

PAIA MANUAL

*Prepared in terms of section 51 of the
Promotion of Access to Information Act
2 of 2000 (as amended)*

DATE OF COMPILATION: 9 January 2023

DATE OF REVISION: 05 March 2025

1. DOCUMENT CONTENT

- [1. DOCUMENT CONTENT](#)
- [2. LIST OF ACRONYMS AND ABBREVIATIONS](#)
- [3. INTRODUCTION](#)
- [4. PURPOSE OF THE PAIA MANUAL](#)
- [5. BODY OVERVIEW](#)
- [6. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF Origin Fintech](#)
- [7. CATEGORIES OF RECORDS HELD \(UNRELATED TO POPIA\)](#)
- [8. CATEGORIES OF RECORDS HELD \(IN ACCORDANCE WITH OTHER LEGISLATION\)](#)
- [9. SUBJECTS OF INFORMATION HELD AND RELATED CATEGORIES OF RECORDS HELD](#)
- [10. CATEGORIES OF DATA SUBJECTS AND RELATED PERSONAL INFORMATION HELD](#)
- [11. REQUESTING ACCESS TO RECORDS & RELATED PROCESSES](#)
 - [11.1. Requesting Access](#)
 - [11.2. Grounds for Refusal of Access](#)
 - [11.3. Appeal Procedures](#)
 - [11.4. Supporting resources:](#)
- [12. INFORMATION SECURITY MEASURES FOR PROTECTING PERSONAL INFORMATION](#)
- [13. AVAILABILITY OF THE MANUAL](#)
- [14. UPDATING OF THE MANUAL](#)
- [ANNEXURE A](#)

2. LIST OF ACRONYMS AND ABBREVIATIONS

- | | | |
|-----|-----------------|---|
| 2.1 | CEO | Chief Executive Officer |
| 2.2 | DIO | Deputy Information Officer |
| 2.3 | IO | Information Officer |
| 2.4 | Minister | Minister of Justice and Correctional Services |
| 2.5 | PAIA | Promotion of Access to Information Act No2 Of 2000 (As Amended) |

2.6	PFMA	Public Finance Management Act No.1 of 1999 (As Amended)
2.7	POPIA	Protection of Personal Information Act No. 4 of 2013
2.8	Regulator	Information Regulator
2.9	Republic	Republic of South Africa

3. INTRODUCTION

3.1. The Promotion of Access to Information Act, 2000 (PAIA), gives effect to the constitutional right of access to information held by the state or private bodies, which is necessary to exercise or protect any rights. This PAIA Manual, as per Section 51 of PAIA, provides guidance to members of the public on how to request access to records held by Origin Fintech in a manner that aligns with the Protection of Personal Information Act, 2013 (POPIA) and ensures the protection of personal information.

4. PURPOSE OF THE PAIA MANUAL

4.1. This PAIA Manual is intended to assist the public in understanding and accessing information held by Origin Fintech. It provides the following information:

- 4.1.1. **Available Records:** Identifies categories of records that are accessible without the need for a formal PAIA request.
- 4.1.2. **Guidance on Access Requests:** Offers a clear process for requesting access to records, including a description of the types of records maintained by Origin Fintech and the subjects they cover.
- 4.1.3. **Records Available through Other Legislation:** Lists records that may be accessible through legislation other than PAIA.
- 4.1.4. **Contact Information:** Provides the contact details of the Information Officer and Deputy Information Officer, who are available to assist the public with questions and facilitate access to requested records.
- 4.1.5. **PAIA Guide:** Explains where to find the Information Regulator's guide on how to use PAIA, including how to obtain access to it.
- 4.1.6. **Processing of Personal Information:** Outlines Origin Fintech's approach to processing personal information, including:

- 4.1.7. **Purpose of Processing:** The reasons for collecting and processing personal information.
 - 4.1.8. **Categories of Data Subjects and Information:** The types of individuals whose data may be held and the categories of information stored.
 - 4.1.9. **Recipients of Personal Information:** The potential recipients of personal information, grouped by category.
 - 4.1.10. **International Data Transfers:** Indicates whether Origin Fintech transfers or processes personal information outside South Africa and identifies the categories of recipients involved.
 - 4.1.11. **Security Measures:** Describes the security measures to ensure the confidentiality, integrity, and availability of personal information processed by Origin Fintech.
- 4.2.** Through this information it will:
- 4.2.1. Assist requesters in accessing information in possession of Origin Fintech.
 - 4.2.2. Describe the categories of records held by Origin Fintech and outline the process for requesting access.
 - 4.2.3. Define the procedures for lodging a request for access to information.
- 4.3.** Explain the rights of requesters in terms of the grounds on which access may be refused.

5. BODY OVERVIEW

Origin Fintech processes information in accordance with the Protection of Personal Information Act. Any mention of Origin Fintech is to be understood to include related subsidiaries, including Origin Pay and Origin Rocket Insurtech. Information is collected and processed in accordance with the guidelines set out in the mentioned act.

- 5.1.** Processing Personal information for the following reasons
- 5.1.1. To comply with legal obligations
 - 5.1.2. To provide services
 - 5.1.3. To communicate with individuals
 - 5.1.4. To improve products or services
 - 5.1.5. To conduct research
 - 5.1.6. To protect the vital interests of the individual
 - 5.1.7. To prevent fraud
 - 5.1.8. To fulfil a contract
 - 5.1.9. To comply with a public interest task
 - 5.1.10. For underwriting purposes

5.1.11. For audit and record-keeping purposes

6. KEY CONTACT DETAILS FOR ACCESS TO INFORMATION OF Origin Fintech

6.1. Information Officer

Name: Chrisna Stander
Tel: 021 830 5222
Email: *Can be requested via our contact line on the Website*

6.2. Deputy Information Officer

Name: Sheldon Redman
Tel: 021 830 5222
Email: *Can be requested via our contact line on the Website*

6.3. Contact email to Access Information

Email: *Can be requested via our contact line on the Website*

6.4. Head Office:

Physical Address: Spaces Century City, No. 1 Bridgeway, Bridgeways
Precinct, Cape Town, South Africa, 7441
Telephone: 021 830 5222
Website: <https://www.originfintech.io>

7. CATEGORIES OF RECORDS HELD (UNRELATED TO POPIA)

These are mostly records that are either available on the website, and may be downloaded or requested telephonically or by sending an email or a letter to Origin Fintech. No formal request is required.

Category of Records	Types of the Record	Available on Website	Available upon request
Governance and Verification Information	Board of Directors, Governance Policies, Board Committees, Annual General Meeting, Licenses and Certifications, Privacy Policy		x
Financial Information	Annual Audited Financial Statements		x
Publicly Available Government Records	Government reports, publications, or documents.		x
Legal Records	Regulatory filings, court records, or public notices		x
Publicly Available Business Records	Company's products, services, or public announcements that are openly shared with the public	x	x

8. CATEGORIES OF RECORDS HELD (IN ACCORDANCE WITH OTHER OTHER LEGISLATION)

Below are the records which are created and available in accordance with any of the South African legislation.

Category of Records	Applicable Legislation
Memorandum of Incorporation	Companies Act 71 of 2008
PAIA Manual	Promotion of Access to Information Act 2 of 2000
POPIA Manual	Protection of Personal Information Act No.4 of 2013

9. SUBJECTS OF INFORMATION HELD AND RELATED CATEGORIES OF RECORDS HELD

The table below describes the subjects (i.e. Finance, SCM or HR), in respect of which the body holds records and the categories of records held on each subject.

Subjects on which the body holds records	Categories of Records
Strategic Documents, Plans, Proposals	<ul style="list-style-type: none"> • Budgets • Annual Reports • Strategic Plan • Annual Performance Plan • Funding and Investment Proposals • Policy- and Practices Documents • Investment pitches (Due Diligence)
Human Resources	<ul style="list-style-type: none"> • HR policies and procedures • Job Applicants and Leads records • Employees records • Payroll and Finances • Disciplinary Records • Training and Development Records and - Profiles
Company Sec and Governance	<ul style="list-style-type: none"> • Shareholder Records
Technical / Production	<ul style="list-style-type: none"> • Client Records • Supplier Records • Merchant Records • Customer Records • Product- and System Testing

10. CATEGORIES OF DATA SUBJECTS AND RELATED PERSONAL INFORMATION HELD

Below are the categories of data subjects and the description of the nature or categories of the personal information to be processed. Note that the nature or categories of personal information are dependent on the purpose of the body in performing its functions or services.

Categories of Data Subjects	Personal Information that may be processed
Employees	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Identification numbers (e.g. ID numbers, passport numbers), Gender, Marital status, Nationality, Employment history, Education and qualifications, Financial information (e.g. bank account numbers, credit card details), Medical information (e.g. health conditions, medical history, biometric information) employment status and bank details
Customers	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Financial information (e.g. bank account numbers, credit card details)
Suppliers	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Financial information (e.g. bank account numbers, credit card details)
Shareholders	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Identification numbers (e.g. ID numbers, passport numbers), Gender, Marital status, Nationality, Employment history, Education and qualifications, Financial information (e.g. bank account numbers, credit card details), Medical information (e.g. health conditions, medical history, biometric information)
Directors	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Identification numbers (e.g. ID numbers, passport numbers), Gender, Marital status, Nationality, Employment history, Education and qualifications, Financial information (e.g. bank account numbers, credit card details), Medical information (e.g. health conditions, medical history, biometric information)

Consultants	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Identification numbers (e.g. ID numbers, passport numbers), Gender, Marital status, Nationality, Employment history, Education and qualifications, Financial information (e.g. bank account numbers, credit card details), Medical information (e.g. health conditions, medical history, biometric information)
Job Applicants	Names and surnames, Contact details (e.g. phone numbers, email addresses, physical addresses), Identification numbers (e.g. ID numbers, passport numbers), Gender, Marital status, Nationality, Employment history, Education and qualifications, Financial information (e.g. bank account numbers, credit card details), Medical information (e.g. health conditions, medical history, biometric information)
Children	Names and surnames, birth certificates

10.1. The recipients or categories of recipients to whom the personal information may be supplied

Category of Personal Information	Recipients or Categories of Recipients to whom the personal information may be supplied
Identity number and names, for criminal checks and identity verification (FICA)	South African Police Services, Payroll- and Tax Management Third-Party, and other Funds for Legislative compliance
Qualifications, for qualification verifications	Universities and Training Providers
Credit and payment history, for credit information	Credit Bureaus, Banking Services, Third-Party Verification Services, Debt Collectors
Personal Details and Details of Organisations, Businesses etc.	Banking Services, Third-Party Verification Services, Debt Collectors
Personal Details	Labour- and employment-related services with Third-Party providers (Including leave management systems, application background checks, etc.)

Identity number and names, for criminal checks and identity verification (FICA), Credit and payment history, Personal Details and Details of Organisations, Businesses, et (For Legal Counsel).	Legalise Service Providers, Auditors Lawyers
Identity numbers and names, Credit and payment history, Personal Details and Details of Organisations, Businesses, et (For Audits).	Accounting Consultants and Third-Parties
Identity number and names, Credit and payment history, Personal Details and Details of Organisations, Businesses, et (For Capital Raise Ventures).	Venture Capitalists, Business Consultants

11. REQUESTING ACCESS TO RECORDS & RELATED PROCESSES

11.1. Requesting Access

11.1.1. Who May Request Access

11.1.1.1. Any person may request access to records of Origin Fintech if such access is necessary to exercise or protect their rights. In cases where personal information of a third party is involved, requesters must demonstrate sufficient legal grounds for accessing this information under PAIA.

11.1.2. Procedure for Making a Request

11.1.2.1. Requests must be made in writing using the prescribed PAIA Form C and directed to the Information Officer via [Company Email Address]. The form must be completed in full and must contain:

11.1.2.1.1. The requester’s full name, contact details, and identification or registration number

11.1.2.1.2. A detailed description of the records sought, including any reference numbers

11.1.2.1.3. How the requester wishes to receive access (e.g., paper or electronic copy)

11.1.2.2. Request Fees

11.1.2.2.1. A fee may be applicable for processing access requests as determined by PAIA regulations. If the request pertains to personal information, requesters are generally exempt

from fees. A schedule of applicable fees is available upon request.

11.2. Grounds for Refusal of Access

- 11.2.1. Certain records may be exempt from disclosure if such disclosure would:
 - 11.2.1.1. Lead to an unreasonable invasion of privacy of a third party
 - 11.2.1.2. Compromise the security or strategic interests of Origin Fintech or the state
 - 11.2.1.3. Reveal confidential commercial information of a third party
 - 11.2.1.4. Include legally privileged information
- 11.2.2. The Information Officer will provide reasons in writing if access is refused

11.3. Appeal Procedures

- 11.3.1. If a requester's application for access to information is denied, they may lodge an internal appeal within 30 days of the decision. Appeals are submitted to the Information Officer and must be supported by relevant documentation and reasons for the appeal.
- 11.3.2. Should the internal appeal be unsuccessful, requesters may approach the Information Regulator or the courts for further recourse.

11.4. Supporting resources:

- 11.4.1. The Information Regulator's website ([link](#)) provides the following documents for the public and data subjects to make specific requests and raise issues and concerns.
 - 11.4.1.1. Form 01: [Request for a Guide from the Regulator](#) [Regulation 2]
 - 11.4.1.2. Form 01: [Request for a Copy of the Guide from an Information Officer](#) [Regulations 3]
 - 11.4.1.3. Form 02: [Request for Access to Record](#) [Regulation 7]
 - 11.4.1.4. Form 03: [Outcome of request and of fees payable](#) [Regulation 8]
 - 11.4.1.5. Form 04: [Internal Appeal Form](#) [Regulation 9]
 - 11.4.1.6. Form 05: [Complaint Form](#) [Regulation 10]
 - 11.4.1.7. Form 13: [PAIA Request for Compliance Assessment Form](#) [Regulation 14(1)]

12. INFORMATION SECURITY MEASURES FOR PROTECTING PERSONAL INFORMATION

12.1. Origin Fintech implements comprehensive security measures to ensure the confidentiality, integrity, and availability of personal information. Key measures include:

12.1.1. Access Controls

12.1.1.1. Strong authentication methods like passwords, two-factor, or biometric authentication.

12.1.1.2. Role-based access controls (RBAC) to limit access based on job duties.

12.1.1.3. Regular updates to access privileges and secure physical access controls, particularly in server rooms and other secure areas.

12.1.2. Data Encryption

12.1.2.1. Encryption of sensitive data during transmission, using secure protocols (e.g., SSL/TLS).

12.1.2.2. Protection for all data moving through networks with industry-standard encryption.

12.1.3. Network Security

12.1.3.1. Firewalls, intrusion detection, and secure wireless networks to protect against unauthorised access.

12.1.3.2. Regular updates and monitoring for network integrity.

12.1.4. Secure Software Development

12.1.4.1. Secure coding practices and regular testing to identify and resolve vulnerabilities.

12.1.4.2. Up-to-date software patches and frameworks to prevent security gaps.

12.1.5. Incident Response and Recovery

12.1.5.1. A detailed incident response plan for rapid response to any data breach or incident.

12.1.5.2. Routine backups of critical data and regular testing of restoration processes.

12.1.6. Physical Security

12.1.6.1. Restricted physical access to servers and data centres.

12.1.6.2. Environmental controls to protect equipment and data integrity.

12.1.7. Employee Awareness and Training

- 12.1.7.1. Regular training on security best practices, including policies on handling sensitive data and company devices.
- 12.1.7.2. Clear guidelines for prompt reporting of security incidents.
- 12.1.8. Vendor Management
 - 12.1.8.1. Careful vetting of third-party vendors to ensure they meet security standards.
- 12.1.9. Regular Audits and Compliance
 - 12.1.9.1. Security audits by independent professionals to detect and address vulnerabilities.
 - 12.1.9.2. Compliance with laws and regulations like POPIA, and alignment with standards such as ISO 27001 where relevant.

13. AVAILABILITY OF THE MANUAL

13.1. A copy of the Manual is available-

- 13.1.1. on the body's [website](#).
- 13.1.2. head office of Origin Fintech for public inspection during normal business hours;
- 13.1.3. to any person upon request and upon the payment of a reasonable prescribed fee; and
- 13.1.4. to the Information Regulator upon request.

13.2. A fee for a copy of the Manual, as contemplated in Annexure A of the Regulations, shall be payable per each A4-size photocopy made (or alternative sharing methods). All fees related to searching and preparing records for disclosure to private bodies are capped at the amount specified in the Act.

14. UPDATING OF THE MANUAL

The Information Officer of Origin Fintech will regularly update this manual.

Issued by:

.....

Origin Fintech (Pty) Ltd

By: Lloyd Poelmann

.....

Information Regulator

By: Chrisna Stander

ANNEXURE A

BREAKDOWN OF FEES CONCERNING GETTING ACCESS TO INFORMATION

1. Overview of Section 54 of PAIA

Private bodies are governed by the Promotion of Access to Information Act as to what fees they must charge and in what situations.

- 1.1.1. The specifics may be viewed on the Information Regulator's website ([Link](#))

2. Costs Overview

Below is a list of costs that Origin Fintech may charge for requests to share access to data. These prices include VAT.

Item	Description	Amount
1.	Request fee, payable by every requester	R140.00
2.	Printed black & white copy for every A4 page	R2.00 per page
3.	Printed copy (A4)	R2.00 per page
4.	For a digital copy <ul style="list-style-type: none"> • Device (device must be provided) 	R40.00
5.	An Audio record may be converted upon request. This will be outsourced	Outsourced and billed as per the outsourced party's fees
6.	Every additional hour (excluding the first hour) required to prepare the record for sharing	R145.00
7.	Email	None