



Standard Bank (which also trades as Stanbic Bank) Human Capital (“**SBHC**”) is a division of a Standard Bank group company, which comprises the subsidiaries and their subsidiaries of Standard Bank Group Limited (“**Group**”).

This privacy statement applies to employees (which term includes permanent and temporary employees, interns, secondees and as the context may require, applicants and candidates for positions (together “you”, “your”)) of a Standard Bank Group company (“**we**”, “**us**”, “**our**”). It should be read together with the applicable privacy policy of that Group entity which will set out additional principles that apply when that Group entity processes your personal information.

This statement is addressed to all our employees. It provides an overview of:

- the categories of personal information that Group collects in relation to your employment or engagement with us;
- why and how we collect it;
- where we keep it;
- how we keep it secure;
- whether and under what circumstances we disclose it to any third parties;
- how long we keep your personal information; and
- your rights in respect of your personal information.

The information in this statement is not an exhaustive explanation but gives you an indication of what processing activities you can expect from us with regard to your personal information.

We will be the controller (also referred to as “responsible party”) of your personal information. This means that we are responsible for deciding how we hold and use personal information about you. We are required under data protection legislation to notify you of the information contained in this privacy statement.

We will comply with data protection laws. This says that the personal information we hold about you must be:

- Used lawfully, fairly and in a transparent way.
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes.
- Accurate and kept up to date.
- Kept only as long as necessary for the purposes we have told you about.
- Kept securely.

What is personal information, and what personal information do we collect, have or compile about you?

Personal information (also referred to as “personal data”) is information which identifies you as an individual, and includes:

- contact information (for example, your name, home and business addresses, telephone numbers, e-mail addresses and emergency contact information), date of birth, identity and passport documentation, marital status, bank account and tax information;
- recruitment information, educational information, current and previous employment related records such as your CV, credit record and fraud prevention checks, database registers for dishonest and/or dismissed employees (where applicable), public social media information, remuneration package and bonus information, employment start data, business unit and job title, staff number, education and training (for example, your education level, field and institution, professional licenses and certifications, training courses attended), offer letter and employment contract, employment history and reference letters and checks;
- employment information, your personal opinions for example as expressed in surveys or appraisals, performance objectives and reviews, performance and leadership ratings, awards, problem resolution (like disciplinary matters), expense claims, travel claims and time sheets, flexible working arrangements, holiday, sick leave and other leave balances, and periodic background checks for regulatory compliance or fraud prevention reasons;
- photographs and other visual images of you, for example when captured by office CCTV cameras;
- directorships and other financial interests or personal interests for financial regulatory compliance, anti-money laundering checks, conflict clearance or independent auditor requirements;
- personal information about your dependent family members such as their dates of birth and health related details if relevant for medical aid purposes (which is also classed as special personal information), and their financial interests if relevant for financial regulatory compliance, anti-money laundering checks or independent auditing purposes as well as for outside business interest declarations;
- records and recordings of your telephone conversations while using Group staff telephones or monitoring of activity while using Group email, Skype or other communications media in each case where we are entitled to monitor or record by applicable law; and

- Group equipment data that relates to you, such as computer serial number, facilities access and authentication information, telephone line detail, workstation detail.

We may also process “special category personal information” (also known as “sensitive personal data”) such as nationality, race, gender, sexual orientation, religion, political opinions, trade union membership, criminal records, biometric data, health and disability related information (for example, for medical aid purposes, or if you are disabled to assist in providing access to office premises) in each case where we are allowed or required to do so by applicable law.

The personal information mentioned above is not an exhaustive list, and we may update it for the legitimate business or legal purposes for which it is processed from time to time. If required by law, we will use reasonable endeavours to provide notice of material changes. We may process similar or related information depending on your role, position within, and circumstances while employed or engaged by us.

Where you provide us with information about a third party (such as your next of kin) you must obtain their permission to this disclosure and bring this notice to their attention.

Why do we need to process your personal information?

We will only use your personal information when the law allows us to. Most commonly, we will use your personal information in the following circumstances:

- Where we need to enter into or perform a contract with you including pre-engagement verification and background checks and the payment and administration of any benefits. We may ask you to provide and we may process the personal details of your dependents for the purposes of administering relevant benefits.
- Where we need to comply with a legal obligation, including disability discrimination, equal opportunities and health and safety legislation.
- Where it is necessary for legitimate interests pursued by us or a third party and your interests and fundamental rights do not override those interests. We may use your personal information for employment administration and for strategic and organisational planning and management of our workforce generally. We will engage with governmental, social and industry bodies on various initiatives from time to time and conduct ongoing research and voluntary staff engagements. Other members of the Group support our employees' choices to undergo further formal education. This requires research and analytics as approved by us that comply with the Groups policies and law.

We may also use your personal information in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests). We need contact details for your next of kin for use in emergencies.
- Where it is needed in the public interest, or for official purposes.

We may process special category personal information about you for statistical purposes, or where strictly necessary for purposes related to your employment or applicable legislation. We limit access to this information to those who need to access it, and where possible remove all personal identifiers from such information. We may use this information to bring or defend legal claims.

How do we obtain your personal information?

Most of the personal information we have about you is, or was provided by you during your recruitment and on-boarding process or the course of your engagement with us, for example: by completing your working hours in which you indicate when you are on holiday, or where you were or are away from work due to illness.

Other personal information about you, such as information about your performance is compiled on an ongoing basis, in particular as part of any annual appraisal.

The position you apply for with us as a financial institution requires honesty and integrity. Where permitted by law, we may use third parties to perform risk, integrity, regulatory and related background screening checks. The content of the background check information varies by country to comply with local requirements but may include information gathered from publicly available sources and from other sources such as your former employers or colleagues, schools you have attended, academic qualification registers, credit reporting agencies and criminal records databases. These types of information will be collected with your prior knowledge, and you will receive information about the nature of such a background check before it begins.

Monitoring of electronic communications

We communicate with you through different methods and channels. If allowed by law, we may record and monitor electronic communications to make sure that they comply with our legal and regulatory responsibilities and internal policies.

Where do we keep your personal information?

Most of the personal information about the employees of Group companies is held by SBHC. Employees can view certain types of their own information via the Human Capital management systems or applicant profiles created in the Careers Portal.

Employees are encouraged to regularly update the personal information we have on record through the approved mechanisms. In situations where information cannot be viewed and updated by yourself, you should request assistance from the relevant SBHC representative assigned to your business area.

Other electronic systems and databases are also used to process your personal information for the purposes of administering your employment related activities. All such systems and databases only collect, receive, use and share your personal information in accordance with, and as permitted by applicable laws, Group policies, standards and processes.

Personal information contained in hard copy (paper) format is kept secure and safe and certain information may be made available to you upon request to the SBHC Shared Services department. Such hard copy information may include your CV (as applicant), Letter of Employment (as employee) and such other employment records as Group is required to keep.

Where employee personal information is retained in hard copy (paper) format it is kept secure and safe in locked secure storage.

How do we keep your personal information secure?

We use appropriate technical and organisational measures to keep your personal information secure taking into account, amongst other things, the sensitivity of the personal information, the number of employees whose personal information we collect and process, the technologies available to secure it and their cost.

Our security systems are designed to prevent loss, unauthorised destruction, damage and/or access to your personal information from unauthorised third parties.

All our Group offices are equipped with certain physical access / security systems including secure entry systems and auto-lock door mechanisms, alarm and CCTV systems.

All staff within those offices are subject to our standard take on and vetting processes and have contracts obliging them to keep our information confidential and restricting their use of that information.

All staff are further obliged to adhere to comprehensive written policies and procedures and undertake regular and ongoing training. These address, amongst other things, our clear desk policies, screen locking, use of own devices, disposal of confidential waste, encryption of data, and the use of passwords on the systems they use. Certain staff also have assigned roles and responsibilities to help ensure the security and integrity of our information. We restrict access to our IT systems to those personnel that require it in the performance of their role(s) and where possible endeavour to anonymise the personal information held.

Our IT systems are inherently designed and regularly updated to try to ensure they remain as secure as possible. We use secure servers, firewalls, virus and ransom scanning software, and employ a team of IT professionals to support these systems.

We have a framework in place for undertaking data protection impact assessments whenever a proposed new project or initiative involving our use of personal information is likely to result in a high risk to the individuals whose personal information is affected and in order to identify, manage and address any privacy risks posed.

Who do we disclose your personal information to and why?

Group entities or affiliates and clients:

Group comprises of different member entities or affiliates located in different areas throughout the world. To the extent that another member entity or affiliate reasonably requires us to provide personal information about you, we may do so, but such disclosure will normally be one of which you are aware, for example, where your professional services are required by an engagement team from another member entity or affiliate.

Outsourced service providers:

Where we have business operations that are supported by other organisations, we need to share certain personal information with them for the purposes of the services that they provide. Some service providers may be located in countries different to yours.

We have agreements in place with such third parties which require them to protect personal information in accordance with applicable laws, rules and regulations.

Law enforcement agencies and tax authorities:

Where obliged by law to do so, we may disclose your personal information to law enforcement and revenue agencies and their officers and agents. To the extent required by law, we will inform you of such disclosures.

Safeguards when we share your personal information

When we do share personal information with a data processor then we ensure we have a lawful basis for doing so, have a formal vetting procedure that we follow to assess that data processor's ability to look after any personal information shared with them, ensure we have a written contract in place with them to apply appropriate safeguards to protect personal information to a standard and in a manner that provides us with sufficient guarantees as to the security of that personal information, and undertake ongoing monitoring of that relationship.

When we share personal information with another third party but not to process that personal information on our behalf then we ensure we have a lawful basis for doing so, have a formal procedure that we follow to consider and approve the transfer beforehand, and we follow best practice guidelines to govern the data privacy elements of the relationship whenever that is possible.

Transferring your personal information cross border

We may need to transfer the personal information we collect about you to other countries in order to perform our contract with you, comply with our regulatory obligations, manage the business of the Group companies or in other circumstances that are permitted by law. Certain international transfers of personal data may be restricted by applicable legal rules, for example, transfers may only be made from the European Economic Area (“**EEA**”) in certain situations. It is possible that we may need to transfer your personal data to a country that is not considered by an applicable regulatory body to provide an adequate level of protection for personal data. Where this is the case, we will put in place an appropriate measure to comply with applicable law. At the date of this notice, the Group uses standard contractual terms in a form approved by the EU Commission to protect personal data being transferred from the EEA.

How long we keep your personal information for

We only hold personal information in a format which permits your identification for as long as is necessary for the purposes for which it was obtained.

Where legal requirements oblige us to retain records for a particular period of time then those periods are the minimum period for which we will retain the relevant record.

Each member of the Group has record retention and disposal policies for all of the different types of records that it holds. The versions applicable to you are available on request from the relevant structure within each Group member. Guidance can be obtained from your compliance department.

Your rights

You have a number of rights in respect to your personal information:

- You have a right of access to your personal information;
- You have a right to take action to rectify inaccurate personal information;
- You have a right to erase personal information;
- You have a right to restrict the processing of your personal information;
- You have a right to data portability;
- You have a right to object to processing of personal information (including direct marketing);
- You have a right not to be subject to a decision based solely on automated processing of your personal information, including profiling, which produces legal effects / significantly affects you;
- You have a right to seek compensation for any material or non-material damage caused by a breach of our statutory obligations to look after your personal information;
- You have a right to lodge a complaint with a data protection supervisory authority; and
- You have a right to an effective judicial remedy against us.

In certain circumstances, we may not be able to process any of your above-mentioned requests, namely:

- if we have compelling legitimate grounds for the processing of the personal information;
- for the establishment, exercise or defence of a legal claim;
- for public interest;
- for compliance with our legal obligation/duty; and
- for our legitimate interest.

Legal disclaimer

We reserve the right to disclose your personal information if required by law

Automated decision making

We, at times, utilise automated processes to generate a profile and/or make decisions about you based on your personal information, in example, for the purposes of determining whether an applicant meets the minimum qualifications or criteria for a job application. These decisions are not derived solely via automated means, and elements of human intervention and supervision are applied to all automated processes to ensure that your best interests are always taken into consideration.

Access to information

You have rights to access certain information relating to you held by us.

As a prospective employee you may access the information which you have provided to us as part of your job application process by logging onto the profile which you created on the Careers portal.

As an employee you can access your information through existing processes within the Group. Please contact your local Data Protection Officer or Data Privacy Office for further information on how to access your information.

Changes to our Privacy Statement

Any changes we may make to our Privacy Statement in the future will be posted on this page. The latest version of our Privacy Statement will replace all earlier versions of it, unless stated differently. We will notify you of material changes to this Privacy Statement.

Queries and complaints

If you have any queries or complaints about privacy, please contact the Group Privacy Officer.

Jan Bezuidenhout

Group Privacy Officer

Postal Address: The Standard Bank of South Africa Limited

P O Box 1155

Johannesburg, 2000

Physical address:

Standard Bank Centre

5 Simmonds Street

Johannesburg, 2001

Telephone: +27 11 636 1781

Fax: +27 11 631 8580

Email: info.officer@standardbank.co.za

¹ Subsidiaries and associate companies

Diners Club (S.A.) (Pty) Ltd, Standard Bank Financial Services Holdings (Pty) Ltd, Standard Offshore Finance Company (Pty) Ltd, Melville Douglas Investment Management (Pty) Ltd, FHPManagers (Pty) Ltd, Standard Trust Limited, Standard Insurance Limited, Stanhold Investments (Pty) Ltd, Greenfield Newgate (Pty) Ltd, The Unisec Group Limited, Standard Bank Properties (Pty) Ltd, Blue Waves Properties 78 (Pty) Ltd, SBG Securities (Pty) Ltd, Stanbic Africa Holdings Ltd.