futurity
WEALTH MANAGEMENT

Building your
future collectively

PAIA MANUAL

Contents

This manual has been prepared in terms of section 51
of the Promotion of Access to Information Act 2 of 2000
(as amended)

1. DEFINITIONS

CEO	Chief Executive Officer
Conditions for Lawful Processing	The conditions for the lawful processing of Personal Information as fully set out in chapter 3 of POPI and in paragraph 12 of this Manual.
Client	Any natural or juristic person that received or receives services from the company
Complainant	Any person who lodges a complaint with the Information Regulator
Complaint	(a) A matter reported to the Information Regulator in terms of section 74(1) and (2) of the Act; (b) A complaint referred to in section 76(1)(e) and 92(1) of the Act; (c) A matter reported or referred to the Information Regulator in terms of other legislation that regulates the mandate of the Information Regulator
Conditions for Lawful Processing	The conditions for the lawful processing of personal information as fully set out in chapter 3 of POPI and in section 12 of this manual
Data Subject	The person to whom Personal Information relates
Day	A calendar day, unless the last day of a specified period happens to fall on a Sunday or public holiday, in which case it is calculated exclusive of that Sunday or public holiday (Interpretation Act, 1957 - Act No. 33 of 1957)
DIO	Deputy Information Officer
Information Officer/IO	The individual who is identified herein and legally appointed to ensure compliance with POPIA and PAIA
Manual	This manual
Minister	Minister of Justice and Correctional Services
Office Hours	(a) For the Information Regulator: 08:00-16:00, Monday to Friday (excluding public holidays); (b) For designated offices: Hours during which the offices operate
PAIA	The Promotion of Access to Information Act, No. 2 of 2000
Personal Information	Information relating to an identifiable living person, or an identifiable existing juristic person, including but not limited to race, gender, contact info, biometrics, correspondence, opinions, and identifiers
Personnel	Any person who works for or provides services to or on behalf of the company and receives or is entitled to receive remuneration, including permanent, temporary and part-time staff, directors, and contractors
POPI/POPIA	The Protection of Personal Information Act, No. 4 of 2013
POPI Regulations	Regulations promulgated in terms of section 112(2) of POPI
Private Body	a) A natural person conducting business; (b) A business partnership; (c) A juristic person not being a public body
Processing	Any operation or activity concerning personal information, including collection, storage, dissemination, or destruction
Regulator	Information Regulator established in terms of POPIA
Republic	Republic of South Africa
Signature	Any legally accepted form of signature, including electronic signature where applicable
Writing	As referred to in section 12 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)

Any other terms not described herein will have the meaning as ascribed to it in terms of PAIA or POPI.

2. PURPOSE OF THE PAIA MANUAL

This PAIA Manual is useful for the public to:

2.1 Check the categories of records held by a body which are available without a person having to submit a formal PAIA request.

2.2 Have a sufficient understanding of how to make a request for access to a record of the body, by providing a description of the subjects on which the body holds records and the categories of records held on each subject.

2.3 Know the description of the records of the body which are available in accordance with any other legislation.

2.4 Access all the relevant contact details of the IO and DIO who will assist the public with the records that they intend to access.

2.5 Know the description of the guide on how to use PAIA, as updated by the Regulator, and how to obtain access to it.

2.6 Know if the body will process personal information, the purpose of processing of personal information, and the description of the categories of data subjects and of the information or categories of information relating thereto.

2.7 Know the recipients or categories of recipients to whom the personal information may be supplied.

2.8 Know if the body has planned to transfer or process personal information outside of the Republic of South Africa and the recipients or categories of recipients to whom the personal information may be supplied.

2.9 Know whether the body has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

3. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF FUTURITY WEALTH MANAGEMENT (PTY) LTD

3.1 Chief Information Officer

Name	Ian Martens
Contact number	+27 83 675 2665
Email address	ianm@futurity.co.za

3.2 General contacts for access to information

Email address	marinap@futurity.co.za

3.3 National or head office

Company registration number	2000/018629/07
Postal address	PO Box 652840, Benmore, 2010
Physical address	164 Katherine Street, Sandown, Johannesburg, 2196
Contact number	+27 11 262 2740
Email	ianm@futurity.co.za
Website	www.futurity.co.za

4. GUIDE ON HOW TO USE PAIA AND HOW TO OBTAIN ACCESS TO THE GUIDE

4.1 The Regulator has, in terms of section 10(1) of PAIA, as amended, updated and made available the revised guide on how to use PAIA ("guide"), in an easily comprehensible form and manner, as may reasonably be required by a person who wishes to exercise any right contemplated in PAIA and POPIA.

4.2 The guide is available in each of the official languages and in braille.

4.3 The aforesaid guide contains the description of:

4.3.1 The objects of PAIA and POPIA;

4.3.2 The postal and street address, phone and fax number and, if available, email address of:

4.3.2.1 The IO of every public body, and

4.3.2.2 Every DIO of every public and private body designated in terms of section 17(1) of PAIA and section 56 of POPIA[1];

4.3.3 The manner and form of a request for:

4.3.3.1 Access to a record of a public body contemplated in section 11[2].

4.3.3.2 Access to a record of a private body contemplated in section 50[3].

4.3.3.3 An internal appeal.

4.3.3.4 A complaint to the Regulator.

4.3.3.5 An application with a court against a decision by the IO of a public body, a decision on internal appeal or a decision by the Regulator or a decision of the head of a private body.

4.3.4 The provisions of sections 14[4] and 51[5] requiring a public body and private body, respectively, to compile a manual, and how to obtain access to a manual;

4.3.5 The provisions of sections 15[6] and 52[7] providing for the voluntary disclosure of categories of records by a public body and private body, respectively;

4.3.6 The notices issued in terms of sections 22[8] and 54[9] regarding fees to be paid in relation to requests for access;

4.3.7 The regulations made in terms of section 92[10];

4.3.8 The assistance available from the IO of a public body in terms of PAIA and POPIA;

4.3.9 The assistance available from the Regulator in terms of PAIA and POPIA; and

4.3.10 All remedies in law available regarding an act or failure to act in respect of a right or duty conferred or imposed by PAIA and POPIA, including the manner of lodging.

4.4 Members of the public can inspect or make copies of the guide from the offices of the public and private bodies, including the office of the Regulator, during normal working hours.

4.5 The guide can also be obtained:

23. Upon request to the IO.

24. From the website of the Regulator (www.inforegulator.org.za)

4.6 A copy of the guide is also available in the following three official languages, for public inspection during normal office hours:

4.6.1 English.

4.6.2 Afrikaans.

4.6.3 Zulu.

[2]Section 11 of PAIA - A requester must be given access to a record of a public body if the requester complies with all the procedural requirements in PAIA relating to a request for access to that record, and if access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

[3]Section 50 of PAIA - A requester must be given access to any record of a private body if:
(a) that record is required for the exercise or protection of any rights;
(b) that person complies with the procedural requirements in PAIA relating to a request for access to that record; and
(c) access to that record is not refused in terms of any ground for refusal contemplated in Chapter 4 of this Part.

[4]Section 14 of PAIA - The Information Officer of a public body must update and publish the manual referred to in subsection (1) at intervals of not more than 12 months.

[5]Section 51 of PAIA - The Information Officer of a private body must update and publish the manual referred to in subsection (1) at intervals of not more than 12 months.

[6]Section 15 of PAIA - The Information Officer of a public body must update and publish any notice issued under subsection (2) at intervals of not more than 12 months.

[7]Section 52 of PAIA - The head of a private body must update and publish any notice issued under subsection (2) at intervals of not more than 12 months.

[8]Section 22 of PAIA - If access to a record is granted, the notice must state the access fee (if any) required to be paid by the requester.

[9]Section 54 of PAIA - - If access to a record is granted, the notice must state the access fee (if any) required to be paid by the requester.

[10]Section 92(11) of PAIA - The Information Regulator must update and publish the guide referred to in subsection (1) at intervals of not more than two years.

5. GUIDE OF INFORMATION REGULATOR

5.1 A guide to PAIA and how to access information in terms of PAIA has been published pursuant to section 10 of PAIA.

5.2 The guide contains information required by an individual who may wish to exercise their rights in terms of PAIA.

5.3 Should you wish to access the guide, you may request a copy from the IO by contacting him/her using the details specified above.

5.4 You may also inspect the guide at the company's offices during ordinary working hours.

5.5 You may also request a copy of the guide from the Information Regulator at the following details:

Postal address	P O Box 31533, Braamfontein, Johannesburg, 2017
Contact number	+27 (10) 023-5200
Website	www.inforegulator.org.za
Email	PAIAComplaints@inforegulator.org.za

6. LATEST NOTICES IN TERMS OF SECTION 52(2) OF PAIA

At this stage, no notice(s) has/have been published on the categories of records that are available without having to request access to them in terms of PAIA.

7. AVAILABILITY OF CERTAIN RECORDS IN TERMS OF PAIA

7.1 Categories of records of the Futurity Wealth Management (Pty) Ltd which are available without a person having to request access:

Category of Records	Types of the Record	Available on Website	Available on Request
PAIA Manual	Current PAIA Manual of Futurity Wealth Management (Pty) Ltd	✓	✓
Company Information	Company profile, business overview, service offerings, governance information, contact details and leadership information	✓	✓
Governance Documents	Corporate governance information, regulatory disclosures, compliance statements and governance framework information	✓	✓
Privacy and Data Protection	Privacy Notice, website privacy disclosures, cookies notices and data protection information	✓	✓
Regulatory Information	Information relating to regulatory compliance, Financial Sector Conduct Authority (FSCA) disclosures, complaints procedures and client rights information	✓	✓
Client Information	General information regarding financial planning, wealth management services, investment advisory services and client engagement processes	✓	✓
Marketing and Educational Material	Brochures, newsletters, financial planning guides, articles, market insights and educational content	✓	✓
News and Announcements	Company announcements, industry updates, news releases and service-related communications	✓	✓
Careers and Recruitment	Employment opportunities, recruitment information and career-related notices	✓	✓
Supplier and Procurement Information	Supplier registration information, procurement requirements and applicable accreditation documents		✓
POPIA and PAIA Information	Information regarding data subject rights, access to information procedures and prescribed request forms	✓	✓
Public Compliance Certificates	B-BBEE certificates, regulatory registrations and other publicly available compliance documentation	✓	✓
Website Information	Website terms and conditions, legal notices and disclaimer statements	✓	✓
Complaint and Dispute Resolution Information	Complaints handling procedures, dispute resolution processes and client support information	✓	✓
Contact information for IO	Information Officer contact details, physical address, postal address, telephone numbers and email addresses	✓	✓

The availability of the above records may be subject to periodic updates, amendments, or removal in accordance with applicable legislation, regulatory requirements, and business needs.

7.2 Description of the records/subjects of Futurity Wealth Management (Pty) Ltd which are available in accordance with any other legislation:

Category of Records	Applicable Legislation	Department/Subject Area
Memorandum of Incorporation (MOI), company registration documents, shareholder records, board and committee meeting minutes, governance records	Companies Act, 71 of 2008	Corporate Governance
Financial statements, accounting records, audit reports, taxation records, management accounts, SARS correspondence	Companies Act, 71 of 2008; Income Tax Act, 58 of 1962; Tax Administration Act, 28 of 2011	Finance
VAT returns, VAT records, supporting documentation and SARS submissions	Value-Added Tax Act, 89 of 1991	Finance
Employment contracts, employee records, leave records, remuneration records and attendance records	Basic Conditions of Employment Act, 75 of 1997	Human Resources
Disciplinary records, grievance records, CCMA records, employment-related correspondence and labour dispute records	Labour Relations Act, 66 of 1995	Human Resources
Employment Equity Plans, Employment Equity Reports and Employment Equity Committee records	Employment Equity Act, 55 of 1998	Human Resources
Workplace Skills Plans, Annual Training Reports, learnership records and employee training records	Skills Development Act, 97 of 1998	Human Resources / Training
UIF contribution records, declarations and employee benefit records	Unemployment Insurance Act, 63 of 2001	Human Resources
Compensation Fund registrations, injury-on-duty records and compensation claims	Compensation for Occupational Injuries and Diseases Act, 130 of 1993	Human Resources
Occupational health and safety records, risk assessments, incident reports and safety committee records	Occupational Health and Safety Act, 85 of 1993	Occupational Health and Safety
B-BBEE certificates, ownership and supplier development records	Broad-Based Black Economic Empowerment Act, 53 of 2003	Corporate Governance / Compliance
Client mandates, client agreements, investment advisory agreements, financial planning records, client correspondence and complaints records	Financial Advisory and Intermediary Services Act, 37 of 2002 (FAIS)	Client Services
Records of advice, suitability assessments, needs analyses, replacement advice records, client disclosures and product information	Financial Advisory and Intermediary Services Act, 37 of 2002 (FAIS)	Client Services / Compliance
Financial services provider licences, representative registers, debarment records, compliance monitoring records and regulatory submissions	Financial Advisory and Intermediary Services Act, 37 of 2002 (FAIS)	Compliance
Client due diligence records, Know Your Client (KYC) documentation, identification and verification records, risk assessments and suspicious transaction reporting records	Financial Intelligence Centre Act, 38 of 2001 (if applicable)	Client Services / Compliance
Anti-money laundering (AML) and counter-terrorist financing records, risk management and compliance programme records	Financial Intelligence Centre Act, 38 of 2001 (FICA)	Compliance
Privacy notices, consent records, operator agreements, data processing records, breach registers and personal information impact assessments	Protection of Personal Information Act, 4 of 2013 (POPIA)	Information Compliance

PAIA Manual, PAIA request records, access request registers and PAIA training records	Promotion of Access to Information Act, 2 of 2000 (PAIA)	Information Compliance
Electronic communication records, website terms and conditions, electronic transaction records and electronic consent records	Electronic Communications and Transactions Act, 25 of 2002	Information Technology
Information security policies, cybersecurity records, access control logs, incident response records and business continuity records	Electronic Communications and Transactions Act, 25 of 2002; POPIA	Information Technology
Marketing material, website content, newsletters, client communications and promotional material	Consumer Protection Act, 68 of 2008; FAIS Act, 37 of 2002	Marketing
Client complaints, dispute resolution records, Ombud correspondence and complaint investigation records	Financial Sector Regulation Act, 9 of 2017; FAIS Act, 37 of 2002	Compliance / Client Services
Record retention schedules, destruction records, archive registers and document management records	PAIA; POPIA; Companies Act, 71 of 2008	Records Management
Information Officer and Deputy Information Officer appointment records and Information Regulator correspondence	POPIA; PAIA	Information Compliance

** Although Futurity Wealth Management (Pty) Ltd has used its best endeavours to supply a list of applicable legislation, this list may not be exhaustive. Whenever it comes to the attention of Futurity Wealth Management (Pty) Ltd that existing or new legislation allows a requester access to a record on a basis other than as set out in PAIA, the list will be updated accordingly. If a requester believes that a right of access to a record exists in terms of any legislation listed above or any other legislation, the requester must indicate the legislative basis upon which access is sought to enable the Information Officer to consider the request appropriately.*

7.3 The company holds and/or processes the following records for the purposes of PAIA and POPIA:

7.3.1 PAIA: PAIA Manual; PAIA guides; PAIA records; PAIA submission records; awareness training.

7.3.2 POPIA: Including, but not limited to, the following: IO Registration Certificate; data breach records; retention records; awareness training.

7.3.3 Further information which may be made available upon request.

7.4 The above-mentioned records may be requested; however, it should be noted that there is no guarantee that the request will be honoured. Each request will be evaluated in terms of PAIA and any other applicable legislation.

8. REQUEST PROCESS

8.1 An individual who wishes to place a request must comply with all the procedures laid down in PAIA.

8.2 The requester must complete Form 02 of PAIA Forms (Request for Access to Record) herein, is attached hereto and submit it to the IO at the details specified herein.

8.3 The prescribed form as well as payment of a request fee and a deposit (if applicable) must be submitted to the IO at/via the postal or physical address, fax number or email address as is stated herein.

8.4 The prescribed form must be completed with enough particularity to enable the IO to determine:

8.4.1 The record(s) requested;

8.4.2 The identity of the requestor;

8.4.3 What form of access is required; and

8.4.4 The postal address or fax number of the requestor.

8.5 The requestor must state that the records are required for the requestor to exercise or protect a right, and clearly state what the nature of the right is so to be exercised or protected. An explanation of why the records are requested is required to exercise or protect the right.

8.6 The request for access will be dealt with within 30 (thirty) days from date of receipt, unless the requestor has set out special grounds that satisfies the IO that the request be dealt with sooner.

8.7 The period of 30 (thirty) days may be extended by not more than 30 (thirty) additional days, if the request is for a large quantity of information, or if the request requires a search for information held at another office of the company and the information cannot be reasonably obtained within 30 (thirty) days. The IO will notify the requestor in writing should an extension be necessary.

8.8 The IO must communicate a response to the request for access using Form 03 of PAIA Forms (Outcome of Request and of Fees Payable) herein. This communication shall inform the requestor of:

8.8.1 The decision; and

8.8.2 Fees payable.

8.9 In the event that the IO is of the opinion that the searching and preparation of the record for disclosure would amount to more than six (6) hours, he/she shall inform the requestor to pay a deposit not exceeding one third of the amount payable.

8.10 Should the requestor have any difficulty with the form or the process laid out herein, the requestor should contact the IO for assistance.

8.11 An oral request can be made to the IO should the requestor be unable to complete the form due to illiteracy or a disability. The IO will then complete the form on behalf of the requestor and provide a copy of the form to the requestor.

8.12 Form 2 of POPIA Forms (Request for Correction or Deletion) herein, is used by a data subject to request the correction of inaccurate, outdated, incomplete, irrelevant, or misleading personal information, and/or the deletion or destruction of personal information that is no longer necessary or unlawfully obtained, in accordance with Section 24(1) of POPIA. It ensures that responsible parties maintain accurate and lawful records of personal data.

8.13 Form 3 of POPIA Forms (Application for the Issue of a Code of Conduct) herein is used by an industry body, profession, or class of entities to apply for the issuance of a Code of Conduct under Section 61(1)(b) of POPIA. It allows industries to self-regulate how personal information is processed within their sector, in line with the conditions for lawful processing.

8.14 Form 4 of POPIA Forms (Request for Consent – Direct Marketing) herein enables a responsible party to formally request a data subject's consent to receive direct marketing communications via unsolicited electronic means (e.g., SMS, email), as required under Section 69(2) of POPIA. It ensures that individuals have control over whether and how they are marketed to.

8.15 Form 5 of POPIA Forms (Complaint Regarding Interference with Personal Information) herein allows a data subject or complainant to submit a complaint to the IR concerning unlawful interference with personal information; or a determination made by an adjudicator under POPIA. It provides an avenue for recourse and investigation in cases of non-compliance with data protection obligations.

9. GROUNDS FOR REFUSAL

The following are grounds upon which the company may, subject to the exceptions in chapter 4 of PAIA, refuse a request for access in accordance with chapter 4 of PAIA:

9.1 Mandatory protection of the privacy of a third party who is a natural person, including a deceased person, where such disclosure of personal information would be unreasonable.

9.2 Mandatory protection of the commercial information of a third party, if the records contain:

9.2.1 Trade secrets of that third party;

9.2.2 Financial, commercial, scientific or technical information of the third party, the disclosure of which could likely cause harm to the financial or commercial interests of that third party; and/or

9.2.3 Information disclosed in confidence by a third party to the company, the disclosure of which could put that third party at a disadvantage in contractual or other negotiations or prejudice the third party in commercial competition.

9.3 Mandatory protection of confidential information of third parties if it is protected in terms of any agreement.

9.4 Mandatory protection of the safety of individuals and the protection of property.

9.5 Mandatory protection of records that would be regarded as privileged in legal proceedings.

9.6 Protection of the commercial information of the company, which may include:

9.6.1 Trade secrets;

9.6.2 Financial/commercial, scientific or technical information, the disclosure of which could likely cause harm to the financial or commercial interests of the company;

9.6.3 Information which, if disclosed, could put the company at a disadvantage in contractual or other negotiations or prejudice the company in commercial competition; and/or

9.6.4 Computer programs which are owned by the company, and which are protected by copyright and intellectual property laws.

9.7 Research information of the company or a third party, if such disclosure would place the research or the researcher at a serious disadvantage.

9.8 Requests for records that are clearly frivolous or vexatious, or which involve an unreasonable diversion of resources.

11. FEES

The following are grounds upon which the company may, subject to the exceptions in chapter 4 of PAIA, refuse a request for access in accordance with chapter 4 of PAIA:

Details	Fee
Request fee (payable on every request)	R140.00 once-off
Photocopy of an A4 page or part thereof	R2.00 per page
Printed copy of an A4 page or part thereof	R2.00 per page
Hard copy on flash drive (flash drive to be provided by requestor)	R40.00 once-off
Hard copy on a compact disc (compact disc to be provided by requestor)	R40.00 once-off
Hard copy on a compact disc (compact disc to be provided by the company)	R60.00 once-off
Transcription of visual images per A4 page	As per quotation of service provider
Copy of visual images	As per quotation of service provider
Transcription of an audio record	R24.00 per A4 page
Copy of an audio record on flash drive (flash drive to be provided by requestor)	R40.00 once-off
Copy of an audio on a compact disc (compact disc to be provided by requestor)	R40.00 once-off
Copy of an audio on a compact disc (compact disc to be provided by the company)	R60.00 once-off
Base/starting rate to search for and prepare the record for disclosure	R145.00 per hour for each hour or part thereof, excluding the first hour, reasonably required for such search and preparation (cannot exceed R435.00 per request)
Rate to search for and prepare the record for disclosure	R435.00 per hour for each hour or part thereof, excluding the first hour, reasonably required for such search and preparation (cannot exceed total cost)
Postage, email or any other electronic transfer	Actual expense, if any

12. PROCESSING OF PERSONAL INFORMATION

12.1 The purposes for processing personal information include:

12.1.1 To provide wealth management, financial planning, investment advisory, retirement planning, risk management, and related financial services to clients.

12.1.2 To establish and maintain client relationships, including conducting needs analyses, financial assessments, risk profiling, suitability assessments, and providing financial advice.

12.1.3 To comply with legal, regulatory, and professional obligations, including obligations imposed by the Financial Advisory and Intermediary Services Act (FAIS), Financial Intelligence Centre Act (FICA), Protection of Personal Information Act (POPIA), Income Tax Act, Companies Act, and other applicable legislation.

12.1.4 To perform client due diligence, identity verification, Know Your Client (KYC) procedures, anti-money laundering (AML) screening, sanctions screening, and fraud prevention activities.

12.1.5 To facilitate the implementation, administration, management, and servicing of financial products, investments, retirement funds, insurance products, and other financial solutions.

12.1.6 To communicate with clients, prospective clients, product providers, regulators, service providers, employees, suppliers, and other stakeholders regarding services, transactions, requests, instructions, or regulatory requirements.

12.1.7 To process applications, instructions, transactions, claims, withdrawals, transfers, investments, and other financial service-related activities.

12.1.8 To manage client records, maintain accurate account information, and ensure the quality and integrity of information held by the Company.

12.1.9 To process payments, commissions, fees, invoices, reimbursements, and other financial transactions related to the Company's operations and services.

12.1.10 To respond to enquiries, complaints, disputes, requests for information, regulatory investigations, audits, and legal proceedings.

12.1.11 To conduct internal business administration, governance, risk management, compliance monitoring, record keeping, reporting, and business continuity activities.

12.1.12 To recruit, employ, manage, remunerate, train, and support employees, contractors, representatives, and consultants.

12.1.13 To manage relationships with suppliers, service providers, business partners, and professional advisers.

12.1.14 To maintain physical and electronic security, including access control, visitor management, information security monitoring, cybersecurity measures, and fraud detection.

12.1.15 To conduct market research, client satisfaction surveys, service improvement initiatives, and business analytics.

12.1.16 To provide newsletters, financial insights, educational content, invitations to events, and other marketing communications where permitted by law or where consent has been obtained.

12.1.17 To exercise and defend legal rights, enforce agreements, recover debts, and protect the legitimate interests of Futurity Wealth Management (Pty) Ltd, its clients, employees, and stakeholders.

12.1.18 To fulfil any other purpose directly related to the Company's business activities, where such processing is lawful, reasonable, and necessary.

12.2 Description of the categories of data subjects and of the information or categories of information relating thereto:

Categories of data subjects	Personal information that may be processed
Clients / Customers	Full names, identity numbers, passport numbers, dates of birth, contact details, residential and postal addresses, marital status, employment information, financial information, banking details, tax numbers, investment information, risk profiles, financial needs analyses, records of advice, product holdings, beneficiary information, correspondence and transaction records.
Prospective Clients	Names, contact details, financial objectives, investment requirements, enquiry records, meeting notes, marketing preferences and correspondence.

Continued -

Categories of data subjects	Personal information that may be processed
Beneficiaries and Dependants	Names, identity numbers, dates of birth, relationship to client, contact information, beneficiary nominations and related financial information.
Employees	Names, surnames, identity numbers, tax numbers, contact details, residential addresses, banking details, employment contracts, remuneration records, payroll information, leave records, performance records, disciplinary records, qualifications, training records, employment equity information, health and safety records and benefit information.
Job Applicants	Names, contact details, curriculum vitae, qualifications, employment history, references, interview notes, criminal record checks, credit checks and background verification information where permitted by law.
Representatives, Key Individuals and Compliance Officers	Identity information, qualifications, fit and proper records, FSCA registration information, employment information, regulatory compliance records, training records and professional accreditation information.
Service Providers and Suppliers	Names, company registration numbers, VAT numbers, contact details, banking information, contracts, invoices, tax information, B-BBEE information and correspondence.
Financial Product Providers and Business Partners	Contact person information, company registration details, licensing information, contractual records, service agreements and business correspondence.
Contractors and Consultants	Identity numbers, contact details, qualifications, work history, contractual information, banking details, tax information and performance-related records.
Visitors to Company Premises	Names, contact details, visitor register information, vehicle registration details and CCTV footage where applicable.
Regulatory Bodies / Authorities	Contact information, regulatory correspondence, licensing information, compliance reports, investigation records and statutory submissions.
Complainants and Data Subjects Exercising Their Rights	Identity information, contact details, complaint records, request documentation, correspondence and investigation records.
Directors and Shareholders	Names, identity numbers, contact details, shareholding information, directorship information, declarations of interest, governance records and statutory disclosure information.
Website Users	IP addresses, browser information, cookies, device information, website usage information, online enquiry records and electronic communication details.
Marketing / Newsletter Subscribers	Full name, contact info (email, phone), preferences, consent records, interaction history with communications
Information Officer and Deputy Information Officer	Contact information, identity information, appointment records, registration details and correspondence with the Information Regulator.

13. THE RECIPIENTS OR CATEGORIES OF RECIPIENTS TO WHOM THE PERSONAL INFORMATION MAY BE SUPPLIED

Categories of Personal Information	Recipients or Categories of Recipients to whom the Personal Information may be Supplied
Identity numbers, names, contact details and identification documents (for client verification and due diligence)	Financial Intelligence Centre (FIC), accredited identity verification service providers, authorised financial institutions, product providers and regulatory authorities where required by law
Client due diligence (KYC) information, source of funds information and risk assessment information	Financial institutions, investment providers, insurers, platform administrators, compliance service providers and regulatory authorities
Financial information, banking details and investment information	Banks, investment platform providers, asset managers, financial product providers, insurers, retirement fund administrators and authorised payment service providers
Client mandates, investment instructions and records of advice	Financial product providers, investment administrators, discretionary fund managers, asset managers and authorised third-party service providers involved in providing financial services
Tax information, tax numbers and financial reporting records	South African Revenue Service (SARS), tax consultants, auditors and authorised financial service providers
Employment information and payroll records	Payroll service providers, auditors, SARS, employee benefit providers and statutory authorities
Employee benefit information	Medical aid providers, retirement fund administrators, insurers and employee benefit consultants
Qualifications, fit and proper records and professional accreditation information	Financial Sector Conduct Authority (FSCA), professional bodies, training providers, qualification verification agencies and compliance service providers
Criminal checks, fraud prevention information and identity verification information	South African Police Service (SAPS), accredited background screening providers, fraud prevention agencies and regulatory authorities
Credit information and payment history	Credit bureaux, authorised financial institutions and credit verification service providers where legally permissible
Regulatory reporting and compliance records	Financial Sector Conduct Authority (FSCA), Financial Intelligence Centre (FIC), Information Regulator, Ombud offices and other competent regulatory authorities
Complaints, dispute resolution and investigation records	Ombud for Financial Services Providers, legal advisers, insurers, regulatory authorities and dispute resolution service providers
Supplier and service provider information	Auditors, accountants, banks, regulatory authorities and authorised business partners
Information technology and system user information	Managed IT service providers, cloud hosting providers, cybersecurity providers and authorised software vendors subject to appropriate security safeguards
Website usage information, cookies and electronic communication records	Website hosting providers, analytics providers and authorised technology service providers
Categories of Personal Information	**Recipients or Categories of Recipients to whom the Personal Information may be Supplied**

Continued -

CCTV footage, visitor records and security incident information	Security service providers, law enforcement authorities and regulatory authorities where legally required
Personal information processed for legal proceedings, investigations or debt recovery	Attorneys, advocates, debt collection agencies, courts, tribunals and regulatory authorities
Information Officer registration records and POPIA compliance records	Information Regulator, authorised compliance consultants, legal advisers and regulatory authorities

**Personal information will only be disclosed to recipients where there is a lawful basis for doing so, where such disclosure is necessary to provide services, comply with legal and regulatory obligations, protect legitimate interests, or where consent has been obtained from the data subject where required.*

14. PLANNED TRANSBORDER FLOWS OF PERSONAL INFORMATION

Futurity Wealth Management (Pty) Ltd may transfer, process, or store certain categories of personal information outside the Republic of South Africa where it is necessary for business operations, service delivery, regulatory compliance, information technology services, cloud storage, cybersecurity, communication platforms, or the administration of financial products and services.

Such transfers may occur through the use of reputable third-party service providers, cloud-based systems, software vendors, investment administration platforms, financial product providers, data hosting providers, and technology service providers.

Personal information may be processed or stored in the following jurisdictions, depending on the service provider utilised:

The country in which personal information will be stored	
South Africa	Client records, employee records, supplier information, financial records, compliance records, investment and advisory records
European Union (EU)	Cloud-hosted business information, client correspondence, employee information, compliance records and business communications
United States of America	Email communications, cloud storage, cybersecurity monitoring, software applications, website and technology-related information
United Kingdom	Financial services-related information, cloud-hosted records and business communications where applicable
Other Jurisdictions utilised by authorised service providers	Personal information processed as part of financial services administration, cloud hosting, disaster recovery, software support and business continuity services

NB: Indicate if the body has planned transborder flows of personal information. For example, some personal information may be stored in the cloud outside of the Republic. Please specify the country in which personal information will be stored and categories of personal information.

14.1. Futurity Wealth Management may share personal information with third parties and in certain instances this may result in transborder flow of the personal information. The personal information will always be subject to protection, not less than the protection it is afforded under the Protection of Personal Information Act No.4 of 2013. General description of information security measures to ensure the confidentiality, integrity and availability of the information:

- 14.1.1. Keeping our systems secure through access controls, system monitoring, and usage tracking;
- 14.1.2. Storing physical and digital records in secure, access-controlled environments;
- 14.1.3. Restricting access to buildings, systems, and records to authorised personnel only;
- 14.1.4. Securely destroying or deleting personal information once it is no longer required;
- 14.1.5. Ensuring compliance with relevant data protection standards, legal requirements, and industry codes of **conduct.**

14.2. In addition, the following technical security safeguards have been implemented to support these-objectives:

- 14.2.1 Data encryption (at rest and in transit) to protect sensitive information from unauthorised access;
- 14.2.2 Anti-virus and anti-malware software to detect, prevent, and mitigate cyber threats;
- 14.2.3 Firewalls and intrusion detection/prevention systems (IDS/IPS) to monitor and safeguard network traffic;
- 14.2.4 Multi-factor authentication (MFA) and role-based access controls to limit access based on job function and business need;
- 14.2.5 Secure backup and disaster recovery solutions to ensure business continuity and data integrity;
- 14.2.6. Ongoing system monitoring and access logging to detect and respond to suspicious activity;

14.2.7 Physical security controls such as keycard access, secure storage, and visitor management procedures;

14.2.8 Employee training and awareness programmes to promote secure data handling and prevent human error;

14.2.9 Secure disposal of physical and electronic records when no longer needed or when required by law.

14.2.10 These safeguards are continuously reviewed and enhanced to address new risks, changing business processes, and advancements in technology.

15. AVAILABILITY OF THE MANUAL

15.1. A copy of the manual is available:

15.1.1. On www.futurity.co.za or at any head office of Futurity Wealth Management (Pty) Ltd for public inspection during normal business hours;

15.1.2. To any person upon request and upon the payment of a reasonable prescribed fee; and

15.1.3. To the Information Regulator upon request.

15.2. A fee for a copy of the manual, as contemplated in Annexure B of the Regulations, shall be payable per each A4-size photocopy made.

16. OBJECTION TO THE PROCESSING OF PERSONAL INFORMATION BY A DATA SUBJECT

16.1. A data subject who wishes to object to the processing of personal information in terms of section 11(3)(a) or section 11(3)(b) of the Act, must submit the objection to a responsible party at any time during office hours of a responsible party and free of charge.

16.2. A data subject who wishes to object to the processing of personal information must do so on a form substantially similar to Form 3 herein, free of charge and reasonably accessible to a data subject by hand, fax, post, email, SMS, or WhatsApp and or in any manner expedient to a data subject in terms of section 11(3)(a) of the Act.

16.3. A responsible party must, when collecting personal information of a data subject, notify the data subject, in terms of section 18(1)(h)(iv) of the Act, of their right to object, as referred to in section 11(3) of the Act.

16.4. If an objection to the processing of personal information of a data subject is made telephonically, such an objection shall be electronically recorded by a responsible party and upon request, be made available to the data subject in any manner, including the transcription thereof.

17. REQUEST FOR CORRECTION/DELETION OF PERSONAL INFORMATION OR DESTRUCTION/DELETION OF RECORD OF PERSONAL INFORMATION

17.1. A data subject has the right, in terms of section 24 of the Act, to request, where necessary, the correction, destruction, or deletion of his, her or its personal information.

17.2. A data subject, who wishes to request a correction or deletion of his, her, or its personal information, as provided for in section 24(1)(a) of the Act, has the right to request correction or deletion of personal information at any time and free of charge, if the personal information is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully.

17.3. A data subject who wishes to request the destruction or deletion of a record of his, her, or its personal information in terms of section 24(1)(b) of the Act, has the right to request the destruction or deletion of a record of his, her or its personal information at any time and free of charge, if a responsible party is no longer authorised to retain such information in terms of section 14 of the Act.

17.4. A request for correction to or deletion of personal information, as referred to in sub-regulation 12.11.2 or a request for the destruction or deletion of a record of personal information, as referred to in sub-regulation 12.11.3 must be submitted to a responsible party on a form which is substantially similar to Form 2 of POPIA Forms herein free of charge and reasonably accessible to a data subject by hand, fax, post, email, SMS, WhatsApp message or in any manner expedient to a data subject.

17.5. A request for a correction or deletion of personal information by telephonic means shall be recorded by a responsible party and such recording must, upon request, be made available to a data subject in any manner, including the transcription thereof which shall be free of charge.

17.6. A responsible party must, within 30 (thirty) days of receipt of the outcome of the request referred to in sub-regulation 12.11.2 or 12.11.3, notify a data subject, in writing, of the action taken as a result of the request

18. UPDATING OF THE MANUAL

The head of Futurity Wealth Management (Pty) Ltd will update this manual on a regular basis.

Name of IO	Ian Campbell Martens
Title of the head of the body	Director

APPLICABLE FORMS

PAIA FORMS

Hereby request the following:

Form 01	Request for a Copy of the Guide from an Information Officer [Regulation 3]
Form 02	Request for Access to Record [Regulation 7]
Form 03	Outcome of Request and of Fees Payable [Regulation 8]
Form 05	Complaint Form [Regulation 10]
Form 13	PAIA Request for Compliance Assessment Form [Regulation 14(1)]

POPIA FORMS

Hereby request the following:

Form 1	Objection to the Processing of Personal Information
Form 2	Request for Correction of Deletion of Personal Information or Deletion of Record of Personal Information
Form 3	Application for the Issue of a Code of Conduct
Form 4	Application for the Consent of a Data Subject for the Processing of Personal Information for the Purpose of Direct Marketing
Form 5	Complaint Regarding Interference with the Protection of Personal Information for the Purpose of Direct Marketing