General Information

The Capitalworks Group (or the 'Group') is committed to respecting and protecting your privacy. The Group takes care to use your information only for legitimate and specific business purposes. Our data protection framework relies on the following key principles:

- We respect the privacy rights of our employees, customers, investors and other contacts whose personal data we have and use;
- We obtain personal data fairly and transparently, and only use it for legitimate purposes;
- We have implemented appropriate technical and organisational measures to protect personal data;
- We hold ourselves accountable for demonstrating compliance with the data protection requirements where we operate.

These principles apply to all Group entities globally. They are based on internationally recognized privacy principles, which include the European Union's General Data Protection Regulation ("EU GDPR"), the United Kingdom's General Data Protection Regulation ("UK GDPR"), the Data Protection (Bailiwick of Guernsey) Law and the South African Protection of Personal Information Act ("POPIA"). Additionally, we take care to understand relevant laws and regulations that may apply in other jurisdictions in which we operate.

This Privacy Notice details the Group's data privacy principles and how it collects and processes personal data about you as well as explaining your rights and obligations. Processing will include all actions that can be performed on personal data such as collection, recording, organisation, structuring, storage, adaptation / alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Group is the 'controller' (EU/UK GDPR) or the 'responsible party' (POPIA) of the personal data you provide. Please read the following information carefully in order to understand the Group's practices in relation to the treatment of your personal data. Should you have any questions, please email the Group at [dataprivacy@capitalworksip.com].

What data privacy principles does the Group adhere to?

- The Group will process all personal data in a lawfully, fair and transparent manner;
- The Group will only collect personal data where it is necessary;
    - For the Group to provide a service to you;
    - For you to provide a service to the Group;
    - For the Group to keep you informed of its products and services; or
    - For the Group to comply with its legal and regulatory obligations.
- The personal data collected by the Group will be adequate, relevant and limited to what is necessary in relation to the specific purpose for which your data will be processed;
- The Group will take all reasonable steps to ensure that personal data is accurate and, where necessary, kept up to date;
- The Group will maintain personal data in a form that permits identification no longer than is necessary for the purposes for which the personal data has been collected for processing;

- The Group will hold and process personal data in a manner that ensures appropriate security;
- The Group will only share personal data where it is necessary to provide the agreed service or where it is necessary for the Group to comply with its legal and regulatory requirements; and
- The Group will only utilise a service provider outside of the Group for the processing of personal data where this is strictly necessary to facilitate our services to you or your service to the Group. In all cases, we will ensure service providers demonstrate compliance or certification to the relevant information security standards ahead of transferring any personal data.

What personal data does the Group collect and why?

In the course of providing products/services to you or vice versa, the Group may collect information that is considered personal data (e.g. name, contact details, address etc). We may also collect personal data when you enquire about our business (e.g. using the contact email address on our website), correspond with the Group, speak to or meet with Group representatives or employees, or otherwise interact with the Group.

Once you become a client, vendor or employee of the Group, we will require some personal information in order to verify your identity and have the applicable relationship with you. Some of this data may be required to satisfy legal obligations (e.g. to comply with obligations arising under the money laundering regulations) whereas other data may be required in connection with the provision of services to or from you. The data collected will vary depending on the service the Group provides to you or you provide to the Group, but typically includes:

	Personal Information	**Contact Information**
Employees	• Name • Date of birth • ID / passport number • Tax or national insurance number • Banking details • Qualifications • Other relevant KYC data	• Home address • Telephone number • Email address
Customers **Clients** **Vendors**	• Name • Position • Company • Relevant KYC documentation	• Company address • Telephone number • Email address

In the case of employees, it may be necessary for the Group to collect special personal information or children's data (e.g. for the purposes of the family medical cover). This data will only be collected and processed if the conditions within the relevant data protection legislation can be satisfied and there is a specific purpose / legitimate interest to collect the data.

The Group shall always obtain any required data directly from you, unless it is required by law to obtain the data from another source.

Where does the Group store personal data and how is it secured?

Most personal data collected by the Group is stored electronically. The Group has comprehensive technical and organisational procedures in place to ensure your personal data is kept safe and secure, with these including:

- Data encryption;
- Firewalls;
- Virus prevention & threat / intrusion detection;
- E-mail filters;
- Multi-factor authentication;
- Automated patch management;
- 24/7 physical protection of facilities where your data is stored (i.e. company offices or Microsoft's data centres);
- Controlled access to any physical onsite data storage facilities; and
- Security procedures across all service operations.

Where personal data is stored in hard copy, it is retained in secure environments where access is restricted based on the 'need to know' principle.

How long does the Group retain personal data?

The Group is required to maintain its books and records for a prescribed period (typically five years from either the ceasing of a business relationship, or, in the case of non-clients, from the making of a record – or alternatively, for seven years, where specifically requested to do so by the relevant regulatory authority). As such, information that falls in scope of either of these requirements is retained in line with the mandated timeframe.

Any information that is outside the scope of this requirement will be retained while relevant and useful, and destroyed where this ceases to be the case or where the individual or company specifically requests this.

What is the Group's policy on cross border transfers?

The Group will only transfer personal data to third countries, if:

- The recipient is subject to a law or binding corporate agreement which provides an adequate level of protection that effectively upholds principles for reasonable processing of the data that are substantially similar to the conditions for lawful processing under EU/UK GDPR or POPIA;
- The individual consents to the transfer;
- The transfer is necessary for the performance of a contract between the individual and the Group, or for the implementation of pre-contractual measures taken in response to the individuals request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Group and a third party;
- The transfer is for the benefit of the individual, and it is not reasonably practicable to obtain the consent of the individual but if it were, the individual would be likely to give it, or;
- The transfer is necessary to establish, make or defend a legal claim or for important reasons of public interest.

What legal basis does the Group rely on to process personal data?

We set out below the legal bases that we rely upon in order to process the personal data that we collect from you.

- **Consent**: where you have consented to our use of your information.
- **Contract performance**: where your information is necessary to enter into or perform our contract with you (or to take steps necessary or at your request before entering into such a contract).
- **Legal obligation**: where we need to use your information to comply with our legal and regulatory obligations.
- **Legitimate interests**: where we use your information to achieve a legitimate interest and our reasons for using it outweigh any prejudice to your data protection rights.
- **Legal claims**: where your information is necessary for the Group to defend, prosecute or make a claim against you, the Group or a third party.

Typically, the Group will reach out to you personally to confirm which legal basis is being relied upon to process your personal data; however, as a general rule the following is applicable:

- **Clients** – Information is processed on the basis of *contractual performance* and/or *legitimate interests* (where relevant);
- **Employees** – Information is processed on the basis of *contractual performance*, *legal obligation* and *legitimate interests* (for example, ensuring we recruit the appropriate employee);
- **Service providers** – Information is processed on the basis of *contractual performance*; and
- **Database/marketing contacts** – Information is processed on the basis of *legitimate interest*.

What are your rights?

Once you have provided your details to the Group, you have certain rights that apply, depending on your relationship with the Group, the information you have shared with the Group and the Group's legal and regulatory obligations.

- You have the right to request a copy of the information that we hold about you. If you would like a copy of some, or all, of your personal information, please email the Group at dataprivacy@capitalworksip.com. The Group will provide information for straightforward requests to you within one month at no cost to you. If the request is complex or excessive in nature, the Group will be able to extend the deadline by an additional two months and will inform you of the reasons why within a month. In this case, charges may apply.
- You have the right to request that the information the Group holds about you is erased under certain circumstances including where there is no additional legal and/or regulatory requirement for the Group to retain this information.
- As a client, you have the right to request that any information the Group holds about you be provided to another company in a commonly used and machine-readable format, otherwise known as 'data portability'.

- You have the right to ensure that your personal information is accurate and up to date, or where necessary rectified. Where you feel that your personal data is incorrect or inaccurate and should therefore be updated, please contact dataprivacy@capitalworksip.com.
- You have the right to object to your information being processed, for example for direct marketing purposes.
- You have the right to restrict the processing of your information, for example limiting the material that you receive or where your information is transferred.
- You have the right to object to any decisions based on the automated processing of your personal data, including profiling.
- You have the right to lodge a complaint with the local Information / Data Regulator if you are not happy with the way we manage or process personal data.

What is the Group's policy on cookie usage?

Cookies are small pieces of data, stored in text files on your device when websites are loaded into your browser. The Group's website uses two categories of cookies, namely *strictly necessary* cookies and *security* cookies. Strictly necessary cookies are essential for the website to perform its basic functions, in our case, to generate the company logo. Security cookies are there to help the Group identify and prevent security risks. Neither of these perform any user tracking, analytics or advertising and the Group does not collect any personal data through its use of cookies on its website. Personal data is only collected at the point when the user enquires about the Group using the email address on the "Contact" page of the website.

Will I be notified of changes to this policy?

The Group may, from time to time, review and update this policy. The Group will maintain the latest version of this policy on its website, and where the changes are deemed material, it will make you aware of these.

Who should I direct questions to?

If you have any questions, concerns or complaints about the practices contained within this document or how the Group handles your data, please email: dataprivacy@capitalworksip.com.