Standard Advisory London Limited
Staff Privacy Statement

Purpose of this Privacy Notice

Standard Advisory London Limited ("**SALL**" or "**we**") recognises its obligations to process personal data in accordance with all relevant laws. This notice sets out how we will hold and use your personal data.

Where you provide SALL with personal data relating to any other person (for example, a spouse), you represent that this information is accurate, that you have the consent of that person to provide the information to us and that you will provide that person with the current version of this privacy notice.

We need to collect, process, use, share and store personal data about you in order to perform any agreement we have with you and meet our legal and regulatory obligations. It also explains how we share personal data with our parent company, Standard Bank Group Limited, and its subsidiaries (together the "**SB Group**").

Data Protection Principles

We will comply with data protection law in relation to your personal data. Your personal data means any information relating to you as an individual.

Data protection law says that the personal data 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.

For the purposes of this Privacy Statement "**staff**" is to be given its widest possible interpretation and includes, but is not limited to, any person being a past, present or prospective employee (with a contract of employment) or consultant (with a contract for services or working pursuant to such a contract with a consultancy practice) with SALL, regardless of where situated and whether undertaking voluntary or paid work. Staff also includes any past, present or prospective person on secondment or work experience or as part of an internship programme with SALL and regardless of whether these arrangements are undertaken voluntarily or are paid.

This Privacy Statement should be read together with the Standard International Data Privacy Policy which sets out the principles we apply when we process personal information.

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

We may obtain personal data about you where you provide this to us or we obtain it from third parties. These third parties may include former employers, educational institutions, credit reference and fraud prevention agencies. Personal data may also come from your dealings with the SB Group or third parties and may include information learned from performing an agreement with you.

We will typically collect and use the following personal data:

- your name, gender, date and place of birth, occupation and income, employment history, marital status and dependents.
- your contact information: your name (and any previous names), your home and/or business address, your telephone numbers, your e-mail addresses, emergency contact information and any other contact information we reasonably require.
- your identification and background data including passport, work permit status and documentation, bank account and tax information.
- your banking details, national insurance/social security numbers, pension details and details of emoluments and deductions for payroll purposes.
- some special category / sensitive personal information such as your ethnic origin, race, criminal behaviour, health and disability related information.

- your recruitment information, current and previous employment or directorships and any related records such as your CV, criminal and credit record checks, public social media information, remuneration package and bonus information, employment start data, business unit and job title, staff number, education and training data (such as 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, your personal opinions (such as your views or preferences) or opinions or views about you, 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.
- your financial interests if relevant for personal account trading declarations, outside business interests declarations, politically exposed person status and/or auditor independence.
- personal information about your dependent family members such as their names, dates of birth and health related details if relevant for medical aid or benefit purposes, and their financial interests if relevant for personal account trading declarations, outside business interests declarations, politically exposed person status and/or auditor independence purposes.
- photographs or other visual images of you including from CCTV footage.
- records and recordings of your telephone conversations while using SB Group staff telephones.
- business data such as computer serial number, facilities access and authentication information, telephone line detail, workstation detail, and desk number to mention a few.

Why we use your personal information?

As staff, we collect and use your personal information primarily:

- as is necessary for the performance of, or to take steps on your behalf and at your request to enter you into, the contract that you are, or will be, party to with SALL as staff;

- in the administration of your remuneration and arranging and administering your other employment benefits;

- verify your identity and carry out background checks;

- to ensure we comply with any applicable employment or other relevant laws (for example, disability discrimination, equal opportunities legislation and financial regulatory legislation) that we are subject to as regards our engaging you;

- enforce our rights and protect against harm to our property and interests and allow other members of the SB Group to do the same;

- prevent and detect crime, including fraud, money laundering and identity theft;

- carry out the management of the SB Group (including insurance, risk management, credit management and audit); and/or

- otherwise where it is necessary for the legitimate interests of the SB Group (or those of a third party) and your interests and fundamental rights do not override those interests.

Should you have any dependents that may be eligible to benefit from your employment benefits, we may need you to provide the relevant personal details of such dependents for the purposes of arranging and administering such benefits. Failing to provide this information may result in our being unable to extend those benefits to your dependants.

Where our collecting and processing your personal data is not pursuant to your contract nor to ensure we comply with any particular legal obligation then we will only collect and process your personal information:

- if it is in your vital interests for us to do so (for example, in an emergency situation where physical harm may otherwise result); or

- where (a) the personal information is not sensitive / special category information, (b) we or a third party, have a legitimate interest in using it, (c) after considering your personal fundamental rights and freedoms, we do not determine that legitimate interest is, on balance, overridden by those rights and freedoms, and (d) in undertaking that balancing exercise we have taken into consideration your reasonable expectations as to what the information might be used for based upon your relationship with us. For example, as your employer we may use your personal information for strategic and organisational planning and management of our workforce generally or we may engage with governmental, social and industry bodies on

various initiatives from time to time and conduct ongoing research and voluntary employee engagements, or use it for security or training and monitoring purposes; or

- where the personal information is special category / sensitive information and our processing is necessary to exercise, bring or defend a legal claim.

In some circumstances, we may seek and obtain your explicit consent to our collecting and using your personal information. This is rare and will usually only be relied upon if we are processing certain special category / sensitive personal information, in which case we will fully inform you of what we plan on doing with the information and you will then be asked to consent to our processing this information and have the right to withdraw that consent at any time.

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 during the course of your employment 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 during the course of your employment and particularly as part of the annual performance appraisal process in which you take part.

Your role in SALL requires honesty and integrity in all of your dealings. To help us to determine this we may ask you to provide us with referees and with your permission may contact those to obtain references on your behalf, we may also contract with a third party to perform risk, integrity, regulatory and related background screening checks. The content of the background check information varies with local requirements, but may include information gathered from publicly available sources, where lawful and reasonable, from other sources such as your former employers or colleagues, schools you have attended, academic qualification registers, credit reporting agencies and criminal records databases. This type of information will be collected with your prior consent, 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 staff is held by SB Group Human Capital and can be viewed and accessed by employees via the Human Capital management system or your applicant profile created in the Human Capital portal (Peoplefluent (performance, reward and training)) and Finance (Concur (expenses)), as the case may be.

Employees are encouraged to regularly check and update the personal information SB Group Human Capital has on record through the approved mechanisms. In situations where information cannot be viewed and updated by yourself, you should request assistance from the relevant SB Group Human Capital 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, or internal business policies, standards and processes applicable to SALL.

Where staff 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 staff whose personal information we collect and process, the technologies available to secure it and their cost.

These measures are specifically designed and updated to prevent unauthorised access to / processing of your personal information and/or its accidental loss, destruction or damage. A general description of some of these security measures are set out below.

SALL's 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 – including Compliance and the Standard International Data Privacy team. We restrict access to information to those personnel that require it 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.

Who do we disclose it to and why?

We maintain comprehensive and detailed registers of all the 3rd parties with whom we share staff personal information that we are responsible for. These registers include information on 3rd party service providers and also 3rd parties we may otherwise share personal information with. They also include information regarding the countries / territories in which those organisations are based.

Where we share staff personal information it is usually only with other organisations in countries / territories in which the SB Group companies are themselves based and/or certain other countries / territories that have been granted EU adequacy rulings from a data protection perspective (if different).

The only 3rd country to which we routinely transfer certain staff personal information is to South Africa for payroll processing (internally within the wider SB Group of companies) and talent management assessment purposes (to external 3rd party assessment services providers).

Where we outsource work to be undertaken on our behalf we ensure we are provided with sufficient guarantees as to the safeguarding of the information we provide to those service providers before we provide any information to them. We follow a strict vetting process which involves undertaking data protection due diligence on the counterparty supplier, ensuring we put in place appropriate EU model clauses processing agreements with those counterparties, and monitor those relationships on a systematic and ongoing basis. In other circumstances where we are obliged to, or otherwise share personal data we have an approval process for doing so and will, where possible, endeavour to use an appropriate EU model clauses transfer agreement.

The following provides a general summary of our register information in terms of where we presently or may share staff personal information.

Standard Bank Group

To the extent that we need to send your personal information to another company in the wider SB Group (which comprises companies in different areas throughout the world), such as we mentioned previously for payroll processing to South Africa, or where a company in the wider group reasonably requires us to provide personal information about you, we will make this known to you at the time we consider doing so, for example where your professional services are required by an engagement team from another member company in the wider SB Group and will only share your information where we are legally entitled to do so and on the basis we have satisfied ourselves that appropriate safeguards are in place to protect the personal information to be transferred.

Outsourced service providers:

Where we have business operations that are supported by other external organisations, we may need to share certain staff personal information with them for the purposes of the services that they provide. These service providers are either based in the European Economic Area or other countries with EU adequacy rulings from a data protection perspective or in South Africa.

We vet such external organisations from a data protection perspective, have agreements in place with such third parties which require 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 monitor those relationships on an ongoing basis.

Law enforcement agencies and tax authorities:

Where obliged by law to do so, we may disclose your personal information to law enforcement agencies and / or tax or revenue authorities.

The periods for which we store your personal information

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.

SALL maintains comprehensive record retention and disposal policies for all of the different types of records we hold, including staff records.

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.

Our staff / employment record retention and disposal policies applicable to SALL are available on the SALL Intranet.

Your rights in respect to your personal information and how you can exercise those rights

If you have any questions about this privacy notice, how we handle your personal data or if you wish to exercise any of your legal rights or other rights under this privacy notice, please contact dataprivacy@standardsbg.com.

You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues. You can find out more about your rights in relation to your personal data at www.ico.org.uk.

You have rights to obtain a copy of your personal data and in certain situations to obtain correction, erasure and restriction of processing of your personal data. You have a right of data portability.

Where processing is based on your consent you have a right to withdraw this at any time. You can ask us to stop or start sending you marketing messages at any time by contacting us at dataprivacy@standardsbg.com.

Changes to our Privacy Statement

We may change this notice from time to time. Where we make material changes we will notify these to you. All updates will be published at:

https://corporateandinvestment.standardbank.com/CIB/Country-profiles/Europe-&-Asia-Pacific/United-Kingdom.

Please check this address regularly

Contact

Any queries or concerns about this Privacy Statement should please be made in writing and addressed to dataprivacy@standardsbg.com whose contact details are set out in this Privacy Statement.