



THE FANAKA FOUNDATION NPC

PRIVACY POLICY

DEFINITIONS

In this Policy (as defined below), unless the context requires otherwise, the following capitalised terms shall have the meanings given to them —

"Active Processing" means instances where the Company has directly been provided with the Personal Information/Personal Data of Data Subjects, such as when Data Subjects submit an enquiry in respect of our Services, or when Data Subjects provide Personal Information/Personal Data to the Company pursuant to concluding any commercial agreement(s) with the Company.

"Inactive Processing" means instances where the Company has not actively been provided with the Personal Information/Personal Data of Data Subjects, such as when the Company deploys Passive Processing Means to collect information from Data Subjects. These Passive Processing Means allow the Company to Process certain kinds of Non-personally Identifiable Information which can perhaps not be linked to Data Subjects.

"Anonymisation" means the Processing of Personal Information/Personal Data in such a manner that the Personal Information/Personal Data can no longer be attributed to Data Subjects without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the Personal Information/Personal Data are not attributed to Data Subjects.

"Applicable Laws" means any laws applicable to Personal Data and Personal Information and includes any statute, regulation, notice, policy, directive, ruling or subordinate legislation; the common law; any binding court order, judgement or ruling; any applicable industry code, policy or standard enforceable by law; or any applicable direction, policy or order that is given by any regulator, competent authority or organ of state or statutory industry body.

"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.

"Company" means the Fanaka Foundation NPC with registration number 2015/245688/08, a non-profit company registered in terms of the laws of the Republic of South Africa.



"Controller" means the Company, in circumstances where it Processes Personal Data (as defined in Article 4 of the GDPR).

"Consent" means any voluntary, specific and informed expression of will in terms of which permission is given for the Processing of Personal Information.

"Cookies" means small text files that store Non-personally Identifiable Information/Data about Data Subjects, either temporarily in connection with a Data Subjects Internet Protocol (IP) address (known as a temporary or session cookie, and deleted once a Data Subject closes their browser window) or more permanently on the hard drive of a Data Subject's device (known as a permanent or persistent cookie). The Company's Website(s) or Mobile Application(s) may from time to time use session cookies so that Data Subject's do not have to fill in the same information from page to page within our Website(s) or Mobile Application(s). If Data Subject's elect not to receive cookies, they may be able to view some, but not all, of the content on our Website(s) or Mobile Application(s).

"Member(s)" means a person who holds membership in, and specified rights in respect of the Company.

"Data Subject" means the Company's Member(s) or any Third Party in respect of whom the Company Processes Personal Information/Personal Data.

"Data Processing Infrastructure" means any and all systems, networks, servers, workstations, laptops, mobile devices, web applications, mobile applications, cloud storages, websites owned, controlled or operated by the Company.

"Embedded Scripts" means, programming code that is designed to collect information about a Data Subject's interactions with the relevant Website(s) or Mobile Application(s). It is temporarily downloaded onto a Data Subject's device from our web server or a Third-Party Operator. This program is active only while a Data Subject is connected to the relevant Website(s) or Mobile Application(s) and is deleted or deactivated thereafter.

"Electronic Means" means, in relation to the Processing of any Personal Information/Personal Data, the use of any Website(s), Mobile Application(s), electronic mail (email), text, voice, sound or image messages by the Company.

"Non-Electronic Means" means, in relation to the Processing of any Personal Information/Personal Data, the use of traditional means of Processing, such as hard copy documents, traditional filing systems deployed for the storage and retention of Personal Information/Personal Data and face-to-face personal engagements with Data Subjects.

"GDPR" means the General Data Protection Regulation, which is a European law that governs all collection and processing of personal data from individuals inside the European Union.



"Mobile Application(s)" means any multi-device software application, whether in web-based format or device-native format, to which this Privacy Policy relates and through which Member(s) and Third Parties gain access to the Company's Products and/or Services.

"Mobile Device Identifier" means device information if you access our Website(s) or Mobile Application(s) through mobile devices. Certain features of the relevant Website(s) or Mobile Application(s) may require collection of mobile phone numbers and we may associate that phone number with the mobile device identifiers. Additionally, some mobile phone service providers operate systems that pinpoint the physical location of devices that use their service. Depending on the provider, the Company and/or our Third-Party Operators may receive this information. If the Company associates any such passively collected information with the Personal Information/Personal Data of Data Subjects, we will treat the combined information as Personal Information/Personal Data as contemplated in this Policy.

"Non-personally Identifiable Information/Data" means any information/data which cannot be linked to Data Subjects, such as an internet domain name, the type of web browser used by a Data Subject, the type of operating system relied on by a Data Subject, the date and time of a Data Subject's visit to our Website(s) and Mobile Application(s), the specific pages a Data Subject may have visited, and the address of the website which a Data Subjects may have visited prior to entering or gaining access to the Company's Website(s) or Mobile Application(s).

"Operator" means a person or entity who Processes Personal Information/Data for a Responsible Party.

"Passive Processing Means " means the use of technologies to facilitate the Inactive Processing of Personal Information/Personal Data, namely the use of Cookies, Web Beacons, Embedded Scripts and/or Mobile Device Identifiers.

"Personal Data" (as defined in Article 4 of the GDPR) means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, which in the context of the Company shall comprise of the types of Personal Data recorded in this Policy below.

"Personal Information" shall have the same meaning as is given in section 1 of POPIA, but shall in the context of the Company comprise of the types of Personal Information recorded in this Policy below.

"Policy" means this Data Protection and Privacy Policy.

"POPIA" means the Protection of Personal Information Act, No 4 of 2013.

"Processing" means any operation or activity or any set of operations, whether or not by automatic means, concerning Personal Information/Personal Data, including:



- the collection, receipt, recording, organisation, collation, storage, updating or modification, retrieval, alteration, consultation or use;
- dissemination by means of transmission, distribution or making available in any other form by electronic communications or other means; or
- merging, linking, blocking, degradation, erasure or destruction. For the purposes of this definition, "**Process**" has a corresponding meaning.

"**Regulator**" means the Information Regulator established in terms of POPIA.

"**Responsible Party**" means in the context of this Policy, the Company.

"**Services**" means the various services provided by the Company to its Member(s), the particulars of which services are clearly set forth on the Company's Website from time to time and/or stipulated within respective legal documents.

"**Special Personal Information/Data**" means Personal Information/Personal Data concerning, amongst other aspects contemplated in terms of section 26 Part B of POPIA, a Data Subject's, religious beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, biometric data, or criminal behaviour.

"**Third-Party**" means any group company (if applicable), Member(s), Data Subject(s), employees, independent contractor, agent, consultant or user of the Company's Services, Website or any other digital application interface.

"**Unique Identifier**" means any identifier that is assigned to a Data Subject and is used by the Responsible Party for the purposes of the operations of that Responsible Party and that uniquely identifies that data subject in relation to the Responsible Party.

"**Website**" means the website owned and operated by the Company sourced at <https://fanakasa.org/>

"**Web Beacons**" means small graphic images called web beacons, also known as "Internet tags" or "clear gifs," which Web Beacons may be deployed in the Company's Website(s) pages and e-mail messages. Web beacons may be invisible to Data Subjects, but any electronic image inserted into a web page or e-mail can act as a Web Beacon. The Company may use web beacons or similar technologies for a number of purposes, including, without limitation, to count the number of visitors to our Websites, Mobile Application(s), to monitor how users navigate the Website(s) or Mobile Application(s), to count how many e-mails that we have sent were actually opened or to count how many particular articles or links were actually viewed by Data Subjects in certain circumstances.



INTRODUCTION

This Policy regulates the Processing of Personal Information/Personal Data by the Company and sets forth the requirements with which the Company undertakes to comply when Processing Personal Information/Personal Data pursuant to undertaking its operations and fulfilling its contractual obligations in respect of Data Subjects and Third Parties in general.

The Company places a high premium on the privacy of every person or organisation with whom it interacts or engages with and therefore acknowledges the need to ensure that Personal Information/Personal Data is handled with a reasonable standard of care as may be expected from it. The Company is therefore committed to ensuring that it complies with the requirements of POPIA, and also with the terms of the GDPR to the extent that the GDPR applies.

When a Data Subject or Third Party engages with the Company, whether it be physically or via any digital, electronic interface such as the Company's Website, the Data Subject or Third Party acknowledges that they trust the Company to Process their Personal Information/Personal Data, including the Personal Information/Personal Data of their dependents, beneficiaries, customers, members, or employees as the case may be, which further entrenches the importance of the Company's compliance with Applicable Laws in regards to the Processing of Personal Information/Personal Data.

All Data Subjects and Third Parties have the right to object to the processing of their Personal Information/Personal Data. It should be voluntary to accept the Terms and Conditions to which this Policy relates. However, the Company does require the Data Subject or Third Party's acceptance to enable the proper use of the Company's Website and/or Services.

PURPOSE AND APPLICATION

The purposes of this Policy are not only to inform Data Subjects of what Personal Information/Personal Data of theirs the Company may Process, where the Company may have collected such Personal Information/Personal Data from (if not directly from them as the Data Subject), how the Company Processes their Personal Information/Personal Data, but also to establish a standard by which the Company and its employees, representatives and operators shall comply in as far as the Processing of Personal Information/Personal Data is concerned.

The Company, in its capacity as a Responsible Party and/or Operator and/or Controller, as the case may be, shall strive to observe and comply with its obligations under POPIA and the GDPR (as may be applicable and to the extent necessary) when it Processes Personal Information/Personal Data from or in respect of any Data Subject.



COLLECTING AND PROCESSING OF PERSONAL INFORMATION/PERSONAL DATA

Whenever any Data Subject engages with the Company, whether it be physically or electronically, or through the use of its Services, facilities or Website the Company will in effect be Processing the Data Subject's Personal Information/Personal Data.

It may be from time to time that the Company has collected a Data Subject's Personal Information/Personal Data from other sources and in such instances the Company will inform the Data Subject by virtue of any privacy notices it deploys from time to time. In the event that a Data Subject has shared their Personal Information/Personal Data with any third parties, the Company will not be responsible for any loss suffered by the Data Subject, their dependents, beneficiaries, customers, representatives, agents or employees (as the case may be).

When a Data Subject provides the Company with the Personal Information of any other Third Party, the Company will process the Personal Information/Personal Data of such Third Party in line with this Policy, as well as any terms and conditions or privacy notices to which this Policy relates.

The Company will primarily Process Personal Information/Personal Data in order to facilitate and enhance the delivery of Products and/or Services to its Members, manage and administer its business, foster a legally compliant workplace environment, as well as safeguard the Personal Information/Personal Data relating to any Data Subjects which it in fact holds. In such an instance, the Data Subject providing the Company with such Personal Information/Personal Data may also be required to confirm that they are a Competent Person and that they have authority to give the requisite consent to enable the Company to process such Personal Information/Personal Data.

The Company undertakes to process any Personal Information/Personal Data in a manner which promotes the constitutional right to privacy, retains accountability and Data Subject participation.

Prior to recording the purpose(s) for which the Company may, or will, process the Personal Information/Personal Data of Data Subjects, the Company hereby records the types of Personal Information/Personal Data of Data Subjects it may process from time to time:

- Full names;
- Identity numbers;
- Registration numbers;
- Financial information, including banking account information;
- Statutory information;
- Physical and postal address particulars;



- Telephone numbers;
- Email addresses.

In supplementation of the above and any information privacy notices provided to any Data Subjects from time to time pursuant to any engagement with them, the Company may process Personal Information/Personal Data for the following purposes:

- To provide or manage any information, Products and/or Services requested by or delivered to Data Subjects in general;
- To establish a Data Subject's needs, wants and preferences in relation to the Products and/or Services provided by the Company;
- To help the Company identify Data Subjects when they engage with the Company;
- To facilitate the delivery of Products and/or Services to Members;
- To allocate to Members and Data Subjects Unique Identifiers for the purpose of securely storing, retaining and recalling their Personal Information/Personal Data from time to time;
- To maintain records of Data Subjects and specifically Member records;
- For employment purposes;
- For general administration purposes;
- For legal and/or contractual purposes;
- To improve the quality of the Company's Services;
- To transfer Personal Information/Personal Data to any other group company so as to enable the relevant group company to market its products and/or services to the Company's Member(s) or Third Party's, as well as to render specific services to the Company itself which would in turn enable the Company to render its Services to its Member(s);
- To transfer Personal Information/Personal Data to Third Party service providers so as to enable the Company to deliver Services to its Member(s);
- To analyse the Personal Information/Personal Data collected for research and statistical purposes;
- To help recover bad debts;



- To transfer Personal Information/Personal Data across the borders of South Africa to other jurisdictions if it is required;
- To carry out analysis and Member profiling;
- To identify other products and services which might be of interest to our Members and Data Subjects in general, as well as to inform them of such products and/or services;
- To comply with any Applicable Laws applicable to the Company.

When collecting Personal Information/Personal Data from a Data Subject, the Company shall comply with the notification requirements as set out in Section 18 of POPIA, and to the extent applicable, Articles 13 and 14 of the GDPR.

The Company will collect and Process Personal Information/Personal Data in compliance with the conditions as set out in POPIA and/or the Processing principles in the GDPR (as the case may be), to ensure that it protects the Data Subject's privacy.

The Company will not Process the Personal Information/Personal Data of a Data Subject for any purpose other than for the purposes set forth in this Policy or in any other privacy notices which may be provided to Data Subjects from time to time, unless the Company is permitted or required to do so in terms of Applicable Laws or otherwise by law.

The Company may from time-to-time Process Personal Information/Personal Data by making use of automated means (without deploying any human intervention in the decision-making process) to make decisions about the Data Subject or their application. In this instance it is specifically recorded that the Data Subject may object to or query the outcomes of such a decision.

PERSONAL INFORMATION/PERSONAL DATA FOR DIRECT MARKETING PURPOSES

The Company acknowledges that it may only use Personal Information/Personal Data to contact Data Subjects for purposes of direct marketing where the Company has complied with the provisions of POPIA and GDPR (where applicable) and when it is generally permissible to do so in terms of Applicable Laws.

In the event that the Company may lawfully direct market to a Data Subject in terms of section 69 of POPIA, the Company will ensure that a reasonable opportunity is given to such Data Subjects to object (opt-out) to the use of their Personal Information/Personal Data for the Company's marketing purposes when collecting the Personal Information/Personal Data and on the occasion of each communication to the Member for purposes of direct marketing.



STORAGE AND RETENTION OF PERSONAL INFORMATION/PERSONAL DATA

The Company will retain Personal Information/Data it has Processed, in an electronic or hardcopy file format, with a Third-Party service provider appointed for this purpose (the provisions of clause 9 below will apply in this regard).

Personal Information/Personal Data will only be retained by the Company for as long as necessary to fulfil the legitimate purposes for which that Personal Information/Personal Data was collected in the first place and/or as permitted or required in terms of Applicable Law.

It is specifically recorded that any Data Subject has the right to object to the Processing of their Personal Information and the Company shall retain and store the Data Subject's Personal Information/Personal Data for the purposes of dealing with such an objection or enquiry as soon and as swiftly as possible.

FAILURE TO PROVIDE PERSONAL INFORMATION

Where the Company is required to collect Personal Information/Personal Data from a Data Subject by law or in order to fulfil a legitimate business purpose of the Company and the Data Subject fails to provide such Personal Information/Personal Data, the Company may, on notice to the Data Subject, decline to render services without any liability to the Data Subject.

SECURING PERSONAL INFORMATION/PERSONAL DATA

The Company will always implement appropriate, reasonable, physical, organisational, contractual and technological security measures to secure the integrity and confidentiality of Personal Information/Personal Data, including measures to protect against the loss or theft, unauthorised access, disclosure, copying, use or modification of Personal Information/Personal Data in compliance with Applicable Laws.

In further compliance with Applicable Laws, the Company will take steps to notify the relevant Regulator(s) and/or any affected Data Subjects in the event of a security breach and will provide such notification as soon as reasonably possible after becoming aware of any such breach.

Notwithstanding any other provisions of this Policy, it should be acknowledged that the transmission of Personal Information/Personal Data, whether it be physically in person, via the internet or any other digital data transferring technology, is not completely secure. Whilst the Company has taken all appropriate, reasonable measures to secure the integrity and confidentiality of the Personal Information/Personal Data its Processes, in order to guard against the loss of, damage to or unauthorized destruction of Personal Information/Personal Data and unlawful access to or processing of Personal Information/Personal Data, the Company in no way guarantees that its security system(s) are 100% secure or error-free. Therefore, the Company does not guarantee the security or accuracy



of the information (whether it be Personal Information/Personal Data or not) which it collects from any Data Subject.

Any transmission of Personal Information/Personal Data will be solely at the own risk of a Data Subject. Once the Company has received the Personal Information/Personal Data, it will deploy and use strict procedures and security features to try to prevent unauthorised access to it. As indicated above, the Company reiterates that it restricts access to Personal Information/Personal Data to Third Parties who have a legitimate operational reason for having access to such Personal Information/Personal Data. the Company also maintains electronic and procedural safeguards that comply with the Applicable Laws to protect your Personal Information from any unauthorized access.

The Company shall not be held responsible and by accepting any terms and conditions to which this Policy relates, any Data Subject agrees to indemnify and hold the Company harmless for any security breaches which may potentially expose the Personal Information/Personal Data in the Company's possession to unauthorized access and or the unlawful processing of such Personal Information/Personal Data by any Third-Party.

PROVISION OF PERSONAL INFORMATION/PERSONAL DATA TO THIRD PARTIES

The Company may disclose Personal Information/Personal Data to Third-Party service providers and any group company where necessary and to achieve the purpose(s) for which the Personal Information/Personal Data was originally collected and Processed. The Company will enter into written agreements with such Third-Party service providers and group company, to ensure that they comply with Applicable Laws pursuant to the Processing of Personal Information/Personal Data provided to it by the Company from time to time.

TRANSFER OF PERSONAL INFORMATION/PERSONAL DATA OUTSIDE OF SOUTH AFRICA

The Company may, under certain circumstances, transfer Personal Information/Personal Data to a jurisdiction outside of the Republic of South Africa in order to achieve the purpose(s) for which the Personal Information/Data was collected and Processed, including for Processing and storage by Third-Party service providers.

If it is required, the Company will obtain the Data Subject's consent to transfer the Personal Information/Personal Data to such foreign jurisdiction.

The Data Subject should also take note that, where the Personal Information/Personal Data is transferred to a foreign jurisdiction, the Processing of Personal Information/Personal Data in the foreign jurisdiction may be subject to the laws of that foreign jurisdiction.



ACCESS TO PERSONAL INFORMATION/PERSONAL DATA

A Data Subject has the right to a copy of the Personal Information/Personal Data which is held by the Company (subject to a few limited exemptions as provided for under Applicable Law).

The Data Subject must make a written request (which can be by email) to the Information Officer designated by the Company from time to time and whose contact details can be sourced in the Company's PAIA Manual.

The Company will provide the Data Subject with any such Personal Information/Personal Data to the extent required by Applicable Law and subject to and in accordance with the provisions of the Company's PAIA Manual [published in terms of section 51 of the Promotion of Access to Information Act, 2000 ("PAIA"), which PAIA Manual can be sourced upon request to legal@m4jam.com].

The Data Subject can challenge the accuracy or completeness of his/her/its Personal Information/Personal Data in the Company's records at any time in accordance with the process set out in the Company's PAIA Manual.

KEEPING PERSONAL INFORMATION/PERSONAL DATA ACCURATE

The Company will take reasonable steps to ensure that Personal Information/Personal Data that it Processes is kept updated where reasonably possible. For this purpose, the Company shall provide Data Subjects with the opportunity to update their information at appropriate times.

The Company may not always expressly request the Data Subject to verify and update his/her/its Personal Information/Personal Data and expects that the Data Subject will notify the Company from time to time in writing:

- of any updates or amendments required in respect of his/her/its Personal Information/Personal Data;
- where the Data Subject requires the Company to delete his/her/its Personal Information/Personal Data; or
- where the Data Subject wishes to restrict the Processing of his/her/its Personal Information/Personal Data.

COSTS TO ACCESS PERSONAL INFORMATION/PERSONAL DATA

In the event that a cost is applicable, the prescribed fees to be paid for copies of the Data Subject's Personal Information/Personal Data are listed in the Company's PAIA Manual.

The Company reserves the right to make amendments to this Policy from time to time.



COMPLAINTS TO THE INFORMATION REGULATOR

If any Data Subject or Third Party is of the view or belief that the Company has Processed their Personal Information/Personal Data in a manner or for a purpose which is contrary to the provisions of this Policy, the Data Subject is requested to first attempt to resolve the matter directly with the Company , failing which the Data Subject or Third Party shall have the right to lodge a complaint with the Information Regulator, under the provisions of POPIA.

The current contact particulars of the Information Regulator are:

The Information Regulator (South Africa)

Website: <https://www.justice.gov.za/infoereg/index.html>

JD House 27 Stiemens Street Braamfontein Johannesburg, 2001

PO Box 31533

Braamfontein, Johannesburg, 2107

CONTACTING US

All comments, questions, concerns or complaints regarding Personal Information/Personal Data or this Policy, should be forwarded to the following email address legal@m4jam.com