KARATIVE (PTY) LTD. ("The Company")
Website Privacy Terms & Protection of Personal Information ("POPI") Policy
Our Website: http://Karative.co.za
Our Email Address: karatjbd@gmail.com

Last updated: 7 December 2022

WHEREAS the Company respects the privacy of all personal data and private information collected, processed and stored, and hereby adhere to the requirements as set out in the Protection of Personal Information Act 4 of 2013 ("POPI"). As such, we undertake to deal with all personal information received and processed with due care and diligence and provide the necessary security to safeguard all information held by us. Our internal system similarly allows us to proactively react should there be a breach of any kind, alternatively our privacy practices and POPI policy dictates that we report any material breach to the Regulator. Although we endeavour to always keep our website secure. We do however advise you that we cannot guarantee the security of any information provided to us or by us through our website, email, internet, or social media. We cannot be held responsible for any loss or unauthorised use, or interception of information transmitted via the internet which is beyond our control.

This Privacy Policy applies to all users of our website, related mobile sites and software applications, collectively referred to as "Platforms", which are used to access and purchase our products and services.

The purpose of this Privacy Policy is to set out how, why and when KARATIVE (Pty) Ltd. uses your Personal Information so as to comply with the Protection of Personal Information Act 4 of 2013 ("POPI").

It is important that you read this Privacy Policy together with our other terms and conditions, privacy notices or policies we may provide from time to time when we collect or use your Personal Information. Further, please pay special attention to the clauses in this Privacy Policy that appear in similar text and style (i.e. bold) which:

- May limit the risk or liability of KARATIVE (Pty) Ltd. or a third party;
- May create risk or liability for the user;
- May compel the user to indemnify KARATIVE (Pty) Ltd. or a third party; and/or
- Serves as an acknowledgement, by the user, of a fact.

We respect your privacy and take the protection of Personal Information very seriously. We strive to deliver excellent service every time you shop with us, and to do this, we need to use some of your Personal Information. This Privacy Policy describes how we handle the

Personal Information we collect about you and/or receive from you. By using our Platforms, you agree to the processing of your Personal Information as set out in this Privacy Policy.
In this Privacy Policy, the terms -

- **"Personal Information"**, and **"process/processing"** bear the same meanings as set out in POPI.
- **"we"**, **"us"** or **"our"** refers to KARATIVE (Pty) Ltd..
- "**you**" and "**your**" refers to every person that accesses or uses our Platforms also referred to as a user.
- "**registered user(s)"** refers to anyone registered on our Platforms and has provided us with a unique username and password as well as other Personal Information in order to order goods on our Platforms.

WEBSITE PRIVACY & POPI:

Your privacy is important to the Company. This policy explains the Company's privacy practices and the choices you have about the way your personal information will be dealt with. All practices are in line with the Company's PAIA Manual and the provisions of POPI. vii. Personal information is collected only when knowingly and voluntarily submitted. viii. Personal information is only used for the purpose for which it was collected and/or submitted or such secondary purposes that are related to the primary purpose. ix. In addition to where you have consented to the disclosure of your personal information, personal information may be disclosed in special situations where the Company has reason to believe that doing so is necessary to identity or act against anyone damaging or interfering with our rights or property, users or anyone else that could be harmed by such activities. x. The Company may engage third parties to provide you with goods or services on our behalf and in such circumstances may disclose your personal information to such parties in order to provide such goods and services.

THIRD PARTY WEBSITES:

Our website may contain links to other websites outside of *KARATIVE (PTY) LTD.* We are not responsible for the content, privacy or security of other websites.

SOCIAL PLUGINS:

We use social plugins of social networks such as Instagram, Facebook, YouTube, LinkedIn, Google+ and Twitter.
Please note that we have no influence on or control over the extent of the data retrieved by the social networks' interfaces and we can accordingly not to be held responsible or liable for any processing or use of personal information transmitted via these social plugins. For information on the purpose and extent of the data retrieval by the social network concerned,

and about the rights and settings possibilities for the protection of your private sphere, please refer to the data protection information provided by the social network in question.

COOKIES:

The Company uses cookies, pixels and other technologies (collectively referred to as "cookies") to recognize your browser or device, learn more about your company or industry, and provide you with essential features and services, as well as for additional purposes, including:
i. Recognizing you when you sign-up to use our services. This allows us to provide each user or data subject with customized features and services, if applicable.
ii. Conducting research and diagnostics to improve the Company's website content, products, and services.
iii. Preventing fraudulent activity.
iv. Improving security.
v. Delivering content, including ads, relevant to your interests.
vi. Reporting. This allows us to measure and analyze the performance of our services.

You can manage browser cookies through your browser setting. The "Help" feature on most browsers will tell you how to prevent your browser from accepting new cookies; how to have the browser notify you when you receive a new cookie; how to disable cookies; and when cookies will expire. If you disable all cookies on your browser, the Company, nor any of its third parties, will transfer cookies to your browser. If you do this, however, you may have to manually adjust some preferences every time you visit a site, and some features and services may not work.

INFORMATION SECURITY ON OUR WEBSITE:

xi. Any information that you upload on our website will be stored on a secure server and be used for limited purposes such as future communications (which you are always entitled to un-subscribe to).
xii. The Company will not disclose, sell, rent, or disseminate your personal information to third parties without your consent unless the Company is compelled to do so by law. The Company may do so if you have granted consent thereto.
xiii. While all reasonable efforts are taken to ensure that your personal information is protected as it travels over the internet, the Company cannot guarantee the absolute security of any information you exchange with us due to reason beyond our control.
xiv. The Company may use cookies and web beacons to facilitate improvement of our website. However, neither cookies nor web beacons collect personal information such as the user's name or email address. You may reject cookies, as most browsers permit individuals to decline the same.

PROTECTION OF PERSONAL INFORMATION & BREACH PROTOCOL

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 ("POPI Act").
The POPI Act 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 organization 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, being able to conduct her or her affairs relatively free from unwanted intrusions. Given the importance of privacy, the organization is committed to effectively managing personal information in accordance with the POPI Act'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, and where applicable, an identifiable, existing juristic person (such as a company), including but not limited to information concerning:

2.1.1. 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 person;
2.1.2. Information relating to the education or medical, financial, criminal or employment history of the person;
2.1.3. Any identifying number, symbol, email address, physical address, telephone number, location information, online identifier or other particular assignment to the person;
2.1.4. Biometric information of the person;
2.1.5. The personal opinions, views or preferences of the person;
2.1.6. 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;
2.1.7. The views or opinions of another individual about the person;
2.1.8. The name of the person if it appears with other personal information relating to the person or if the disclosure of the name itself would reveal information about the person.

2.1.9. Some other sensitive or special categories of personal information, including biometric information mentioned above, such as images, fingerprints and voiceprints.
2.2. **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 organization with products or other goods.
2.3. **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 organization is the responsible party.
2.4. **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 organization 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.
2.5**. Information Officer:** the information officer is responsible for ensuring the organization's compliance with the POPI Act. Where no information officer is appointed, the head of the organization will be responsible for fulfilling the information officer's duties. Once appointed, the information officer must be registered with the South African Information Regulator established under the POPI Act prior to performing his or her duties. Deputy Information Officers can also be appointed to assist the Information Officer.
2.6. **Processing:** the act of processing information includes any activity or any set of operations, whether by automatic means, concerning personal information and includes:
2.6.1. The collection, receipt, recording, organization, collation, storage, updating or modification, retrieval, alteration, consultation or use;
2.6.2. Dissemination by means of transmission, distribution or making available in any other form; or
2.6.3. Merging, linking, as well as any restriction, degradation, erasure or destruction of information.
2.7. **Record**: means any recorded information, regardless of form or medium, including:
2.7.1. Writing on any material;
2.7.2. 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
2.7.3. Label, marking or other writing which identifies or describes anything of which it forms part, or to which it is attached by any means;

2.7.4. Book, map, plan, graph or drawing;
2.7.5. 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.
2.8. **Filing System:** means any structed set of personal information, whether centralized, decentralized or dispersed on a functional or geographical basis, which is accessible according to specific criteria.
2.9. **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 the responsible party and that uniquely identifies that data subject in relation to that responsible party.
2.10. **De-Identify**: 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.
2.11. **Re-Identity**: means any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
2.12. **Direct Marketing:** means to approach a data subject, either in person or by mail or electronic communication, for the direct or indirect purpose of:
2.12.1. Promoting or offering to supply, in the ordinary course of business, any goods or services to the data subject; or
2.12.2. Requesting the data subject to make a donation of any kind for any reason.
2.13. **Biometrics**: means a technique of personal identification that is based on physical, physiological or behavioral characterization including blood typing, fingerprinting, DNA analysis, retinal scanning and voice recognition.
2.14. **Subscriber**: Individual that subscribes or logs in to our Platforms and/ or to the services offered by the App or any sort of app/ third-party app (if applicable) and *KARATIVE (PTY) LTD.* by way of its website agrees to the terms and conditions of the use of the App.
2.15. ***"KARATIVE (PTY) LTD."*** shall mean KARATIVE (Pty) Ltd., a company duly registered in the Republic of South Africa with registration number 2022/525872/07.
2.16. **"Platform"** shall mean hardware architecture and software frameworks that allow the Applications, website and integrated systems to run.
2.17. **"Application**" shall mean the/ a future *KARATIVE (PTY) LTD.* app, which app gives its Subscriber access to the Platform, alternatively any third-party app that might sell/ distribute *KARATIVE (PTY) LTD.* products.
2.18. **"Service"** shall mean the service offered via the *KARATIVE (PTY) LTD.* website and/ or any other platform/ app/ social media platform.

3. POLICY PURPOSE:

3.1. **The purpose of this policy is to protect the organization from the compliance risks associated with the POPI Act which includes:**
3.1.1. **Breaches of confidentiality.** For instance, the organization could suffer loss in revenue where it is found that the personal information of data subjects has been shared or disclosed inappropriately.
3.1.2. **Failing to offer choice.** For instance, all data subjects should be free to choose how and for what purpose the organization uses information relating to them.
3.1.3. **Reputational damage**. For instance, the organization could suffer a decline in shareholder value following an adverse event such as a computer hacker deleting the personal information held by an organization.
3.2. **This policy demonstrates the organization's commitment to protecting the privacy rights of data subjects in the following manner:**
3.2.1. Through stating desired behavior and directing compliance with the provisions of the POPI Act and best practice.
3.2.2. By cultivating an organizational culture that recognizes privacy as a valuable human right.
3.2.3. By developing and implementing internal controls for the purpose of managing the compliance risk associated with the protection of personal information.
3.2.4. 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 organization.
3.2.5. By assigning specific duties and responsibilities to control owners, including the appointment of an Information Officer and where necessary, Deputy Information officers, to protect the interests of the organization and data subjects.

4. POLICY APPLICATION

4.1. **This policy and its guiding principles applies to:**
4.1.1. The organization's governing body;
4.1.2. All branches, business units and divisions of the organization;
4.1.3. All employees and volunteers;
4.1.4. All contractors, suppliers and other persons acting on behalf of the organization.
4.2. The policy's guiding principles find application in all situations and must be read in conjunction with the POPI Act, as well as any other applicable documentation (PAIA Manual).
4.3. The legal duty to comply with the POPI Act is activated in any situation where there is: a processing of personal information entered into a record by or for a responsible party who is domiciled in South Africa.
4.4. The POPI Act does not apply in situations where the processing of personal information:

4.4.1. Is concluded in the course of purely personal or household activities; or
4.4.2. Where the personal information has been de-identified.

5. RIGHTS OF DATA SUBJECTS

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

5.1. The right to access of personal information
5.1.1. The organization recognizes that a data subject has the right to establish whether the organization holds personal information related to him, her or it, including the right to request access to that personal information.
5.2. The Right to have Personal Information Corrected or Deleted
5.2.1. The data subject has the right to request, where necessary, that his, her or its personal
information must be corrected or deleted where the Company is no longer authorised to retain the personal information.
5.3. The Right to Object to the Processing of Personal Information
5.3.1. 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 organization will give due consideration to the request and the requirements of POPIA. The organization 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.
5.4. The Right to Object to Direct Marketing
5.4.1. 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.
5.5. The Right to Complain to the Information Regulator
5.5.1. 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.
5.6. The Right to be Informed
5.6.1. 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 organization has reasonable grounds to believe that the personal information of the data subject has been accessed or acquired by an unauthorised person.

6. GENERAL GUIDING PRINCIPLES

All employees and persons acting on behalf of the organization (all affiliates and third-parties acting for and on behalf of the Company) will at all times be subject to, and act in accordance with, the following guiding principles:

6.1. Accountability

Failing to comply with the POPI Act could potentially damage the Company's reputation or expose the Company 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 Company 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.

6.2. Processing Limitation

The Company will ensure that personal information under its control is processed:
in a fair, lawful and non-excessive manner;
only with the informed consent of the data subject; and
only for a specifically defined purpose.

The Company 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 Company will maintain a voice recording of the stated purpose for collecting the personal information followed by the data subject's subsequent consent. The Company will under no circumstances distribute or share personal information between separate legal entities, associated Companies (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.

6.3. 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 Company
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 Company will first obtain additional consent from the data subject.

6.4. Information Quality

The Company will take reasonable steps to ensure that all personal information collected is complete, accurate and not misleading. Where personal information is collected or received from third parties, the Company 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.

6.5. Open Communication

The Company 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 Company 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;
Request access to related personal information;
Request the Company to update or correct related personal information; or
Make a complaint concerning the processing of personal information.

6.6. Security Safeguards

6.6.1. The Company will manage the security of its filing system to ensure that personal information is adequately protected. To this end, security controls will be implemented 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.

6.6.2. The Company 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 Company will ensure that all paper and electronic records comprising personal information are securely stored and made accessible only to authorised individuals.

6.6.3. 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 Company 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.

6.6.4. The Company's operators and third-party service providers/ independent contractors will be required to enter into service level agreements with the Company where both parties pledge their mutual commitment to POPIA and the lawful processing of any personal information pursuant to the agreement. These SLA's will be accessible on request via email to karatjbd@gmail.com. You will however have a separate relationship with these entities in relation to its use of your personal information. Approved *KARATIVE (PTY) LTD.* third-party service providers/ independent contractors are separate legal entities to *KARATIVE (PTY) LTD.* If you have any queries relating to the concerned third-party service providers/ independent contractors use of your personal information, you must contact the relevant entity directly.

6.7. Data Subject Participation A data subject may request the correction or deletion of his, her or its personal information held by the Company. The Company 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 Company will include a link to unsubscribe from any of its electronic newsletters or related marketing activities.

7. PURPOSE SPECIFICATION

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

7.1 Information we collect automatically through the use of technology

When you visit our website, use our mobile app/ any other third-party app (if applicable), read our emails or otherwise engage with us, we and our business partners may automatically collect certain information about your computer or device through a variety of tracking technologies, including cookies, web beacons, log files, embedded scripts, location-identifying technologies, or other tracking/recording tools (collectively, "tracking technologies"), and we may combine this information with other personal information we collect about you. We use these tracking technologies to collect usage and device information, such as:

- Information about how you access the Service, for example, referral/exit pages, how frequently you access the Service, whether you open emails or click the links

contained in emails, whether you access the Service from multiple devices, and other actions you take on the Service.

- Information about how you use the Service, for example, the features you use, the links you click, the ads you view and click on, purchase transaction information, your location when you access or interact with our Service, and other similar actions.
- Information about the computer, tablet, smartphone or other device you use, such as your IP address, browser type, Internet service provider, platform type, device type/ model/ manufacturer, operating system, phone number, mobile carrier, date and time stamp, a unique ID that allows us to uniquely identify your browser, mobile device or your account (including, for example, a UDID, IDFA, Google Ad ID, Windows Advertising ID or other persistent device identifier or Ad ID), battery life, and other such information. With your permission, we may also access your photo or camera roll.

7.2 What personal information we collect and process

KARATIVE (Pty) Ltd. processes Personal Information in a manner that is reasonable, adequate, relevant, non-excessive and purpose specific. In order for users to access and use our Platforms we collect and process some Personal Information. When you become a registered user, we have to collect and process your Personal Information to render our services to you.

When you register to use our Platforms, we may collect the following Personal Information:

- Name and surname;
- Email address;
- Physical address;
- Billing address;
- Payment details;
- Gender;
- Mobile phone number;
- Online identifiers;
- Date of birth; and/or

- Identification number.

Should your Personal Information change or you wish to amend and/or correct this Personal Information you can do this by updating your registered user information in your account profile.

You warrant that the information you have provided is accurate, current, true and correct and that does not impersonate or misrepresent any person or entity or falsely state or otherwise misrepresent your affiliation with anyone or anything.

7.3 Information from using our platforms

When you access our Platforms, whether or not you are a registered user of KARATIVE (Pty) Ltd., we process some of your Personal Information. Depending on how you access and use our Platforms, we may receive:

- log information, through online identifiers, including information on how, when and for how long you use our Platforms and other services, the content you view and search queries you submit.

- information about the equipment you use to access or use our Platforms, including the type of device you are using, how you access our Platforms, your browser or operating system and your Internet Protocol address.

- the geographic location from which you accessed our Platforms, including your device's global positioning system signal and information about nearby wifi networks and cell towers. We get this information when you use location-enabled services.

- other information about you from third parties, such as social media.

7.4 Why do we process your personal information?

We process the Personal Information we collect and receive to:

- identify you;

- verify your identity;

- create a user account for you; and/or

- enter into a contract with you.

As a registered user, we also process your Personal Information in order to:

- fulfil our contractual obligations to you when you have ordered goods in order for us to deliver those goods and process returns.

- provide you with information, products or services you request from us.

- communicate with you regarding our Platforms and provide you with information, products or services, including billing, customer support, resolving complaints and quality control.

- notify you about changes to our Platforms, services and products, terms and conditions, privacy policy or notices, and any other changes that impact our Platforms, services and products.

- send you information about competitions, products or services that may interest you (unless you have opted out of receiving such information).

- get feedback from you which we need to develop our products and services and grow our business.

- comply with any legal or regulatory obligations such as tax or financial laws.

- undertake research and statistical purposes. The research and statistics we get from this process do not include your Personal Information and cannot be linked to you, nor can you be identified from these statistics.

7.5 Retention and restriction of records

We keep your Personal Information for as long as:

- we need it to provide our Platforms, products or services to you.

- it is required or allowed by law and is in line with our internal retention policies.

- it is necessary to uphold the contract between you and us.

- you have agreed to us keeping your Personal Information subject to your request for us to stop processing your Personal Information.

We will retain your Personal Information for as long as is necessary to achieve the purpose for which this information was collected or subsequently processed. If your Personal Information is used for more than one purpose, we will retain it until the purpose with the latest period expires but we will stop using it for the purpose with a shorter period once that period expires.

By accessing and using the Platform, you consent to us retaining records of your Personal Information for no longer than may be necessary to achieve the purpose for which the information was initially collected or subsequently processed.

7.6 We may receive information about you in alternative ways, including but not limited to:

- When you contact us directly, either via our website, web chat service, our Customer Service teams, by email, telephone or via social media, whether to apply for one of our products or services or to make an enquiry or other request;
- From our network of authorized *KARATIVE (PTY) LTD.* Retailers/Agencies;
- From other *KARATIVE (PTY) LTD.* entities or entities within, or affiliates of, *KARATIVE (PTY) LTD.*;
- From third parties, such as credit bureaus, when we do credit checks or decide whether to enter into an agreement with you; or
- Occasionally from other third parties who may lawfully pass your information on to us.
- Telephone calls to us may be recorded and/or monitored for training and quality assessment purposes.

8. INFORMATION OFFICER

8.1. 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.
8.2. 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 re-appointment or replacement of any Deputy Information Officers.
8.3. 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.

9. SPECIFIC DUTIES AND RESPONSIBILITIES

9.1. Governing Body/Board of Directors
The Company's governing body cannot delegate its accountability and is ultimately answerable for ensuring that the Company meets its legal obligations in terms of POPIA. The

governing body may however delegate some of its responsibilities in terms of POPIA to management or other capable individuals.

The governing body is responsible for ensuring that:

9.1.1. The Company appoints an Information Officer, and where necessary, a Deputy Information Officer.

9.1.2. All persons responsible for the processing of personal information on behalf of the Company:

9.1.2.1. are appropriately trained and supervised to do so;

9.1.2.2. understand that they are contractually obligated to protect the personal information they come into contact with; and

9.1.2.3. are aware that a wilful or negligent breach of this policy's processes and procedures may lead to disciplinary action being taken against them.

9.1.3. Data subjects who want to make enquiries about their personal information are made aware of the procedure that needs to be followed should they wish to do so.

9.1.4. The scheduling of a periodic POPI Audit in order to accurately assess and review the ways in which the Company collects, holds, uses, shares, discloses,
destroys and processes personal information.

9.2. Information officer

The Company's Information Officer is responsible for:

9.2.1. Taking steps to ensure the Company's reasonable compliance with the provision of POPIA.

9.2.2. Keeping the governing body updated about the Company's information protection responsibilities under POPIA. For instance, in the case of a security breach, the Information Officer must inform and advise the governing body of their obligations pursuant to POPIA.

9.2.3. Continually analysing privacy regulations and aligning them with the Company's personal information processing procedures. This will include reviewing the Company's information protection procedures and related policies.

9.2.4. Ensuring that POPI Audits are scheduled and conducted on a regular basis.

9.2.5. Ensuring that the Company makes it convenient for data subjects who want to update their personal information or submit POPI related complaints to the Company. For instance, maintaining a "contact us" facility on the Company's website.

9.2.6. Approving any contracts entered with operators, employees and other third parties which may have an impact on the personal information held by the Company. This will include overseeing the amendment of the Company's employment contracts and other service level agreements.

9.2.7. Encouraging compliance with the conditions required for the lawful processing of personal information.

9.2.8. Ensuring that employees and other persons acting on behalf of the Company are fully aware of the risks associated with the processing of personal information and that they remain informed about the Company's security controls.

9.2.9. Organising and overseeing the awareness training of employees and other individuals involved in the processing of personal information on behalf of the Company.
9.2.10. Addressing employees' POPIA related questions.
9.2.11. Addressing all POPIA related requests and complaints made by the Company's data subjects.
9.2.12. Working with the Information Regulator in relation to any ongoing investigations.
The Information Officers will therefore act as the contact point for the Information Regulator authority on issues relating to the processing of personal information and will consult with the Information Regulator where appropriate, regarding any other matter. The Deputy Information Officer will assist the Information Officer in performing his or her duties.

9.3. IT Manager / IT Support

The Company's IT Manager or IT Support is responsible for:
9.3.1. Ensuring that the Company's IT infrastructure, filing systems and any other devices used for processing personal information meet acceptable security standards.
9.3.2. Ensuring that all electronically held personal information is kept only on designated drives and servers and uploaded only to approved cloud computing services.
9.3.3. Ensuring that servers containing personal information are sited in a secure location, away from the general office space.
9.3.4. Ensuring that all electronically stored personal information is backed-up and tested on a regular basis.
9.3.5. Ensuring that all back-ups containing personal information are protected for unauthorised access, accidental deletion and malicious hacking attempts.
9.3.6. Ensuring that personal information being transferred electronically is encrypted.
9.3.7. Ensuring that all servers and computers containing personal information are protected by a firewall and the latest security software.
9.3.8. Performing regular IT audits to ensure that the security of the Company's hardware and software systems are functioning properly.
9.3.9. Performing regular IT audits to verify whether electronically stored personal information has been accessed or acquired by any unauthorised persons.
9.3.10. Performing a proper due diligence review prior to contracting with operators or any other third-party service providers to process personal information on the Company's behalf. For instance, cloud computing services.

9.4. Marketing & Communications Manager / Team

The Company's Marketing & Communication Manager / Team is responsible for:
9.4.1. Approving and maintaining the protection of personal information statements and disclaimers that are displayed on the Company's website, including those attached to communications such as emails and electronic newsletters.

9.4.2. Addressing any personal information protection queries from journalists or media outlets such as newspapers.
9.4.3. Where necessary, working with persons acting on behalf of the Company to ensure that any outsourced marketing initiatives comply with POPIA.

9.5. Employees and other persons acting on behalf of the Company
9.5.1. Employees and other persons acting on behalf of the Company will, during the course of the performance of their services, gain access to and become acquainted with the personal information of certain clients, suppliers and other employees.
9.5.2. Employees and other persons acting on behalf of the Company are required to treat personal information as a confidential business asset and to respect the privacy of data subjects.
9.5.3. Employees and other persons acting on behalf of the Company may not directly or indirectly, utilise, 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.
9.5.4. Employees and other persons acting on behalf of the Company must request assistance from their line manager or the Information Officer if they are unsure about any aspect related to the protection of a data subject's personal information.
9.5.5. Employees and other persons acting on behalf of the Company will only process personal information where:
9.5.5.1. The data subject, or a competent person where the data subject is a child, consents to the processing; or
9.5.5.2. The processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is a party; or
9.5.5.3. The processing complies with an obligation imposed by law on the responsible party; or
9.5.5.4. The processing protects a legitimate interest of the data subject; or
9.5.5.5. The processing is necessary for pursuing the legitimate interests of the Company or of a third party to whom the information is supplied.
9.5.6. Furthermore, personal information will only be processed where the data subject:
9.5.6.1. Clearly understands why and for what purpose his, her or its personal information is being collected; and
9.5.6.2. Has granted the Company with explicit written or verbally recorded consent to process his, her or its personal information.
9.5.7. Employees and other persons acting on behalf of the Company will consequently, prior to processing any personal information, obtain a specific and informed expression of will from the data subject, in terms of which permission is given for the processing of personal information.
9.5.8. Informed consent is therefore when the data subject clearly understands for what

purpose his, her or its personal information is needed and who it will be shared with.
9.5.9. Consent can be obtained in written form which includes any appropriate electronic medium that is accurately and readily reducible to printed form. Alternatively, the Company will keep a voice recording of the data subject's consent in instances where transactions are concluded telephonically or via electronic video feed.
9.5.10. Consent to process a data subject's personal information will be obtained directly from the data subject, except where:
9.5.10.1. the personal information has been made public;
9.5.10.2. where valid consent has been given to a third party; or
9.5.10.3. the information is necessary for effective law enforcement.
9.5.11. Employees and other persons acting on behalf of the Company will under no circumstances:
9.5.11.1. Process or have access to personal information where such processing or access is not a requirement to perform their respective work-related tasks
or duties.
9.5.11.2. Save copies of personal information directly to their own private computers, laptops or other mobile devices like tablets or smartphones.
All personal information must be accessed and updated from the Company's central database or a dedicated server.
9.5.11.3. Share personal information informally. In particular, personal information should never be sent by email, as this form of communication is not
secure. Where access to personal information is required, this may be requested from the relevant line manager or the Information Officer.
9.5.11.4. Transfer personal information outside of South Africa without the express permission from the Information Officer.
9.5.12. Employees and other persons acting on behalf of the Company are responsible for:
9.5.12.1. Keeping all personal information that they come into contact with secure, by taking sensible precautions and following the guidelines outlined within this policy.
9.5.12.2. Ensuring that personal information is held in as few places as is necessary. No unnecessary additional records, filing systems and data sets should therefore be created.
9.5.12.3. Ensuring that personal information is encrypted prior to sending or sharing the information electronically. The IT Manager will assist employees and where required, other persons acting on behalf of the Company, with the sending or sharing of personal information to or with authorised
external persons.
9.5.12.4. Ensuring that all computers, laptops and devices such as tablets, flash drives and smartphones that store personal information are password protected and never left unattended. Passwords must be changed regularly and may not be shared with unauthorised persons.
9.5.12.5. Ensuring that their computer screens and other devices are switched off or locked when not in use or when away from their desks.

9.5.12.6. Ensuring that where personal information is stored on removable storage medias such as external drives, CDs or DVDs that these are kept locked away securely when not being used.
9.5.12.7. Ensuring that where personal information is stored on paper, that such hard copy records are kept in a secure place where unauthorised people cannot access it. For instance, in a locked drawer of a filing cabinet.
9.5.12.8. Ensuring that where personal information has been printed out, that the paper printouts are not left unattended where unauthorised individuals could see or copy them. For instance, close to the printer.
9.5.12.9. Taking reasonable steps to ensure that personal information is kept accurate and up to date. For instance, confirming a data subject's contact details when the client or customer phones or communicates via email. Where a data subject's information is found to be out of date, authorisation must first be obtained from the relevant line manager or the Information Officer to update the information accordingly.
9.5.12.10. Taking reasonable steps to ensure that personal information is stored only for as long as it is needed or required in terms of the purpose for which it was originally collected. Where personal information is no longer required, authorisation must first be obtained from the relevant line manager or the Information Officer to delete or dispose of the personal information in the appropriate manner.
9.5.12.11. Undergoing POPI Awareness training from time to time.
9.5.13. Where an employee, or a person acting on behalf of the Company, becomes aware or suspicious of any security breach such as the unauthorised access, interference, modification, destruction, or the unsanctioned disclosure of personal information, he or she must immediately report this event or suspicion to the Information Officer or the Deputy Information Officer.

10. POPI AUDIT

10.1. The Company's Information Officer will schedule periodic POPI Audits.
10.2. The purpose of the POPI Audit is to:
10.2.1. Identify the processes used to collect, record, store, disseminate and destroy personal information.
10.2.2. Determine the flow of personal information throughout the Company. For instance, the Company's various business units, divisions, branches and other associated Companies.
10.2.3. Redefine the purpose for gathering and processing personal information.
10.2.4. Ensure that the processing parameters are still adequately limited.
10.2.5. Ensure that new data subjects are made aware of the processing of their personal information.
10.2.6. Re-establish the rationale for any further processing where information is received via a third party.
10.2.7. Verify the quality and security of personal information.

10.2.8. Monitor the extent of compliance with POPIA and this policy.
10.2.9. Monitor the effectiveness of internal controls established to manage the Company's POPI related compliance risk.
10.3. In performing the POPI Audit, Information Officers will liaise with line managers in order to identify areas within the Company's operation that are most vulnerable or susceptible to the unlawful processing of personal information. Information Officers will be permitted direct access to and have demonstrable support from line managers and the Company's governing body in performing their duties.

11. REQUEST TO ACCESS PERSONAL INFORMATION

11.1. Data subjects have the right to:
11.1.1. Request what personal information the Company holds about them and why.
11.1.2. Request access to their personal information.
11.1.3. Be informed how to keep their personal information up to date.
11.2. 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" also attached hereto as **Annexure "A**", to be completed and submitted to the Information Officer via email at karatjbd@gmail.com.
11.3. 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.
11.4. The Information Officer will process all requests within a reasonable time.

12. POPI COMPLAINTS PROCEDURE

12.1. 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:
12.1.1. 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", also attached hereto as **Annexure "A**", to be completed and submitted to the Information Officer.
12.1.2. 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.
12.1.3. The Information Officer will provide the complainant with a written acknowledgement of receipt of the complaint within 2 working days.
12.1.4. 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 endeavour to resolve the complaint in a fair manner and in

accordance with the principles outlined in POPIA.
12.1.5. 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.
12.1.6. Where the Information Officer has reason to believe that the personal information of data subjects has been accessed or acquired by an unauthorised 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.
12.1.7. 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.
12.1.8. The Information Officer's response to the data subject may comprise any of the following:
12.1.8.1. A suggested remedy for the complaint,
12.1.8.2. A dismissal of the complaint and the reasons as to why it was dismissed, or
12.1.8.3. An apology (if applicable) and any disciplinary action that has been taken against any employees involved.
12.1.9. 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.
12.1.10. 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.

13. PERSONAL DATA BREACH PROTOCOL

13.1. For the purposes of this section, a personal data breach is any attempt at, or occurrence of, unauthorized acquisition, exposure, disclosure, use, modification or destruction of personal and/or sensitive data as described in this policy. The breach protocol is meant to address security incidents involving any and all personal data held, collected, processed and/or stored by the Company, including personal data under the control or responsibility of an affiliated business or third party.
13.2. The Company shall ensure that, inter alia, all personal data breaches are reported to the Regulator, investigated and contained within the Company or by the Company and in terms of this policy.
13.3. The following is an indication of the timelines necessary herein and to be followed by the Company and/or its Information Officer when responding to, investigating and reporting on any personal data breach within the Company:
13.3.1. Initial response to discovering personal data breach, or potential breach:
13.3.1.1. Identifying personal data breach or potential breach;

13.3.1.2. Involvement of Information Officer, IT/Server Department and any necessary and/or applicable parties;
13.3.1.3. Involvement of compliance department, legal department or similar (if applicable to the Company).
13.3.2. Immediate Response (0–1 Business Day):
13.3.2.1. Containment
13.3.2.2. Opening of Incident Report or POPI Breach report;
13.3.2.3. Escalation to the relevant individuals or authorative body(ies);
13.3.2.4. Activation of initial response plan and/or containment plan.
13.3.3. Continuing Response (0-15+ days)
13.3.3.1. Analysis and Planning (both in terms of closure of the pending breach and initiation of any plans regarding prospective breaches or the avoidance thereof);
13.3.3.2. Investigation;
13.3.3.3. Mitigation and Correction;
13.3.3.4. Notification;
13.3.3.5. Closing of Incident Report or POPI Breach report;
13.3.3.6. Final reporting (Information Officer, Regulator and Data Subjects).
13.4. Initial Response: the Company must take proactive steps to ensure that any personal data breach or potential breach is identified as soon as reasonably possible. Once identified, the Company, through its IT department and Information Officer, must bring the personal data breach or potential breach to the attention of the necessary parties who will be responsible for containing the personal data breach or potential breach.
13.5. Immediate Response: the Company, its IT department and the Information Officer must, when a breach is discovered, conduct containment activities to stop additional information from being lost or disclosed, or to reduce the number of persons to whom personal information may reach. The Company may, over its areas of responsibility or collaboratively, take steps to attempt having lost/stolen/inappropriately disclosed information returned or destroyed. For instance, area managers may attempt to contain and control an incident by suspending certain activities or locking and securing areas of record storage; Human Resources may suspend employees as appropriate to prevent compromising behavior; and the Information IT Department may shut down particular applications or third party connections, reconfigure firewalls, change computer access codes, or change physical access codes.
13.6. If applicable, staff members closest to the incident will determine the extent of the breach or potential breach by identifying all information (and systems) affected, and take action to stop the exposure.
This may include:
13.6.1. Securing or disconnecting affected systems;
13.6.2. Securing affected records or documentation;
13.6.3. Halting affected business processes;
13.6.4. Pausing any processes that may rely on exposed information or that may have given rise to the incident (as necessary to prevent further use/exposure/etc)

This would most typically occur in instances of electronic system intrusion, exposed physical (e.g. medical) files or records or similar situations.
13.7. If an active cyber-insurance policy exists or the need is otherwise determined, the Company or its Information Officer may contact contracted third parties
(cyber-insurance vendors or affiliates) for breach response services and resources to include forensics, investigation and response consulting, notification and call center services. Though recommended to occur as soon as possible after discovery, this can occur at any point as more information is obtained or the need is otherwise determined.
13.8. All documentation, investigation and initial and/or containment reports must be kept throughout the personal data breach protocol procedure and included in any report from the Information Officer to the Regulator in terms of section 22 of the POPI Act.
13.9. As more information is gathered, responsible staff will assess each personal data breach or potential breach to determine appropriate handling. This may involve the development and use of internal procedures by individual departments. For instance, while a minor and low risk incident may be assigned to and investigated by competent technicians within a department, the department may require that technician to escalate to management any incident that may damage the Company. The manager, in turn, may escalate the incident to the director, VP, or other level (subject to the Company's internal structure and/or organogram).
13.10. This may also involve activating alternate plans – for instance, Data Recovery Plans and/or any applicable alternative.
13.11. Additionally, responsible departments will assess each personal data breach to determine which parties should be included in communications and/or the further reporting of the personal data breach incident. For instance, the Company or Information Officer may grant certain access and permissions pertaining to cases to include area managers, directors, and vice-presidents unless circumstances exist that would preclude sharing information – for instance, if a conflict of interest exists; if sharing the information could compromise an investigation; or if the responsible manager (or a friend or family member of the responsible manager) is involved as an affected party, as a subject, or in other ways.
13.12. Continued response and reporting to the Regulator: all efforts, including but not limited to the initial reporting; the containment and any containment plans; any further planning and proposed corrections; and/or record of any correspondence or notice sent to any of the Company's affected data subjects must be kept and form a material part of the final incident report submitted to the Regulator in terms of section 22 of the POPI Act.
13.13. After containment of the personal data breach and implementation of any necessary containment plan; interim plan or relief; correction plan; data recovery plan; and/or similar plan implemented in response to the personal data breach, the Company's Information Officer must prepare a written report to submit to the Regulator.
13.14. The aforementioned written report must contain all necessary and material information pertaining to the personal data breach, including but not limited, any supporting documentation, investigation outcomes and/or improvement plans. The report must indicate whether the breach was low, moderate or high risk and the extent of the personal data breach, including but not

limited to any actual damages suffered; any damage or injury to affected data subjects; and any potential or further threat created by the personal data breach.
13.15. The Information Officer must further notify all affected data subjects of the personal data breach as soon as reasonably possible after discovery of the personal data breach, taking into account the legitimate needs of law enforcement or any measures reasonably necessary to determine the scope of the breach and to restore the integrity of the Company's information system. The notification must be done in writing and communicated to the data subject in one of the following ways:
13.15.1. Mailed to the data subject's last known physical or postal address;
13.15.2. Sent by email to the data subject's last known email address;
13.15.3. Placed in a prominent position on the website of the Company;
13.15.4. Published in the news or media; or
13.15.5. As may be directed by the Regulator.
13.16. The notification must provide the affected data subjects with sufficient information to allow the data subject to take protective measures against the personal data breach, including –
13.16.1. A description of the possible consequences of the breach;
13.16.2. A description of the measures that the Company intends to take of has taken to address the personal data breach and/or security compromise;
13.16.3. A recommendation with regard to the measures to be taken by the data subject to mitigate the possible adverse effects of the personal data breach; and
13.16.4. The identity of the unauthorised person or entity who may have accessed or acquired personal information, if known to the Company.
13.17. The Regulator may direct any Company to publicize, in any manner specified, the fact of any personal data breach or compromise to the integrity of personal
information, if the Regulator has reasonable grounds to believe that such publicity would protect a data subject who may be affected by the breach.

14. DISCIPLINARY ACTION

14.1. Where a POPI complaint or a POPI infringement investigation has been finalised, the Company may recommend any appropriate administrative, legal and/or disciplinary action to be taken against any employee reasonably suspected of being implicated in any non-compliant activity outlined within this policy.
14.2. In the case of ignorance or minor negligence, the Company will undertake to provide further awareness training to the employee.
14.3. Any gross negligence or the wilful mismanagement of personal information, will be considered a serious form of misconduct for which the Company may summarily dismiss the employee. Disciplinary procedures will commence where there is sufficient evidence to support an employee's gross negligence.
14.4. Examples of immediate actions that may be taken subsequent to an investigation include:

14.4.1. A recommendation to commence with disciplinary action.
14.4.2. A referral to appropriate law enforcement agencies for criminal investigation.
14.4.3. Recovery of funds and assets in order to limit any prejudice or damages caused.

15. **CAN THIS PRIVACY STATEMENT BE AMENDED?**

We may amend this Statement from time to time for any of the following reasons:

15.1. to provide for the introduction of new systems, methods of operation, services, products, property offerings or facilities;
15.2. to reflect an actual or expected change in market conditions or general financial services or lending practices;
15.3. to comply with changes to any Applicable Laws;
15.4. to ensure that this Statement is clearer and more favourable to you;
15.5. to rectify any mistake that might be discovered from time to time; and/or
15.6. for any other reason which *KARATIVE (PTY) LTD.*, in its sole discretion, may deem reasonable or necessary.
15.7. Any such amendment will come into effect and become part of any agreement you have with *KARATIVE (PTY) LTD.* when notice is given to you of the change by publication on our website. It is your responsibility to check the website often.

16. FREQUENTLY ASKED QUESTIONS – PRIVATE AND PERSONAL DATA

Is my information safe with *KARATIVE (PTY) LTD.*?

We continuously implement technical and Company security measures in order to protect the data we hold against unauthorised access as well as accidental or wilful manipulation, loss or destruction.

It is also important that you take all necessary and appropriate steps to protect your personal information yourself (for example, by ensuring that all login details, including passwords and access codes are kept secure).

How is my personal information processed?

We take the privacy and protection of your personal information very seriously and will only process your personal information in accordance with the Applicable Laws and this Statement.

Accordingly, *KARATIVE (PTY) LTD.* will comply with the relevant data privacy principles or conditions relating to the processing (including, but not limited to, the collection, handling, transfer, sharing, correction, storage, archiving and deletion) of your personal information set out in Applicable Laws.

KARATIVE (PTY) LTD. employees attend regular data protection training. Your personal information will only be processed for purposes set out in this Statement or if we are entitled to do so under Applicable Laws.

Can *KARATIVE (PTY) LTD.* retain my information?

We may retain your personal information indefinitely, unless you object, in which case we will only retain it if we are permitted or required to do so in terms of Applicable Laws. However, as a general rule, we will retain your information in accordance with retention periods set out in Applicable Laws, unless we need to retain it for longer for a lawful purpose (for example, for the purposes of complaints handling, legal processes and proceedings).

What rights do I have regarding my personal information?

You have the right to contact relevant credit bureau(s), to have the credit record(s) disclosed and to correct any inaccurate information.

You have a right in certain circumstances to request the destruction or deletion of and, where applicable, to obtain restriction on the processing of personal information held about you. If you wish to exercise this right, please contact us using the contact details set out in our **PAIA Manual** and on our website.

You have a right to object on reasonable grounds to the processing of your personal information where we claim such processing is necessary to pursue our legitimate interests, your legitimate interests or the legitimate interests of a third party to which the information is supplied. We may then stop such processing, unless Applicable Laws provide for such processing.

Can information be shared with third parties? / Can *KARATIVE (PTY) LTD.* share my information?

We may share your personal information with:

- Other *KARATIVE (PTY) LTD.* entities, our agents and sub-contractors, third parties who process personal information on our behalf and *KARATIVE (PTY) LTD.* companies, or affiliates, in South Africa and in other countries;
- Our authorised *KARATIVE (PTY) LTD.* Retailers/Agencies/ Affiliates and Independent Contractors;
- Our carefully selected business partners, including those who provide products and services under any of our brands;
- Our service providers and agents who perform services on our behalf;
- Any person who has agreed or is considering providing security for your indebtedness, including any surety, guarantor, potential surety or potential guarantor under any

finance document who requests such information to evaluate any actual or potential liability under such suretyship or guarantee;

- A prospective buyer or seller of any of our businesses, assets or debt;
- A person who acquires substantially all of the assets of a *KARATIVE (PTY) LTD.* Affiliate;
- Any person if we are under a duty to disclose or share your personal information in order to comply with any Applicable Laws, or to protect the rights, property or safety of *KARATIVE (PTY) LTD.*, its clients or other third parties;
- banks, collection agencies, lawyers, accountants, auditors, regulators and law enforcement agencies, to the extent necessary to protect, preserve or enforce *KARATIVE (PTY) LTD.*'s rights and interests in respect of any agreement or any finance document or to respond to any legal enquiry or to comply with any regulatory obligation.

We may disclose your personal information to these third parties for any purpose permitted in terms of Applicable Laws, including to-

- assess and monitor any of your applications for *KARATIVE (PTY) LTD.* products or services, including the risk involved to comply with Applicable Laws;
- determine which products and services may be of interest to you and/or to send you information about such products and services, unless you object or choose not to receive such communications;
- keep your usual contact within *KARATIVE (PTY) LTD.* informed of the progress of any new applications for new services or products, and the other way around;
- have a better understanding of your circumstances and needs to provide and improve *KARATIVE (PTY) LTD.*'s products and services;
- comply with Applicable Laws requiring *KARATIVE (PTY) LTD.* and/or any third party to collect personal information;
- identify whether other financial institutions have received payment from you due to us;
- detect and report fraud and criminal activities, to identify the proceeds of unlawful activities and to combat crime;
- use for marketing purposes; and
- make reports to any regulator or supervisory authority, including those in foreign jurisdictions, if *KARATIVE (PTY) LTD.* is required to do so in terms of Applicable Laws.

We do not share your personal information with any third parties, except if:

- we are legally permitted or obliged to provide such information for legal or regulatory purposes;
- we are required to do so for purposes of existing or future legal proceedings;
- we are selling one or more of our businesses to someone to whom we may transfer our rights under any agreement we have with you;
- Necessary for purposes of preventing fraud, loss, bribery or corruption;
- they perform services and process personal information on our behalf;
- it is required in order to provide or manage any information, products and/or services to you;
- needed to help us improve the quality of our products and services.

If you do not wish us to disclose this information to third parties, please contact us at the contact details set out herein. We may, however, not be able to provide products or services to you if such disclosure is necessary.

Can I share information with *KARATIVE (PTY) LTD.* on third Parties?

Where you provide us with the personal information of third parties you should take steps to inform the third party that you need to disclose their details to us and identify us. We will process their personal information in accordance with this Statement. If you give us information on behalf of someone else, you confirm to us that you have their permission to do so and that they are aware of the contents of this Statement and do not have any objection to us processing their information in accordance with this Statement.

What is my personal information used for?

Subject to Applicable Laws, we may use your personal information for a variety of purposes, including:

Legal Contractual

- Legal or contractual purposes;
- To manage other contractual arrangement or relationship;
- To detect and prevent fraud and money laundering and/or in the interest of security and crime prevention;
- To conduct sanction party list and politically exposed person screening against any relevant list which *KARATIVE (PTY) LTD.* may in its sole discretion determine;
- To verify your identity;

- To comply with applicable laws, including lawful requests for information received from local or foreign law enforcement, government and tax collection agencies;

Marketing & Data Analytics/Enrichment

- Data analytics and/or enrichment;
- To carry out analysis and customer profiling;
- To identify other products and services which might be of interest to you;
- To assess and deal with complaints and requests;
- To conduct market research and provide you with information about *KARATIVE (PTY) LTD.*'s products or services from time to time via email, telephone or other means (for example, events).
- Where you have unsubscribed from certain direct marketing communications, for the purposes of ensuring that we do not send such direct marketing to you again.

Financial

- To help us recover debts;
- To help us collect all subscriptions due and payable for the services rendered.

Operational & Customer Service

- To obtain a single view of a customer for all of *KARATIVE (PTY) LTD.*;
- To improve your customer experience;
- To help us improve the quality of our products and services;
- To provide you with the services, products or offerings you have requested, and to notify you about important changes to these services, products or offerings;
- To comply with your instructions or requests;
- For operational, marketing, auditing, legal and record-keeping requirements;
- To transfer or process your personal information outside of the Republic of South Africa to such countries that may not offer the same level of data protection as the Republic of South Africa, including for cloud storage purposes and the use of any of our websites. We will however only transfer your personal information across South African borders if the relevant situation requires trans-border processing and will do so only in accordance with Applicable Laws.
- To record, access and/or monitor your telephone calls and electronic communications to/with *KARATIVE (PTY) LTD.*, including all forms of notifications, correspondence received by or sent from *KARATIVE (PTY) LTD.* (including its employees, agents or

contractors) in order to accurately carry out your instructions and requests, to use as evidence and in the interests of crime prevention and to comply with Applicable Laws;

- In circumstances where we wish to protect our legitimate interest, where: we have exercised our right to terminate the agreement through a proper legal process as a result of default in respect of any of your obligations under an agreement;
- To disclose your personal information to third parties, including other *KARATIVE (PTY) LTD.* Entities, for reasons set out in this Statement or where it is not unlawful to do so;
- To conduct surveys; and
- To improve or evaluate the effectiveness of *KARATIVE (PTY) LTD.*'s business or products, services or offerings.

What should I do if my personal details change?

We strive to maintain the integrity and accuracy of your personal information at all times. You are responsible for informing us of any change in your details, such as a change of address. You have a right to ask us to correct any inaccuracies in the information we hold about you.

If your personal information changes at any time or our records appear to be incorrect, please inform us immediately so that we may update or correct our records accordingly. If you fail to keep your information updated, or if your information is incorrect, *KARATIVE (PTY) LTD.* may limit the products and services offered to you or elect not to provide any of these to you.

Can *KARATIVE (PTY) LTD.* contact me?

We (and these other parties) may contact you by post, telephone, e-mail, SMS and other electronic means, to inform you about services, products and offerings available from *KARATIVE (PTY) LTD.*, specific *KARATIVE (PTY) LTD.* Entities, the *KARATIVE (PTY) LTD.*, or selected third parties, which we believe may be of interest to you, unless you have unsubscribed from receiving such communications. We will only send you marketing communications if we are entitled to do so under Applicable Laws and where you have given us permission to do so.

Your participation is completely voluntary. You may unsubscribe or opt out from receiving such communications from *KARATIVE (PTY) LTD.* Entities by accessing your online customer profile by making use of the "Unsubscribe" option available on the relevant communication or by contacting 0827065475 or karatjbd@gmail.com at any time.

You may also contact us utilising the contact details set out in this Statement if you have previously asked not to receive marketing communications from us but would now like to hear from us with news on *KARATIVE (PTY) LTD.* and other associated products and services.

KNOW YOUR RIGHTS IN TERMS OF THIS POLICY

Having provided adequate proof of your identity, you have the right to:

- view, correct and/or amend your Personal Information we process. Please note that as a registered user, you can do this through your user account for the Personal Information reflected therein.
- request a record or description of your Personal Information. KARATIVE (Pty) Ltd. may charge a fee in order to provide you with this record of your Personal Information. Where requests to access and amend your Personal Information are manifestly unfounded, excessive or repetitive KARATIVE (Pty) Ltd. may charge an additional administrative fee or refuse the request.
- request to have your Personal Information corrected, destroyed or deleted. **Please note that you can stop being a registered user by cancelling your account. In this instance KARATIVE (Pty) Ltd. will retain your Personal Information subject to any legislative requirement and/or our internal retention policy.**
- us complying with your requests upon receipt unless we have credible reason why we cannot comply.
- us indicating where, if we cannot agree whether to correct or delete your Personal Information as requested, that a correction or deletion was requested but was not made.
- inform you if reasonably practicable, should we change your Personal Information and this has an impact on decisions about you.
- notify you of the action taken by us because of your request.
- notify you of unauthorised access to your Personal Information.
- provide you with reasonable evidence of our compliance with our obligations under this policy on reasonable notice and request.
- Submit a complaint to the Information Regulator.

As a registered user, you can exercise all your rights set out above in terms of POPIA by navigating to the profile section of your account on the web, where you will be required to confirm your identity via email verification.

You can further lodge a query/ complaint as set out above, by completing Annexure "A" below and submitting it via email to karatjbd@gmail.com.

HOW TO LODGE A COMPLAINT WITH THE INFORMATION REGULATOR

If you have any complaints about this Privacy Policy or our compliance with this Privacy Policy you can lodge a complaint with the Information Regulator. The contact details of the Information Regulator are available on its website at: https://justice.gov.za/inforeg/

This version of the Privacy Policy replaces any preceding privacy policy provisions on our website. We may occasionally update this Privacy Policy. When you use our Platforms the version of the Privacy Policy posted on this page applies to you.

PERSONAL INFORMATION REQUEST FORM / COMPLAINT FORM "ANNEXURE A"

PERSONAL INFORMATION REQUEST:

I, _____ (full names & ID number), hereby request the following personal information:

_____

_____

_____

_____

_____

_____

for the following reasons:

_____

_____

_____

_____

_____

and also, hereby indemnify KARATIVE (Pty) Ltd. from any legal or punitive action against it for reasons of disclosure of the above requested information, and I further acknowledge and affirm that I am legally and rightfully entitled to the requested information.

_____ _____

Signature of Requestee **Date & Place Signed**

_____ _____

Signature of Information Officer **Date & Place Signed**

after processing request

PRIVACY COMPLAINTS FORM:

I, _____ (full names & ID number), hereby wish to lodge the following privacy complaint in terms of the POPI Act and the Company's Privacy Policy:

_____

_____

_____

_____

_____

_____

further reasons for complaint(s), if any:

_____

_____

_____

_____

_____

and also, hereby acknowledge that KARATIVE (Pty) Ltd. will have to address the above complaints and concerns as per its timelines set out in its Privacy Policy.

_____ _____

Signature of Complainant **Date & Place Signed**

_____ _____

Signature of Information Officer **Date & Place Signed**

after processing complaint