PAIA MANUAL

ACCESS TO INFORMATION MANUAL OF FINGLOBAL MIGRATION (PTY) LTD

Prepared in accordance with Section 51 of the Promotion of Access to Information Act, No. 2 of 2000 as amended by the Protection of Personal information Act, No 4 of 2013.

Tel +27 28 312 2764 | Email info@finglobal.com | Address 7 Marine Sq, College Rd, Hermanus, 7200 | Postnet Suite 154, Private Bag X16, Hermanus, 7200
FinGlobal Migration (Pty) Ltd 2009/023667/07 trading as FinGlobal is a licensed South African financial services provider. FSP no. 42872 | www.finglobal.com

Contents

1. COMPANY OVERVIEW

FinGlobal Migration (Pty) Limited t/a FinGlobal (the company) is a licensed category 1 Financial Services Provider, registered with the Financial Sector Conduct Authority with FSP no. 42872. The company provides a wide range of global financial migration services, including but not limited to:

1.1. Emigration services;
1.2. Encashment of insurance policies and investments;
1.3. Tax services;
1.4. Foreign exchange services; and
1.5. Financial planning.

2. LIST OF ACRONYMS AND ABBREVIATIONS

Acronym / Abbreviation	Description
CEO	Chief Executive Officer
DIO	Deputy Information Officer
IO	Information Officer
Minister	Minister of Justice and Correctional Services
PAIA	Promotion of Access to Information Act No. 2 of 2000 (as amended)
POPIA	Protection of Personal Information Act No.4 of 2013
Regulator	Information Regulator
Republic	Republic of South Africa
The Act	Promotion of Access to Information Act No. 2 of 2000 (as amended)

3. PURPOSE OF PAIA MANUAL

This PAIA Manual is useful for the public to:

3.1. check the categories of records held by a company which are available without a person having to submit a formal PAIA request;
3.2. have a sufficient understanding of how to make a request for access to a record of the company, by providing a description of the subjects on which the company holds records and the categories of records held on each subject;
3.3. know the description of the records of the company which are available in accordance with any other legislation;
3.4. access all the relevant contact details of the Information Officer and Deputy Information Officer who will assist the public with the records they intend to access;
3.5. know the description of the guide on how to use PAIA, as updated by the Regulator and how to obtain access to it;
3.6. know if the company 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;
3.7. know the description of the categories of data subjects and of the information or categories of information relating thereto;

3.8. know the recipients or categories of recipients to whom the personal information may be supplied;
3.9. know if the company has planned to transfer or process personal information outside the Republic and the recipients or categories of recipients to whom the personal information may be supplied; and
3.10. know whether the company has appropriate security measures to ensure the confidentiality, integrity and availability of the personal information which is to be processed.

4. COMPANY DETAILS (SECTION 51(1)(A))

Company

Name of company	**FinGlobal Migration (Pty) Ltd**
Registration number	2009/023667/07
Physical address	7 Marine Square, College Road, Hermanus, Western Cape
Postal address	Postnet Suite 154, Private Bag x16, Hermanus, Western Cape
Telephone number	028 312 2764
E-mail	legal@finglobal.com
Directors	Hannah Mmamollo Margaret Sadiki Ryno Pieter Viljoen (CEO) Jacobus Johannes Sieberhagen Tendani Sikhwivhilu

Chief Information Officer

Name	**Ryno Pieter Viljoen**
Telephone number	028 312 2764
E-mail	legal@finglobal.com

Deputy Information Officer

Name	**Werner Kriel**
Telephone number	028 312 2764
E-mail	legal@finglobal.com

5. SECTION 10 GUIDE (SECTION 51(1)(B))

The Information Regulator has compiled an official PAIA Guide to assist in understanding how to exercise any right contemplated in PAIA or POPIA.

This Guide is available in each of the official languages and can be obtained from the website of the Information Regulator (under the heading PAIA Guide and Manual).

https://inforegulator.org.za/information-regulator-paia-manuals/

The contact details of the Information Regulator are:	
Physical address	JD House, 27 Stiemens Street, Braamfontein, Johannesburg, 2001
Telephone number	+27 (0)10 023 5207
Complaints e-mail address	PAIAcomplaints@inforegulator.org.za
General enquiries e-mail address	enquiries@inforegulator.org.za
Website	https://inforegulator.org.za/

NOTE: Copies of the Regulators' PAIA Guide are available in at least 2 of the official languages, for public inspection, during normal office hours, at the offices of FinGlobal Migration (Pty) Ltd.

6. APPLICABLE LEGISLATION (SECTION 51(1)(D))

Records are kept in accordance with such other legislation, as is applicable to the company, which includes but is not limited to the following:

No	Act	Ref
1	Companies Act	71 of 2008
2	Copyright Act	98 of 1978
3	Consumer Protection Act	68 of 2008
4	Employment Equity Act	55 of 1998
5	Income Tax Act	95 of 1967
6	Labour Relations Act	66 of 1995
7	Value-Added Tax Act	89 of 1991
8	Financial Advisory and Intermediary Services Act	37 of 2002
9	Basic Conditions of Employment Act	75 of 1997
10	Financial Intelligence Centre Act	28 of 2001
11	Electronic Communications and Transactions Act	25 of 2002
12	Promotion of Access of Information Act	2 of 2000
13	Unemployment Insurance Act	63 of 2001
14	Compensation for Occupational Injuries and Disease Act	130 of 1993
15	Occupational Health and Safety Act	85 of 1993
16	Skills Development Act	9 of 1999
17	Prevention of Organised Crime Act	121 of 1998
18	Protection of Constitutional Democracy against terrorist related activities Act	33 of 2004
19	Protection of Personal Information Act	4 of 2013

The above records are of a public nature and are available automatically without a person having to request access to them in terms of the Act, as envisaged in Section 52.

7. ACCESS TO RECORDS HELD BY THE COMPANY (SECTION 51(1)(E))

For the purpose of this manual and the Act, the records held by the company are categorised by the nature and content thereof. Please note that by listing the categories and information held by the company below does not mean that a request for any information listed below will automatically be granted. All requests will be evaluated in accordance with the circumstances of the individual request and the provisions of the Act.

7.1. Company Secretarial Records

7.1.1. Documents of Incorporation
7.1.2. Memorandum of Incorporation
7.1.3. Minutes of Director's meetings
7.1.4. Records relating to the appointment of directors, auditors and public officers
7.1.5. Share register
7.1.6. Other statutory documents

7.2. Financial Records

7.2.1. Annual financial records
7.2.2. Tax returns
7.2.3. Accounting records
7.2.4. Banking records
7.2.5. Asset register
7.2.6. Invoices
7.2.7. Internal and external audit reports

7.3. Income Tax Records

7.3.1. PAYE Records
7.3.2. Documents issued to employees for income tax purposes
7.3.3. Records of payments made to the South African Revenue Service
7.3.4. All other statutory compliances – VAT, UIF, skills development levies

7.4. Human Resources Documents and Records:

7.4.1. Arbitration awards
7.4.2. CCMA records
7.4.3. Confidentiality agreements
7.4.4. Disciplinary records
7.4.5. Employee personal details
7.4.6. Employment contracts
7.4.7. Employment Equity Plan
7.4.8. Human Resources policies and procedures
7.4.9. Leave records
7.4.10. Remuneration and benefits records
7.4.11. Restraint of trade records
7.4.12. Retirement fund records
7.4.13. Salary records
7.4.14. Training records

7.5. Compliance Records

7.5.1. Declarations, registers, policies and procedures in terms of the Financial Advisory and Intermediary Services Act, No 37 of 2002
7.5.2. FICA Risk Management and Compliance Programme
7.5.3. Conflict of Interest management policy
7.5.4. Risk management policy
7.5.5. All compliance policies and procedures
7.5.6. Service level agreements

7.6. Legal Records

7.6.1. Documentation pertaining to litigation or arbitration
7.6.2. General agreements
7.6.3. Licences, permits and authorisations

7.7. Insurance Records

7.7.1. Claims records
7.7.2. Details of insurance coverage, limits, and insurers
7.7.3. Insurance policies

7.8. Fixed property and fixed assets

7.8.1. Financial lease agreements
7.8.2. Fixed asset registers
7.8.3. Property lease agreements

7.9. Marketing and Strategic Records

7.9.1. Marketing materials
7.9.2. Marketing strategies
7.9.3. Strategic Planning documents, Business Plans etc.

7.10. Client information

The company complies with the Protection of Personal Information Act, No. 4 of 2013 and therefore has very strict procedures in place to protect client information. Any request for client information will require detailed motivation for the request, including the reason why the information is required.

8. ACCESS REQUEST PROCEDURE (SECTION 51(1)(E))

It is important to note that the successful completion and submission of an access request form does not automatically allow the requester access to the requested record.

An application for access to a record is subject to certain limitations if the requested record falls within a certain category as specified within Chapter 4 of PAIA.

If it is reasonably suspected that the requester has obtained access to records through the submission of materially false or misleading information, legal proceedings may be instituted against such a requester.

The requester must complete Form 2 together with a request fee (the form can be obtained from the company) and submit it to the company by hand or email.

8.1. Completion and submission of Access Request Form 2

The prescribed Form 2 must be completed in full and contain sufficient detail in order to enable the Information Officer to identify:

8.1.1. The records requested;

8.1.2. Proof of identity of the requester (and if an agent is lodging the request, proof of capacity) by attachment of the identity document of the requester;
- 8.1.2.1. Form 2 must be filled in type or block letters.
- 8.1.2.2. All questions on Form 2 must be answered. If a question does not apply state N/A. If nothing to disclose state Nil.
- 8.1.2.3. If there is insufficient space on the form, additional information may be provided on an attached folio and each answer on such folio must reflect the applicable title.

8.1.3. Which form of access is required; and

8.1.4. The postal address or email address of the requester in the Republic.
- 8.1.4.1. The requester must identify the right which the requester is seeking to exercise or protect.

The requester must provide an explanation of the reason the record is required for the exercise or protection of any right.

If, in addition to a written reply, the requester wishes to be informed of the decision in respect of the request in any other manner, the requester is making the request to the reasonable satisfaction of the appointed Information Officer.

8.2. Notification

8.2.1. The Information Officer will, within 30 days of receipt of the request, decide whether to grant or decline the request and give notice with reasons (if required) to that effect.

8.2.2. The 30-day period within which the Information Officer must decide whether to grant or refuse the request may be extended for a further period of not more than 30 days if the request is for a large volume of information or requires the Information Officer to search through a large volume of records, or the records are not kept at the offices of FinGlobal.

8.2.3. The Information Officer will notify the requester in writing should an extension be sought.

8.2.4. If a record requested cannot be found, or does not exist, the Information Officer shall by means of an affidavit notify the requester. In the affidavit, a full account is required of all steps taken to find the record in question.

8.2.5. If the Request for Access to a record is not successful, the requester will be notified of the following:

8.2.5.1. Adequate reasons for the refusal (refer to Third Party Information and Grounds for Refusal below); and

8.2.5.2. That the requester may lodge an application with a court against the refusal of the request and the procedure, including the period for lodging the application.

8.3. Payment of fees (section 51(1)(f))

8.3.1. Requested fees

Where a requester submits a request for access to information held by an institution on a person other that the requester himself/herself, a request fee in the amount of R50.00 is payable upfront before the company will further process the request received.

Note: This fee is not applicable to personal requesters (data subjects), referring to any person seeking access to records that contain their personal information in terms of the Protection of Personal Information Act, No 4 of 2013.

8.3.2. Access fees

An access fee is payable in all instances where a request for access to information is granted, except in those instances where payment of an access fee is specially excluded in terms of the Act, or an exclusion is determined by the Minister in terms of Section 54 (8).

Payment details can be obtained from the Information Officer as indicated in this Manual and payment can be made either via a direct deposit or by bank guaranteed cheque (no credit card payments are accepted). Proof of payment must be supplied.

The requester may be notified whether a deposit is required. A deposit will be required depending on certain factors such as the volume and/or format of the information requested.

If the preparation of the record requested requires more than the prescribed hours (six), a deposit shall be paid (of not more than one third of the access fee which would be payable if the request were granted). Records may be withheld until the fees have been paid.

FEES FOR REPRODUCTION OF INFORMATION		
1	For every photocopy of an A4-size page or part thereof	R 1.10
2	For every printed copy of an A4-size page or part thereof held on a computer or in electronic or machine-readable form	R 0.75
3	For a copy in a computer-readable form on: - floppy disk - compact disk	 R 7.50 R70.00
4	A transcription of visual images, for an A4-size page or part thereof	R40.00
5	For a copy of visual images	R60.00
6	A transcription of an audio record, for an A4-size page or part thereof	R20.00
7	For a copy of an audio record	R30.00
8	To search for the record for disclosure (per hour or part thereof reasonable required for such search)	R30.00
9	Where a copy of a record needs to be posted the actual postal fee is payable.	

8.4. Third party information

8.4.1. If access is requested to a record that contains information about a third party, the relevant Information Officer is obliged to attempt to contact this third party to inform them of the request. This enables the third party the opportunity of responding by either consenting to access or by providing reasons why access should be denied.

8.4.2. In the event of the third-party furnishing reasons for the support or denial of access, the Information Officer will consider these reasons in determining whether access should be granted, or not.

8.5. Grounds for refusal

The Information Officer may legitimately refuse to grant access to a requested record that falls within a certain category. Grounds for refusal of access may include:

8.5.1. protecting personal information that the Information Officer holds about a third person (who is a natural person), including a deceased person, from unreasonable disclosure;

8.5.2. protecting commercial information that is held about a third party or the group or a particular company or entity in the group (for example trade secrets: financial, commercial, scientific or technical information that may harm the commercial or financial interests of the organisation or the third party);

8.5.3. if disclosure of the record would result in a breach of a duty of confidence owed to a third party in terms of an agreement;

8.5.4. if disclosure of the record would endanger the life or physical safety of an individual;

8.5.5. if disclosure of the record would prejudice or impair the security of property or means of transport;
8.5.6. if disclosure of the records would prejudice or impair the protection of a person in accordance with a witness protection scheme;
8.5.7. if disclosure of the record would prejudice or impair the protection of the safety of the public;
8.5.8. the record is privileged from production in legal proceedings, unless the legal privilege has been waived;
8.5.9. disclosure of the record (containing trade secrets, financial, commercial, scientific, or technical information) would harm the commercial or financial interests of the group;
8.5.10. disclosure of the record would put the group or a particular company or entity in the Group at a disadvantage in contractual or other negotiations or prejudice it in commercial competition;
8.5.11. the record is a computer programme; and
8.5.12. the record contains information about research being carried out or about to be carried out on behalf of a third party or the group or a particular company or entity in the group.

8.6. Remedies available upon refusal of a Request to Access

8.6.1. Internal remedies - FinGlobal does not have internal appeal procedures. As such, the decision made by the Information Officer is final, and requesters will have to exercise such external remedies at their disposal if the Request for Access is refused.
8.6.2. External remedies - In accordance with sections 56(3) (c) and 78 of PAIA, a requestor may apply to a court for relief within 180 days of notification of the decision for appropriate relief.

8.7. Records that cannot be found or do not exist

If the Information Officer has searched for a record and it is believed that the record either does not exist or cannot be found, the Requester will be notified by way of an affidavit or affirmation. This will include the steps that were taken to try to locate the record.

9. PROCESSING OF PERSONAL INFORMATION ACT (POPIA)

9.1. Purpose of POPIA

The Protection of Personal Information Act, No. 4 of 2013 (POPIA), regulates and controls the processing, including the collection, use, and transfer of personal information relating to identifiable, living, naturals persons and juristic persons.
Personal information as defined in terms of POPIA includes but is not limited to, information as follows: Name, address, contact details, date of birth, place of birth, identity number, passport number, bank details, tax number, financial information and criminal history.

In terms of POPIA, a person (responsible party) has a legal duty to collect, use, transfer and destroy (process) another's (data subject) personal information in a lawful, legitimate and responsible manner and in accordance with the provisions and the 8 processing conditions set out under POPIA.

9.2. Descriptions of categories of data subjects

The company holds information and record information relating to the following broad categories of data subjects or persons, which list is not limited to:

9.2.1. Employees, job applicants, learnership candidates, directors, interns, agents, sponsors;
9.2.2. Customers and clients of the company;
9.2.3. Contractors, vendors, suppliers, service providers, operators;
9.2.4. Business partners whether acting on behalf of the company or not or those that provide services, goods and other benefits to the company such as banks, pension and provident funds, administrators, service providers, insurance companies, advertising, marketing or PR agencies;
9.2.5. Regulators and Public Bodies who the company engage with in order to discharge legal and public duty obligations, including the South African Revenue Service, National Treasury, Department of Labour and the South African Reserve Bank;
9.2.6. Users of website/applications/mobile applications/social media portals or platforms whether in order to enquire more about the company or to do business with the company; and
9.2.7. Persons who interact with the company physically or enter the offices, and all facilities of the company or interact via websites/email/correspondence.

9.3. Reasons for processing personal information

The company will process personal information which belongs or is held by a data subject. This processing is required by the company to allow it to perform the following (without detracting from the generality hereof):

9.3.1. to pursue their business objectives and strategies;
9.3.2. to comply with a variety of lawful obligations, including without detracting from the generality thereof, to carry out actions for the conclusion and performance of a contract as between the company and the data subject;
9.3.3. to put in place protective mechanisms to protect the data subject's and/or the company's legitimate interests including the performance of risk assessments and risk profiles where applicable and necessary;
9.3.4. to obtain as required by law or to protect the respective party's legitimate interests,
9.3.5. to obtain or provide personal information from a credit bureau or credit provider or credit association, information about certain data subject's credit record, including personal information about any judgement or default history;
9.3.6. for the purposes of making contact with the data subject and attending to the data subject's enquiries and requests;

9.3.7. for the purpose of providing the data subject from time to time with information pertaining to the company, their officers, employees, services and goods and other ad hoc business related information;

9.3.8. to pursue the data subject's and/or company's legitimate interests, or that of a third party to whom the personal information is supplied;

9.3.9. for the purposes of providing, maintaining, and improving the company's services, and to monitor and analyse various usage and activity trends pertaining thereto;

9.3.10. for the purposes of performing internal operations, including management of employees, employee wellness programmes, the performance of all required HR functions, attending to all financial matters including budgeting, planning, invoicing, facilitating and making payments, sending receipts, and generally providing commercial support, where needed, requested or required; and

9.3.11. for the purpose of preventing fraud and abuse of the company's processes, systems, procedures and operations, including conducting internal and external investigations and disciplinary enquiries and hearings.

9.4. Storage, retention, and destruction of information

9.4.1. The company will ensure that the data subject's personal information is securely stored electronically, which for operational reasons, will be accessible to certain categories of authorised persons within the company on a need to know and business basis, save that where appropriate, some of the data subject's personal information may be retained in hard copy and stored securely.

9.4.2. All such personal information will be held and/or stored securely. In this regard the company will ensure that it performs regular audits regarding the safety and the security of all data subject's personal information.

9.4.3. Appropriate technical and organisational measures will be taken by the company to ensure that personal information remains confidential and secure against unauthorised or unlawful processing and accidental loss or destruction or damage.

9.4.4. Once the data subject's personal information is no longer required due to the fact that the purpose for which the personal information was held has come to an end and expired, such personal information will be safely and securely archived for the required prescribed periods or longer should this be required by the company. The company thereafter will ensure that such personal information is permanently destroyed.

9.5. Access by others and cross border transfer

The company may from time to time have to disclose a data subject's personal information to other parties, including organs of state, other departments or subsidiaries, product or third party service providers, regulators and/or governmental officials, overseas service providers and/or agents, but such disclosure will always be subject to an agreement which will be concluded as between the company and the party to whom it is disclosing the data subject's personal information to, which contractually obliges the recipient of this personal information to comply with strict confidentiality and data security conditions.

Where personal information and related data is transferred to a country which is situated outside the borders of South Africa, the data subject's personal information will only be transferred to those countries which have similar data privacy laws in place or where the recipient of the personal information is bound contractually to a no lesser set of obligations than those imposed by POPIA.

9.6. Access of information by the data subject

POPIA provides that a data subject may, upon proof of identity, request the responsible party to confirm, free of charge, all the information it holds about the data subject and may request access to such information, including information about the identity of third parties who have or have had access to such information.

Where a data subject is desirous of obtaining details of the personal information which the company may hold of and which pertain to it, then it must make application as described in section 7 of this Manual.

POPIA provides that a data subject may object, at any time, to the processing of personal information by the responsible party, on reasonable grounds relating to his/her particular situation, unless legislation provides for such processing. In order to object, the data subject must complete the standard "Objection" (Form 1) and submit it to the Information Officer at the postal or physical address or electronic mail address set out in section 5 of this Manual.

A data subject may also request the responsible party to correct or delete personal information about the data subject in its possession or under its control that is inaccurate, irrelevant, excessive, out of date, incomplete, misleading, or obtained unlawfully; or destroy or delete a record of personal information about the data subject that the responsible party is no longer authorised to retain records in terms of POPIA's retention and restriction of records provisions.

A Data Subject that wishes to request a correction or deletion of personal information or the destruction or deletion of a record of personal information must submit a request to the Information Officer at the postal or physical address or electronic mail address set out in section 5 of this Manual on the standard "Rectification" (Form 2). The Information Officer will handle the request in accordance with PAIA.

10. AVAILABILITY OF THE MANUAL (SECTION 51(1)(3))

The manual is available for inspection on our website at www.finglobal.com or at the offices of the company, free of charge.