OVERSEAS
TRUST & PENSION

Data Protection Policy for Protecting Personal Information

At Overseas Trust and Pension Limited (OTAP) we value the trust our clients and employees place in us when they share their **personal information** with us.

Without this data, we would not be able to function effectively, so it is crucial that we protect it in accordance with the guidelines set out in the Protection of Personal Information Act 2013 (POPIA) and the Data Protection (Bailiwick of Guernsey) Law, 2017.

This sentiment aligns with the core **values** of our business being INTEGRITY, ACCOUNTABILITY, TEAMWORK and GROWTH. This policy will give you more information about how we do that.

TABLE OF CONTENTS

1. WHY WE HAVE THIS POLICY

We have this policy to help guide our actions so that we keep our customer and employee data safe, protect our reputation, and comply with all relevant data protection regulations, including the Protection of Personal Information Act 2013 (POPIA) and principles of the Data Protection (Bailiwick of Guernsey) Law, 2017. We base our principles on the ethos of ethics and integrity in all that we do at OTAP and align ourselves constantly to Treating Customers Fairly.

OTAP as a registered Financial Services Provider registered with the FSCA in South Africa, 47261, and a licensed company by the Guernsey Financial Services Commission, registration number 55506, is obligated to comply with the Protection of Personal Information Act 4 of 2013 and the Data Protection (Bailiwick of Guernsey) Law 2017. POPIA and DPL requires OTAP to inform their clients, employees and stakeholders as to the manner in which their personal information is used, disclosed and destroyed. OTAP is committed to protecting the privacy of the data we hold ensuring that the personal information is used appropriately, transparently, securely and in accordance with all applicable laws.

2. SCOPE OF THIS POLICY

This policy applies to:

- any activity where we produce or use personal information (processing activities);
- anybody involved in processing activities where we produce or use personal information; and
- all employees, service providers, contractors, and other individuals who have access to personal information.

3. WHY IT IS IMPORTANT TO COMPLY WITH THIS POLICY

The legal duty to comply with POPI's provisions is activated in any situation where there is:

"A processing of personal information entered into a record by or for a responsible person who is domiciled in South Africa"

" The data protection principles sit at the core of the compliance requirements of the Law. They set out how personal data must be handled, ensuring that individuals rights are respected."

It is imperative to comply with the provisions, rules and regulations under which we are governed to protect all involved parties from the risk associated with breaching data records. It is important to understand the consequences of failure to comply and be aware of the reputational damage it could cause, financial losses and the administrative penalties it can bring if non-compliance should occur. OTAP has stringent policies, procedures and controls in place to ensure, to the best of its ability, that non-compliance should not occur.

3.1 IF THE ORGANISATION DOES NOT COMPLY

Our reputation is our biggest asset. Without our reputation, our relationships with key stakeholders would suffer and we could lose clients, prospective clients, and top-class candidates. In addition, we could face substantial fines.

3.2 IF YOU DO NOT COMPLY – EMPLOYEES OF OTAP

This company only works when we all do our part, and none of us want to see the company suffer. If you do not comply with this policy, or if you discover that we are not complying with the policy and you do not tell us about it, you could face disciplinary action.

4. OUR POLICY

While all **personal information** should be protected, we take a risk-based approach to compliance. We prioritise the protection of personal information that is used in our important business activities, and in activities that could have a substantial impact on an individual's right to privacy.

Our general approach to risk management is set out in the following key documents:

- AML and CTF Manual
- Compliance Manual
- Compliance Monitoring Programme

It is our policy to:

- follow the principles of privacy protection that are set out in the **POPIA and Data Protection Law (DPL)**
- conduct data protection impact assessments
- ensure we adhere to our risk based approach
- ensure we adhere to our Privacy Statement

4.1 WE FOLLOW THE PRINCIPLES OF PRIVACY PROTECTION

For clarification of the processes below, please refer to Appendix 1 on page 12 of this document***

WHAT THE POPIA SAYS	WHAT WE DO
Classify personal information	We must identify and classify the personal information that we use and produce.
Document processing activities	We document all processing activities to ensure that we can respond to requests from the Information Regulator and requests for information by data subjects or authorised third parties.

WHAT THE POPIA SAYS	WHAT WE DO
Specify the purpose for processing	We specify and document the purposes for which we process personal information. We collect data for specific, explicit and legitimate purposes and do not further process it in a manner which is incompatible with the original purpose. Data is processed for the purpose of complying with regulatory responsibility; to proceed into a contract with the data subject; where a data subject has opted to received further information from us. This is found in our privacy statement.
Provide legal basis for processing activities	**We ensure that:** • all processing activities have a legal basis in that the data we process is required to ensure we comply with regulatory responsibility, specifically to Know Your Client and AML/CTF requirements; and • we document the specific legal basis for processing personal information for each activity.
Keep processing to a minimum	**We ensure that:** • we process personal information that is adequate, relevant, and not excessive, considering the purpose of the activity; • we de-identify personal information before we start the activity where possible. Where de-identification is not possible, we must consider masking the personal information.
Obtain personal information from lawful sources	We obtain personal information from lawful sources only. Lawful sources of personal information include: • the data subject; • information that the data subject made public deliberately; • public records; and • a source that the data subject consented to. Other sources may be lawful in special circumstances. If you are unsure, speak to the Information Officer.
Process transparently	We disclose all processing activities to data subjects in our privacy notices.
Ensure personal information quality	We take reasonable steps to ensure that personal information is complete, accurate, not misleading, and updated when necessary.

WHAT THE POPIA SAYS	WHAT WE DO
Limit sharing	We only share personal information if it is legal to do so and ethically justifiable. We: • identify all instances when personal information is shared with external organisations or individuals (third parties); • ensure that sharing personal information complies with data protection legislation and the Information Sharing Procedure; • enter into appropriate contracts and take additional steps that may be necessary to reduce the risk created by sharing personal information; • conduct an information sharing assessment to determine who is responsible to ensure that contracts are concluded, who must review the contracts, and whether we must take additional steps to reduce the risks created by sharing; • keep a record of personal information sharing activities, including the outcome of assessments, a record of additional steps taken, what personal information was shared and when, and the method we used to share the personal information.
Keep personal information secure	We protect all personal information that we use against breaches of confidentiality, failures of integrity, or interruptions to the availability of that information. All personal information processing must comply with our Privacy Statement.
Manage personal information incidents	You must report incidents in accordance with our Data Breaches Policy An incident includes: • non-compliance with this policy and any procedures that relate to it; • contraventions of any data protection legislation such as the POPIA; and • security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information. You must report an incident within 24 hours of becoming aware of an incident that has already occurred, suspect that an incident has occurred or may occur in future, or are aware of circumstances that increase the risk of an incident occurring as per our PP&C's.
Manage retention periods	**We ensure that all records:** • are managed appropriately and in accordance with any operational or legal rules that may apply; and • comply with the regulations under which we are governed. • Are managed in accordance with our Data Retention policy

WHAT THE POPIA SAYS	WHAT WE DO
Respect data subjects' rights	**We respect the rights of data subjects to:** • access their data; • know who their information was shared with; • correct or delete inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or illegally obtained information; • withdraw consent; and • object to the processing of their information when it is not necessary for the conclusion or performance of a contract or to comply with an obligation imposed by law. All data subject requests must go through the Data Subject Request Procedure.

4.2 WE CONDUCT DATA PROTECTION IMPACT ASSESSMENTS

Compliance and senior management must ensure that a data protection impact assessment is done before we start a new **processing activity**. The data protection impact assessment must include a risk analysis of the activity.

A data protection impact assessment is to ensure we understand what data we collect, what we do with that data, how we process that data, how we store that data and how we destroy that data and the impact it has on the business from a risk perspective.

We must conduct a data protection impact assessment before we:

- continue to process **personal information** as part of an activity that has not undergone a data protection impact assessment before;
- change an existing processing activity;
- launch a new product or service;
- expand into other countries;
- use new systems or software for **processing** personal information; or
- share personal information with third parties.

A data protection impact assessment has three phases:

- Identify activities in which personal information is processed.
- Complete the data protection impact assessment questionnaire to document the activity, classify information, and perform a risk-rating for the activity.
- Complete a further investigation and assessment with assistance from the **Compliance and IT teams** if the activity had a risk rating of high or critical after the data protection impact assessment questionnaire was completed.

All activities that are rated as critical or high risk during the data protection impact assessment must undergo an assessment every three years.

5. ROLES AND RESPONSIBILITIES

This policy establishes a sustainable model for data protection. While the POPIA Programme Team is responsible for the development of data protection policies and procedures, Senior Management is responsible for the implementation of policies in their business areas.

These are the responsibilities in respect of this policy:

ROLE	RESPONSIBILITY
The Information Officer (IO)	The IO is the custodian of all our information. The IO has a co-ordinating function that focuses on the policy-based protection of personal information. **The IO must:** • ensure compliance with this policy; • respond to all data subject requests and objections; • respond to requests from the Information regulator when there is an investigation; • create an environment where managing personal information and data protection risks is accepted as part of the responsibilities of Senior Management; • provide or obtain advice on compliance with the POPIA and any other applicable regulations. • consider the results of data protection impact assessments to identify and develop plans to mitigate organisation wide data protection risks • assign responsibility for personal information assets when it is not clear who owns the asset • identify new opportunities and improve business processes for better data protection and business outcomes • receive and manage reports of incidents and audit findings • monitor POPI compliance
The Compliance Team	The Compliance Team supports the IO by supporting the implementation of this policy. The IO and the Compliance Team must: • record, rate, and manage organisation-wide data protection risks in accordance with the Company policies; • advise [Senior Management] on the implementation of this policy; • review and update this policy and its supporting documents to ensure that it reflects established frameworks, best practices, and current regulations in data protection; • evaluate the implementation of this policy in business areas when requested; • monitor incidents and amend this policy to prevent future incidents; • conduct data protection impact assessments when requested by [Senior Management]; • assist the IO in investigations of organisation-wide data protection risks;

ROLE	RESPONSIBILITY
Senior Management	They must monitor and advocate for compliance within their business areas. **They must ensure that:** • their business areas comply with this policy; • personal information that is used in processing activities remains protected
Users of personal information	**All users who have access to the organisation's information or information systems must:** • adhere to all policies, procedures, and guidelines that relate to the processing of personal information; and • report any actual or suspected incidents.

6. OUR POLICY GLOSSARY

WHAT WE SAY	WHAT WE MEAN
Data subjects	The person or organisation to whom personal information relates. This includes: • individual members of pension plans; • staff members and job applicants; • service providers, contractors, and suppliers; • shareholders and directors; and • members of the public and visitors.
DPL	• The Data Protection (Bailiwick of Guernsey) Law 2017
Incident	**An incident includes:** • non-compliance with this policy and any procedures relating to it; • contraventions of any data protection legislation such as the POPIA or DPL; and • security incidents such as breaches of confidentiality, failures of integrity, or interruptions to the availability of personal information.
Processing activities	Processing activities are a collection of interrelated work tasks that achieve a specific result during which personal information is created, collected, used, shared, transformed, stored, or destroyed. A processing activity is important if we could experience critical or high levels of risk if the process or activity is disrupted or could no longer continue.

WHAT WE SAY	WHAT WE MEAN
Personal information	Personal information means any information relating to an identifiable individual (living or deceased) or an existing organisation (a company, public body, etc.). This includes the personal information of all customers, staff members, job applicants, shareholders, board members, service providers, contractors, suppliers, members of the public, and visitors. Examples include: • identifiers, such as a name, identity number, staff number, account number, customer number, company registration number, tax number, photos, videos, or any other unique information that can be used to identify a person; • demographic information, such as race, gender, sex, pregnancy, marital status, national or ethnic or social origin, colour, sexual orientation, age, religion, conscience, belief, culture, language, and birth; • information relating to physical or mental health, wellbeing, or disability; • background information, such as education, financial, employment, medical, criminal or credit history; • contact details, such as physical and postal address, email address, telephone number, online identifier (e.g. a person's twitter handle) or location information; • biometric information: this refers to techniques of identification that are based on physical, physiological, or behavioural characterisation, such as blood-typing, fingerprinting, DNA analysis, retinal scanning, facial recognition, and voice recognition; • someone's opinions, views, and preferences; • private or confidential correspondence and any further correspondence that would reveal the contents of the original correspondence; • views or opinions about a person, such as interview notes and trade references; and • the criminal behaviour of a data subject to the extent that such information relates to the alleged commission by a data subject of any offence; or any proceedings in respect of any offence allegedly committed by a data subject.
POPIA	The Protection of Personal Information Act 4 of 2013 and its regulations.
POPIA Programme	The POPIA Programme is our ongoing efforts to comply with the provisions of the POPIA and includes: • stakeholder consultation; • defining roles and responsibilities; • policy development; • policy implementation; • monitoring and audit; and • continual improvement.

WHAT WE SAY	WHAT WE MEAN
Processing	Any operation or activity or any set of operations concerning personal information, including: • collecting, receiving, recording, organising, collating, storing, updating or modifying, retrieving, altering, consulting, or using; • disseminating by means of transmission, distributing, or making available in any other form; or • merging, linking, restricting, degrading, erasing, or destroying information.

7. SUPPORTING DOCUMENTS

You must read this policy with:

- OTAP Privacy Statement
- Data Subject Access Request Procedure (reference #1513167)

8. CONTACT

If you need to contact OTAP with regards to your personal information, please email our IO, Candice Price, on **compliance@trustandpension.com**.

9. DOCUMENT METADATA

Document Number:	1
Document Version:	2
Document Approval Authority	Board of Directors of OTAP
Document Approval Date	29.06.2021
Document Owner	Candice Price
Document Author(s)	Candice Price
Last Updated	12.07.2021
Next Review Date	
Visibility (where will it be displayed):	Website and internal Policy and Procedure Files

Appendix 1 - Data Subjects

OVERSEAS TRUST & PENSION

Data subject type	Personal Information held by OTAP	Processing activities	Purpose of processing	Legal Basis *** see explanation below	Minimise Processing	Source of Data	Processing transparency	Data Quality	Limit sharing	Secure Data	Manage Incidents	Data subject access rights
Member of Multi member scheme	• Name • Address • DoB • Employment history • Income • Bank account details	• New Business App • Contributions • Investment • Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Contractual • Consent	• App forms and data fields limited to only those data items needed to fulfil service.	• Direct from Member in form of App & CDD forms	• Disclosed by Privacy statement	• Increasingly introducing checks for completeness of data	• AML Purposes: • Dow Jones • Investment houses • Appointed IFA	• Access to premises and systems limited by door codes / cards and passwords. Network access overseen by IT provider.	• Policy and procedures for reporting	• DSAR available if requested
Death Beneficiary of Multi-member Scheme	• Name • Address • DoB • Employment history • Income • Bank account details	• New Business App • Contributions • Investment • Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Vital • Legitimate	• DD not collected until benefit payment being contemplated	• Name and contact details from Member • Post member death, direct AML information from beneficiary						
Member of Corporate Scheme	• Name • Address • DoB • Employment history • Income • Bank account details	• Contributions • Investment • Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Contractual • Consent	• App forms and data fields limited to only those data items needed to fulfil service.	• From Employer in form of data sheets						
Death Beneficiary of corporate Scheme	• Name • Address • DoB • Employment history • Income • Bank account details	• Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Vital • Legitimate	• DD not collected until benefit payment being contemplated	• From Employer in form of Death nomination form						
Member of EBT	• Name • Address • DoB • Employment history • Income • Bank account details	• New Business App • Contributions • Investment • Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Contractual • Consent	• App forms and data fields limited to only those data items needed to fulfil service.	• From Employer and / or Member in form of data sheets						
Settlor of Trust	• Name • Address • DoB • Employment history • Income • Bank account details	• New Business App • Contributions • Investment • Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Contractual • Consent	• App forms and data fields limited to only those data items needed to fulfil service	• Direct from Settlor in form of App & CDD forms						
Beneficiary of Trust	• Name • Address • DoB • Employment history • Income • Bank account details	• Benefit payments • Death benefits • Transfers in/out • AML	• Provision of Trust and pension services • Regulatory Compliance	• Vital • Legitimate	• DD not collected until benefit payment being contemplated	• Name and contact details from Settlor • Post member death, direct AML information from beneficiary						
Staff	• Name • Address • DoB • Employment history • Income • Bank account details	• AML Screening • Salary & pension payments • Performance management	• Employment in financial services business	• Contractual • Consent	• App forms and data fields limited to only those data items needed to fulfil service	• From staff in App form						

***** Conditions for processing explained:**

Consent: the data subject has requested or given consent to the processing of the personal data for the purpose for which it is processed

Contractual: the processing is necessary for the performance of a contract to which the data subject is a party or that is in the interest of the data subject

Vital interests: the processing is necessary to protect the vital interests of the data subject or other individual

Legitimate interests: the processing is necessary for the purposes of legitimate interests