KOCHO SA (PTY) LTD

PAIA MANUAL

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

Date of compilation: 28/10/25
Date of revision: 28/10/26

1 Definitions

Term	Definition
CEO	Chief Executive Officer
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

Term	Definition
Writing	As referred to in section 12 of the Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)

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 the Kocho SA (Pty) Ltd

3.1 Chief Information Officer

Name	Ricardo Canovi
Contact number	083 414 6979
Email address	ricardo.canovi@kocho.co.uk

3.2 Deputy Information Officer

Name	Candice Pienaar
Contact number	0824774026
Email address	candice.pienaar@kocho.co.uk

3.3 General contacts for access to information

Email address	candice.pienaar@kocho.co.uk

3.4 National or head office

Physical address	Waterford Place, Waterford House, No.2, First Floor, Century City, 7441
Contact number	0824774026
Email	candice.pienaar@kocho.co.uk
Website	www.kocho.co.uk

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;

[1] Section 56(a) of POPIA - Each public and private body must make provision, in the manner prescribed in section 17 of the Promotion of Access to Information Act, with the necessary changes, for the designation of such a number of persons, if any, as deputy information officers as is necessary to perform the duties and responsibilities as set out in section 55(1) of POPIA

[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.

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:
4.5.1 Upon request to the IO.
4.5.2 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.

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] 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.

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 Kocho SA (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	Company's current PAIA Manual and any revisions thereto.	X	X
Company overview	Company profile, business activities (cybersecurity, identity and access management, cloud infrastructure, digital transformation solutions), and contact details.	X	X
Policies (public-facing)	Privacy Policy, Website Cookies Policy, POPIA Notice, and Data Protection Statement outlining how personal information is processed and secured.	X	X
Legal disclosures	Terms of Service, Website Terms & Conditions, and standard contractual clauses for data protection and confidentiality.	X	X
News and announcements	Press releases, service updates, cybersecurity advisories, thought leadership articles, and corporate announcements.	X	X
Public marketing materials	Brochures, whitepapers, case studies, service descriptions (cybersecurity consulting, identity management, cloud enablement), and promotional content.	X	X
Certifications and Accreditations	Copies of relevant industry certifications such as ISO 27001 (Information Security Management), Microsoft Partner accreditations, and cloud compliance certifications.	X	X
POPIA and PAIA awareness training certificates	Records of staff participation in data protection (POPIA) and access to information (PAIA) training sessions.	X	X
Supplier and Partner Information	Partner program details, B-BBEE certificate, and compliance declarations for IT service providers and cloud vendors.	X	X
Contact information for IO	Name, designation, email address, telephone number, and registered business address for the	X	X

Category of Records	Types of the Record	Available on Website	Available on Request
	Information Officer and/or Deputy Information Officer(s).		

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

Category of Records	Applicable Legislation	Department/ Subject Area
Memorandum of Incorporation, company registration documents, board resolutions, minutes of meetings, share register	Companies Act, 71 of 2008	Directors
Employment contracts, employee files, payroll records, and attendance registers	Basic Conditions of Employment Act, 75 of 1997	Human Resources (HR)
Disciplinary records, grievance procedures, internal hearings, CCMA documentation	Labour Relations Act, 66 of 1995	HR
Employment Equity (EE) plans, EE reports, committee meeting minutes	Employment Equity Act, 55 of 1998	HR
UIF declarations, contribution records, and employee benefit claims	Unemployment Insurance Act, 63 of 2001	HR
Occupational health and safety records, incident reports, risk assessments, emergency plans	Occupational Health and Safety Act, 85 of 1993	Health and Safety
Tax and payroll submissions, IRP5 certificates, PAYE and VAT records, SARS correspondence	Income Tax Act, 58 of 1962; Value-Added Tax Act, 89 of 1991	Finance
POPIA compliance records (operator agreements, consent forms, privacy impact assessments, security incident logs)	Protection of Personal Information Act, 4 of 2013	Legal and Compliance
PAIA Manual, access request logs, training attendance registers	Promotion of Access to Information Act, 2 of 2000	Legal and Compliance
Information security, IT governance policies, cybersecurity frameworks, incident response logs, penetration test reports	Cybercrimes Act, 19 of 2020; Electronic Communications and Transactions Act, 25 of 2002	Information Technology (IT) / Cybersecurity
Cloud service and data hosting agreements, software licenses, and vendor contracts	Consumer Protection Act, 68 of 2008; POPIA, 4 of 2013	Client Services
Client contracts, service level agreements (SLAs), and support logs	Consumer Protection Act, 68 of 2008	Client Services/ Marketing

Category of Records	Applicable Legislation	Department/ Subject Area
Financial statements, audit reports, and general accounting records	Companies Act, 71 of 2008; Auditing Profession Act, 26 of 2005	Finance
Document retention and disposal schedules, archive and destruction logs	National Archives and Records Service Act, 43 of 1996	HR/ Relevant Departments

**Although we have used our best endeavours to supply a list of applicable legislation, it is possible that this list may be incomplete. Whenever it comes to our attention that existing or new legislation allows a Requester access on a basis other than as set out in PAIA, we shall update the list accordingly. If a Requester believes that a right of access to a record exists in terms of other legislation listed above or any other legislation, the Requester is required to indicate what legislative right the request is based on, to allow the Information Officer the opportunity of considering the request in light thereof.*

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.

10 Remedies Should a Request be Refused

10.1 If the company does not have an internal appeal procedure in light of a denial of a request, decisions made by the IO is final.

10.2 The requestor may in accordance with sections 56(3) (c) and 78 of PAIA, apply to a court for relief within 180 (one-hundred-and-eighty) days of notification of the decision for appropriate relief.

11 Fees

The following fees shall be payable upon request by a requestor:

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

Details	Fee
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 manage client and partner relationships, including onboarding, contract administration, and account management.
12.1.2. To respond to enquiries, service requests, technical support tickets, and incident reports from clients or partners.
12.1.3. To process payments for services rendered, including invoicing, billing, account reconciliations, and financial reporting.
12.1.4. For user authentication, access control, and identity verification across cloud platforms and cybersecurity systems..
12.1.5. To ensure compliance with data protection, cybersecurity, and information governance frameworks (including POPIA, GDPR, and ISO standards).
12.1.6. To communicate with clients, service providers, and technology partners in the execution of projects and service delivery
12.1.7. To monitor, detect, and investigate cybersecurity threats, breaches, or unauthorised system access, and to take corrective action.
12.1.8. To conduct penetration tests, risk assessments, and IT audits as part of ongoing compliance and information security assurance.
12.1.9. To perform internal employee management functions, including recruitment, payroll, performance monitoring, and access provisioning.
12.1.10. To manage supplier relationships, procurement processes, and vendor compliance (including confidentiality and operator agreements)
12.1.11. To conduct market research, client satisfaction surveys, and marketing campaigns (where consent has been obtained).
12.1.12. To maintain business continuity, disaster recovery, and secure data backup operations (including cloud-hosted environments).
12.1.13. To comply with regulatory, financial, and legal obligations applicable to IT, cybersecurity, and data management industries.

12.1.14. To support dispute resolution, claims investigations, or audit requests from clients, regulators, or service partners.
12.1.15. To develop, enhance, and test new security and technology solutions offered by Kocho SA.
12.1.16. To store, retain, and archive data in accordance with legal, contractual, and operational retention requirements.
12.1.17. For any other legitimate business purpose aligned with the provision of cybersecurity, identity management, and cloud infrastructure services.

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	Company name, registration number, VAT number, business address, contact details of client representatives, email correspondence, service contracts, authentication and user access information, system usage logs, and billing details.
End-Users (Authorised System Users)	Full name, username, login credentials, identity verification data, multi-factor authentication records, IP addresses, device IDs, system activity logs, and email or communication metadata (collected for security purposes).
Service Providers / Technology Partners	Company registration number, VAT number, address, technical contact details, confidentiality agreements, service and compliance certifications (e.g., ISO/IEC 27001), and banking details for payment.
Employees	Full name, ID number, contact details, residential address, tax number, bank details, employment contracts, payroll data, disciplinary records, training and certification records (e.g., cybersecurity or cloud certifications), performance appraisals, emergency contacts, and demographic information (race/gender for Employment Equity).
Job Applicants	Full name, contact details, CV, employment history, qualifications, references, background screening results (including criminal or credit checks, if applicable), and interview assessment records.
Contractors / Freelancers	Full name, ID or company registration number, contact details, tax and banking information, signed contracts, cybersecurity clearances, confidentiality or non-disclosure agreements (NDAs), and proof of professional qualifications.
Visitors / Guests	Full name, contact details, vehicle registration details, visitor sign-in logs, CCTV footage, and access control data for security purposes.
Regulatory and Compliance Bodies	Contact details of liaison officers, registration information, audit and compliance correspondence, certification records, and inspection reports.
Shareholders / Directors	Full name, ID or registration number, contact information, ownership details, financial information (e.g., dividends, investment records), and correspondence with the company.
IT / System Users	Usernames, access credentials, system permissions, device and IP information, activity logs, biometric or

	token-based authentication data, and cybersecurity incident response logs.
Marketing / Newsletter Subscribers	Name, company, email address, phone number, consent preferences (opt-in/opt-out), industry interest areas, and communication engagement history.

13. 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 or background checks)	South African Police Service (SAPS); accredited background screening agencies; or authorised verification partners.
Qualifications and professional certifications (for competency verification)	South African Qualifications Authority (SAQA); accredited training and certification institutions (e.g., cybersecurity or cloud training bodies).
Credit and payment history (for billing and supplier verification)	Financial institutions; credit bureaus; auditors; and authorised debt recovery or financial compliance partners.
Employment history, references, and vetting data)	Previous employers; recruitment agencies; professional background verification service providers.
Banking details and payment details	Financial institutions; payroll administrators; payment processors; and accounting auditors (for salary or supplier payments).
Health information (for employment-related wellness and compliance)	Approved occupational health practitioners; medical aid providers; and authorised employee wellness service providers.
Identity verification and access management data (e.g., login credentials, authentication logs, biometrics)	Cloud infrastructure providers (e.g., Microsoft Azure, AWS, Google Cloud); identity management system partners; cybersecurity monitoring teams.
IT system and cybersecurity logs (e.g., IP addresses, device IDs, access activity)	Internal IT and cybersecurity teams; managed security service providers (MSSPs); system monitoring or threat detection vendors.
Client project and service data	Authorised employees, technical teams, subcontractors, and cloud platform partners (under operator or confidentiality agreements).
Regulatory and compliance documentation	Information Regulator; auditors; relevant industry compliance bodies (e.g., ISO certification authorities).
Skills development and training records	Sector Education and Training Authorities (SETAs); professional development institutions; and internal HR departments.
CCTV footage, access control logs, and building entry data	Authorised internal security teams; facilities management service providers; and law enforcement authorities (if required).
Marketing, events, or communication-related contact data	Marketing department; CRM platform operators; approved third-party communication service providers (under POPIA-compliant operator agreements).

14. Planned Transborder Flows of Personal Information

Kocho SA (Pty) Ltd may transfer or store certain categories of personal information outside the Republic of South Africa, primarily through the use of cloud-based service providers, payment gateways, marketing platforms, and IT hosting providers. These service providers may be located in jurisdictions such as the United States of America, the European Union, and other regions where global service providers host their systems.

The country in which personal information will be stored
UK
Manila

14.1. The Company 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 kocho.co.uk or at any head office of Kocho SA (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 Kocho SA (Pty) Ltd will update this manual on a regular basis.

Name of IO	Ricardo Canovi
Title of the head of the body	Country Director

APPLICABLE FORMS

PAIA Forms

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

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