unauthorized access to or disclosure of your Personal Information, and protect your Personal Information from misuse, loss, alteration, and destruction.

- We review our information collection, storage and processing practices, including physical security measures periodically, to ensure that we keep abreast of good practice.

- We also create a back-up of your information for operational, business continuity and safety purposes and we have a back-up disaster recovery program.

- Despite the above measures being taken when processing Personal Information and Special Personal Information, subject to the provisions of this clause, as far as the law allows, we will not be liable for any loss, claim and/or damage arising from any unauthorized access, disclosure, misuse, loss, alteration, or destruction of your Personal Information and/or Special Personal Information.

- We have implemented policies and procedures to address actual and suspected data breaches and undertakes to notify you and the relevant regulatory authorities of breaches in instances in which we are legally required to do so and within the period in which such notification is necessary.

- In this clause, you acknowledge that you know, and you accept that technology is not absolutely secure and there is a risk that your Personal Information and Special Personal Information will not be secure when processed by means of technology. We do not promise that we can keep your Personal Information and Special Personal Information completely secure. To the maximum extent permitted by law, you will not be able to take action against us if you suffer losses or damages in these circumstances.

13. RETENTION OF YOUR PERSONAL INFORMATION

- We may keep your Personal Information for as long as you continue to engage with us, provide services or products to us, access the Website and content and/or use our products and/or services or for as long as reasonably necessary or until you contact us and ask us to destroy it.

- Aside from clause 13.1 above and any other clause in this Privacy Policy, we may retain and process some or all of your Personal Information if and for as long as:

    - we are required or permitted by law, a code of conduct or a contract with you to do so;
    - we reasonably need it for lawful purposes related to the performance of our functions and activities;
    - we reasonably require it for evidentiary purposes; or
    - you agree to us retaining it for a specified further period.

- To determine the appropriate retention period for Personal Information, we will consider, among other things, the nature and sensitivity of the Personal Information, the potential risks or harm that may result from its unauthorized use or disclosure, the purposes for which we process it and whether those purposes may be achieved through other means. We will always comply with applicable legal, regulatory, tax, accounting, or other requirements as they pertain to the retention of Personal Information, as well as our Record Retention Policy.

14. MAINTENANCE OF YOUR PERSONAL INFORMATION

- Where required by law, we will take all reasonable steps to ensure that your Personal Information is accurate, complete, not misleading and up to date.

- We also acknowledge that you may have rights of access to, and the right to rectify, your Personal Information, and rights to object to the processing of your Personal Information in certain circumstances (clause 15 below contains further information about these rights).

- You must let us know if any of the Personal Information that we have about you is incorrect, incomplete, misleading, or out of date, by notifying us.

- Where required by law, we will take reasonable steps to correct or update your Personal Information, accordingly, having regard to the purpose for which such Personal Information was collected or used.

15. DESTRUCTION OF DOCUMENTS

- Documents may be destroyed after the termination of the retention period specified herein, or as determined by the Company from time to time.

- Each department is responsible for attending to the destruction of its documents and electronic records, which must be done on a regular basis. Files must be checked in order to make sure that they may be destroyed and to ascertain if there are important original documents in the file.

- Original documents must be returned to the holder thereof, failing which, they should be retained by the Company pending such return.

- The documents must made available for collection by the approved document disposal company.

- Deletion of electronic records must be done in consultation with the IT Department, to ensure that deleted information is incapable of being reconstructed and/or recovered.

16. RIGHTS OF DATA SUBJECTS

- Where appropriate, the organisation will ensure that its clients and customers are made aware of the rights conferred upon them as data subjects. The organisation will ensure that it gives effect to the following six rights.

- **The Right to Access Personal Information**

    - The Company recognizes that a data subject has the right to establish whether the organisation holds personal information related to him, her or it includes the right to request access to that personal information.
    - An example of a "Personal Information Request Form" can be found under Annexure A.

- **The Right to have Personal Information Corrected or Deleted**

    - The data subject has the right to request, where necessary, that his, her or its personal information must be corrected or deleted where the organisation is no longer authorised to retain the personal information.

- **The Right to Object to the Processing of Personal Information**

    - The data subject has the right, on reasonable grounds, to object to the processing of his, her or its personal information.
    - In such circumstances, the Company will give due consideration to the request and the requirements of POPIA. The organisation may cease to use or disclose the data subject's personal information and may, subject to any statutory and contractual record keeping requirements, also approve the destruction of the personal information.

- **The Right to Object to Direct Marketing**

    - The data subject has the right to object to the processing of his, her or its personal information for purposes of direct marketing by means of unsolicited electronic communications.

- **The Right to Complain to the Information Regulator**

    - The data subject has the right to submit a complaint to the Information Regulator regarding an alleged infringement of any of the rights protected under POPIA and to institute civil proceedings regarding the alleged non-compliance with the protection of his, her or its personal information.
    - An example of a "POPI Complaint Form" can be found under Annexure B.

- **<u>The Right to be Informed</u>**

    - The data subject has the right to be notified that his, her or its personal information is being collected by the Company.
    - The data subject also has the right to be notified in any situation where the organisation has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

17. GENERAL GUIDING PRINCIPLES

- All employees and persons acting on behalf of the Company will always be subject to, and act in accordance with, the following guiding principles:

- **<u>Accountability</u>**

    - Failing to comply with POPIA could potentially damage the Company's reputation or expose the organisation to a civil claim for damages. The protection of personal information is therefore everybody's responsibility.
    - The Company will ensure that the provisions of POPIA and the guiding principles outlined in this policy are complied with through the encouragement of desired behaviour. However, the organisation will take appropriate sanctions, which may include disciplinary action, against those individuals who through their intentional or negligent actions and/or omissions fail to comply with the principles and responsibilities outlined in this policy.

- **<u>Processing Limitation</u>**

    - The organisation will ensure that personal information under its control is processed:
        - In a fair, lawful and non-excessive manner, and
        - only with the informed consent of the data subject, and
        - only for a specifically defined purpose.
    - The organisation will inform the data subject of the reasons for collecting his, her or its personal information and obtain written consent prior to processing personal information.
    - Alternatively, where services or transactions are concluded over the telephone or electronic video feed, the organisation will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent.
    - The organisation will under no circumstances distribute or share personal information between separate legal entities, associated organisations (such as subsidiary companies) or with any individuals that are not directly involved with facilitating the purpose for which the information was originally collected.

- Where applicable, the data subject must be informed of the possibility that their personal information will be shared with other aspects of the Company's business and be provided with the reasons for doing so.
- An example of a "POPI Notice and Consent Form" can be found under Annexure C.

- **Purpose Specification**

  - All of the Company's business units and operations must be informed by the principle of transparency.
  - The organisation will process personal information only for specific, explicitly defined, and legitimate reasons. The organisation will inform data subjects of these reasons prior to collecting or recording the data subject's personal information.

- **Further Processing Limitation**

  - Personal information will not be processed for a secondary purpose unless that processing is compatible with the original purpose.
  - Therefore, where the organisation seeks to process personal information, it holds for a purpose other than the original purpose for which it was originally collected, and where this secondary purpose is not compatible with the original purpose, the organisation will first obtain additional consent from the data subject.

- **Information Quality**

  - The organisation will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading.
  - The more important it is that the personal information be accurate (for example, the beneficiary details of a life insurance policy are of the utmost importance), the greater the effort the organisation will put into ensuring its accuracy.
  - Where personal information is collected or received from third parties, the organisation will take reasonable steps to confirm that the information is correct by verifying the accuracy of the information directly with the data subject or by way of independent sources.

- **Open Communication**

  - The organisation will take reasonable steps to ensure that data subjects are notified (are at all times aware) that their personal information is being collected including the purpose for which it is being collected and processed.
  - The organisation will ensure that it establishes and maintains a “contact us” facility, for instance via its website or through an electronic helpdesk, for data subjects who want to:
    - Enquire whether the Company holds related personal information, or
    - Request access to related personal information, or
    - Request the Company to update or correct related personal information, or
    - Make a complaint concerning the processing of personal information.

- **Security Safeguards**

  - The organisation will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented in order to minimise the risk of loss, unauthorised access, disclosure, interference, modification, or destruction.
  - Security measures also need to be applied in a context-sensitive manner. For example, the more sensitive the personal information, such as medical information or credit card details, the greater the security required.
  - The organisation will continuously review its security controls which will include regular testing of protocols and measures put in place to combat cyber-attacks on the Company’s IT network.
  - The organisation will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.
  - All new employees will be required to sign employment contracts containing contractual terms for the use and storage of employee information. Confidentiality clauses will also be included to reduce the risk of unauthorised disclosures of personal information for which the organisation is responsible.
  - All existing employees will, after the required consultation process has been followed, be required to sign an addendum to their employment containing the relevant consent and confidentiality clauses.
  - The Company’s operators and third-party service providers will be required to enter into service level agreements with the organisation where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement.
  - An example of “Employee Consent and Confidentiality Clause” for inclusion in the Company’s employment contracts can be found under Annexure D.
  - An example of an “SLA Confidentiality Clause” for inclusion in the Company’s service level agreements can be found under Annexure E.

- **<u>Data Subject Participation</u>**

    - A data subject may request the correction or deletion of his, her or its personal information held by the organisation.
      The organisation will ensure that it provides a facility for data subjects who want to request the correction of deletion of their personal information.
      Where applicable, the organisation will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

18. INFORMATION OFFICER

- The Company will appoint an Information Officer and where necessary, a Deputy Information Officer to assist the Information Officer.

- The Company's Information Officer is responsible for ensuring compliance with POPIA.

- There are no legal requirements under POPIA for an organization to appoint an Information Officer. Appointing an Information Officer is however, considered to be a good business practice, particularly within larger organizations.

- Where no Information Officer is appointed, the head of the Company will assume the role of the Information Officer.

- Consideration will be given on an annual basis to the re-appointment or replacement of the Information Officer and the reappointment or replacement of any Deputy Information Officers.

- Once appointed, the Company will register the Information Officer with the South African Information Regulator established under POPIA prior to performing his or her duties.

19. REQUEST TO ACCESS PERSONAL INFORMATION PROCEDURE

- Data subjects have the right to:
    - Request what personal information the Company holds about them and why.
    - Request access to their personal information.
    - Be informed how to keep their personal information up to date.

- Access to information requests can be made by email, addressed to the Information Officer. The Information Officer will provide the data subject with a “Personal Information Request Form”.

- Once the completed form has been received, the Information Officer will verify the identity of the data subject prior to handing over any personal information. All requests will be processed and considered against the Company’s PAIA Policy.

- The Information Officer will process all requests within a reasonable time.

20. POPI COMPLAINTS PROCEDURE

- Data subjects have the right to complain in instances where any of their rights under POPIA have been infringed upon. The Company takes all complaints very seriously and will address all POPI related complaints in accordance with the following procedure:

- POPI complaints must be submitted to the Company in writing. Where so required, the Information Officer will provide the data subject with a “POPI Complaint Form”.

- Where the complaint has been received by any person other than the Information Officer, that person will ensure that the full details of the complaint reach the Information Officer within 1 working day.

- The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.

- The Information Officer will carefully consider the complaint and address the complainant’s concerns in an amicable manner.

- In considering the complaint, the Information Officer will endeavor to resolve the complaint in a fair manner and in accordance with the principles outlined in POPIA.

- The Information Officer must also determine whether the complaint relates to an error or breach of confidentiality that has occurred and which may have a wider impact on the Company's data subjects.

- Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorized person, the Information Officer will consult with the Company's governing body where after the affected data subjects and the Information Regulator will be informed of this breach.

- The Information Officer will revert to the complainant with a proposed solution with the option of escalating the complaint to the Company's governing body within 7 working days of receipt of the complaint. In all instances, the Company will provide reasons for any decisions taken and communicate any anticipated deviation from the specified timelines.

- The Information Officer's response to the data subject may comprise any of the following:

    - A suggested remedy for the complaint,
    - A dismissal of the complaint and the reasons as to why it was dismissed,
    - An apology (if applicable) and any disciplinary action that has been taken against any employees involved.

- Where the data subject is not satisfied with the Information Officer's suggested remedies, the data subject has the right to complain to the Information Regulator.

- The Information Officer will review the complaints process to assess the effectiveness of the procedure on a periodic basis and to improve the procedure where it is found wanting. The reason for any complaints will also be reviewed to ensure the avoidance of occurrences giving rise to POPI related complaints.

Date: 25/10/2021
Revision No: 00

ANNEXURE A: PERSONAL INFORMATION REQUEST FORM

PERSONAL INFORMATION REQUEST FORM

Please be aware that we may require you to provide proof of identification prior to processing your request.

There may also be a reasonable charge for providing copies of the information requested.

Please submit the completed form to the information Officer:	
Name	
Contact Number	
Email Address	

A. Of Data Subject	
Name & Surname	
Identity Number	
Postal Address	
Contact Number	
Email Address	

B. Request
I request the organisation to: (a) Inform me of whether it hold any of my personal information (b) Provide me with a record or description of my personal information (c) Correct or update my personal information (d) Destroy or delete a record of my personal information
C. Instructions
D. Signature Page
Signature
Date

1 Jakaranda Street
Hennopspark Ext. 7 | P.O. Box 7466
Centurion 0046 | South Africa

Phone +27 87 148 4960
fischer@fischersa.com
www.fischersa.com

Directors:
Hans-Peter Fischer (German)
E.H.G. Kotzenmacher (Austrian)
M.E. Kotzemacher (Managing)

Date: 25/10/2021
Revision No: 00

ANNEXURE B: POPI COMPLAINT FORM

POPI COMPLAINT FORM

We are committed to safeguarding your privacy and the confidentiality of your personal information and are bound by the Protection of Personal Information Act.

Please select your complaint to the Information Officer	
Name	
Contact Number	
Email Address	

Where we are unable to resolve your complaint, to your satisfaction you have the right to complaint to the Information Regulator.

A. Of Complainant	
Name & Surname	
Identity Number	
Postal Address	
Contact Number	
Email Address	
B. Details of Complaint	
C. Desired Outcome	
D. Signature Page	
Signature	
Date	

1 Jakaranda Street
Hennopspark Ext. 7 | P.O. Box 7466
Centurion 0046 | South Africa

Phone +27 87 148 4960
fischer@fischersa.com
www.fischersa.com

Directors:
Hans-Peter Fischer (German)
E.H.G. Kotzenmacher (Austrian)
M.E. Kotzemacher (Managing)

Date: 25/10/2021
Revision No: 00

ANNEXURE C: POPI NOTICE AND CONSENT FORM

We understand that your personal information is important to you and that you may be apprehensive about disclosing it. Your privacy is just as important to us, and we are committed to safeguarding and processing your information in a lawful manner.

We also want to make sure that you understand how and for what purpose we process your information. If for any reason you think that your information is not processed in a correct manner, or that your information is being used for a purpose other than that for what it was originally intended, you can contact our Information Officer.

You can request access to the information we hold about you at any time and if you think that we have outdated information, please request us to update or correct it.

Our Information Officer's Contact Details	
Name	
Contact Number	
Email Address	

Purpose for Processing your information.

We collect, hold, use and disclose your personal information mainly to provide you with access to the services and products that we provide. We will only process your information for a purpose you would reasonably expect, including:

- Providing you with advice, products and services that suit your needs as requested
- To verify your identity and to conduct credit reference searches
- To issue, administer and manage your insurance policies
- To process insurance claims and to take recovery action
- To notify you of new products or developments that may be of interest to you
- To confirm, verify and update your details
- To comply with any legal and regulatory requirements

Some of your information that we hold may include, your first and last name, email address, a home, postal or other physical address, other contact information, your title, birth date, gender, occupation, qualifications, past employment, residency status, your investments, assets, liabilities, insurance, income, expenditure, family history, medical information, and your banking details.

Consent to Disclose and Share your Information.

We may need to share your information to provide advice, reports, analyses, products, or services that you have requested. Where we share your information, we will take all precautions to ensure that the third party will treat your information with the same level of protection as required by us. Your information may be hosted on servers managed by a third-party service provider, which may be located outside of South Africa.

I hereby authorise and consent to the organisation sharing my personal information with the following persons:
Name & Surname
Signature
Date

1 Jakaranda Street
Hennopspark Ext. 7 | P.O. Box 7466
Centurion 0046 | South Africa

Phone +27 87 148 4960
fischer@fischersa.com
www.fischersa.com

Directors:
Hans-Peter Fischer (German)
E.H.G. Kotzenmacher (Austrian)
M.E. Kotzemacher (Managing)

Date: 25/10/2021
Revision No: 00

ANNEXURE D: EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

EMPLOYEE CONSENT AND CONFIDENTIALITY CLAUSE

- "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, color, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email 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 whether the information is recorded electronically or otherwise.

- "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time.

- The employer undertakes to process the PI of the employee only in accordance with the conditions of lawful processing as set out in terms of POPIA and in terms of the employer's relevant policy available to the employee on request and only to the extent that it is necessary to discharge its obligations and to perform its functions as an employer and within the framework of the employment relationship and as required by South African law.

- The employee acknowledges that the collection of his/her PI is both necessary and requisite as a legal obligation, which falls within the scope of execution of the legal functions and obligations of the employer. The employee therefore irrevocably and unconditionally agrees:

  - That he/she is notified of the purpose and reason for the collection and processing of his or her PI insofar as it relates to the employer's discharge of its obligations and to perform its functions as an employer.
  - That he/she consents and authorises the employer to undertake the collection, processing, and further processing of the employee's PI by the employer for the purposes of securing and further facilitating the employee's employment with the employer.
  - Without derogating from the generality of the aforestated, the employee consents to the employer's collection and processing of PI pursuant to any of the employer's Internet, Email, and Interception policies in place insofar as PI of the employee is contained in relevant electronic communications.
  - To make available to the employer all necessary PI required by the employer for the purpose of securing and further facilitating the employee's employment with the employer.
  - To absolve the employer from any liability in terms of POPIA for failing to obtain the employee's consent or to notify the employee of the reason for the processing of any of the employee's PI.
  - To the disclosure of his/her PI by the employer to any third party, where the employer has a legal or contractual duty to disclose such PI.
  - The employee further agrees to the disclosure of his/her PI for any reason enabling the employer to carry out or to comply with any business obligation the employer may have or to pursue a legitimate interest of the employer in order for the employer to perform its business on a day-to-day basis.
  - The employee authorises the employer to transfer his/her PI outside of the Republic of South Africa for any legitimate business purpose of the employer within the international community. The employer undertakes not to transfer or disclose his/her PI unless it is required for its legitimate business requirements and shall comply strictly with legislative stipulations in this regard.

- The employee acknowledges that during the performance of his/her services, he/she may gain access to and become acquainted with the personal information of certain clients, suppliers, and other employees. The employee will treat personal information as a confidential business asset and agrees to respect the privacy of clients, suppliers, and other employees.

- To the extent that he/she is exposed to or insofar as PI of other employees or third parties are disclosed to him/her, the employee hereby agree to be bound by appropriate and legally binding confidentiality and non-usage obligations in relation to the PI of third parties or employees.

- Employees may not directly or indirectly, utilize, disclose, or make public in any manner to any person or third party, either within the Company or externally, any personal information, unless such information is already publicly known, or the disclosure is necessary in order for the employee or person to perform his or her duties on behalf of the employer.

Date: 25/10/2021
Revision No: 00

ANNEXURE E: SLA CONFIDENTIALITY CLAUSE

SLA CONFIDENTIALITY CLAUSE
• "Personal Information" (PI) shall mean the race, gender, sex, pregnancy, marital status, national or ethnic origin, color, sexual orientation, age, physical or mental health, disability, religion, conscience, belief, culture, language and birth of a person; information relating to the education or the medical, financial, criminal or employment history of the person; any identifying number, symbol, email 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 whether the information is recorded electronically or otherwise. • "POPIA" shall mean the Protection of Personal Information Act 4 of 2013 as amended from time to time • The parties acknowledge that for the purposes of this agreement that the parties may come into contact with or have access to PI and other information that may be classified or deemed as private or confidential and for which the other party is responsible. Such PI may also be deemed or considered as private and confidential as it relates to any third party who may be directly or indirectly associated with this agreement. Further, it is acknowledged and agreed by the parties that they have the necessary consent to share or disclose the PI and that the information may have value. • The parties agree that they will always comply with POPIA's Regulations and Codes of Conduct and that it shall only collect, use, and process PI it comes into contact with pursuant to this agreement in a lawful manner, and only to the extend required to execute the services, or to provide the goods and to perform their respective obligations in terms of this agreement. • The parties agree that it shall put in place, and always maintain, appropriate physical, technological and contractual security measures to ensure the protection and confidentiality of PI that it, or its employees, its contractors or other authorized individuals comes into contact with pursuant to this agreement. • Unless so required by law, the parties agree that it shall not disclose any PI as defined in POPIA to any third party without the prior written consent of the other party, and notwithstanding anything to the contrary contained herein, shall any party in no manner whatsoever transfer any PI out of the Republic of South Africa.