



**PROMOTION OF ACCESS TO INFORMATION
ACT (PAIA) MANUAL**

VAYU COACHING TECHNOLOGIES (PTY) LTD

Prepared in terms of Section 51 of the Promotion of Access to Information Act, 2000 (Act No. 2 of 2000), as amended

1. INTRODUCTION

VAYU Coaching Technologies (Pty) Ltd ("the Company") is a South African private company providing life coaching, executive coaching, personal development coaching, digital marketing services, digital content creation services, mobile application development services, and AI-powered coaching technology solutions.

The Company operates under the trading names:

- VAYU
- Vayu Life Coaching

The Company is committed to promoting transparency, accountability, and lawful access to information in accordance with the Promotion of Access to Information Act, 2000 ("PAIA"), and the Protection of Personal Information Act, 2013 ("POPIA").

This Manual serves as a guide to members of the public who wish to request access to records held by the Company and provides information regarding the Company's processing of personal information.

2. COMPANY PARTICULARS

Registered Name

VAYU Coaching Technologies (Pty) Ltd

Registration Number

2026/430224/07

Physical Address

134 Ranger Road
Fish Hoek
Cape Town
7975
Western Cape
South Africa

Postal Address

Same as Physical Address

General Contact Information

Telephone: +27 62 899 2522

Email: compliance@vayulifecoaching.co.za

Websites

vayu.coach

vayulifecoaching.co.za

vayulifecoaching.online

3. INFORMATION OFFICER

In accordance with POPIA and PAIA, the Chief Executive Officer of the Company serves as the Information Officer.

Information Officer

Chris Roos

Position:

Founder, Chief Executive Officer, Director, and Information Officer

Telephone:

+27 62 732 1090

Email:

chris.roos@vayulifecoaching.co.za

The Information Officer is responsible for ensuring compliance with PAIA, POPIA, and all applicable information governance obligations.

4. COMPANY OVERVIEW

The Company conducts business within the following sectors:

- Life Coaching
- Executive Coaching
- Personal Development Coaching
- AI-Powered Coaching Services
- Mobile Application Development
- Digital Marketing Services
- Digital Content Creation
- Coaching Technology Platforms

The Company develops and operates technology solutions, including mobile applications and digital platforms designed to assist individuals in personal growth, goal achievement, accountability, habit formation, coaching, and wellbeing-related activities.

The Company may process personal information obtained from clients, prospective clients, platform users, contractors, suppliers, employees, service providers, and business partners in the course of conducting its operations.

5. GUIDE ON HOW TO USE PAIA

A guide on how to exercise rights under the Promotion of Access to Information Act is available from the Information Regulator of South Africa.

The guide contains information regarding:

- The objectives of PAIA
- The process for requesting access to records
- The rights of requesters
- Applicable fees
- Available remedies

Copies of the guide may be obtained from the Information Regulator.

6. RECORDS AVAILABLE WITHOUT FORMAL REQUEST

The following categories of information are generally available without the need to submit a formal PAIA request:

- Public website content
- Marketing materials
- Blog articles
- Social media publications
- Publicly available service descriptions
- Company contact information
- Promotional materials
- Press releases
- Publicly distributed educational resources
- Published policies intended for public access

The Company reserves the right to determine whether specific information falls within these categories.

7. RECORDS HELD IN TERMS OF OTHER LEGISLATION

The Company retains records in accordance with applicable South African legislation. The following list is not exhaustive but includes the primary legislation governing records held by the Company.

Corporate and Governance Records

- Companies Act, 2008 (Act No. 71 of 2008)
- Companies Regulations, 2011

Examples of records:

- Memorandum of Incorporation (MOI)
- Shareholder records
- Director resolutions
- Statutory company records
- Annual returns and related filings

Tax and Financial Records

- Income Tax Act, 1962 (Act No. 58 of 1962)
- Tax Administration Act, 2011 (Act No. 28 of 2011)
- Value Added Tax Act, 1991 (Act No. 89 of 1991) where applicable

Examples of records:

- Tax returns
- Financial statements
- Accounting records
- Invoices
- Bank statements
- Supporting tax documentation

Employment and Labour Records

Where applicable, the Company maintains records in terms of:

- Basic Conditions of Employment Act, 1997 (Act No. 75 of 1997)
- Labour Relations Act, 1995 (Act No. 66 of 1995)
- Employment Equity Act, 1998 (Act No. 55 of 1998)
- Unemployment Insurance Act, 2001 (Act No. 63 of 2001)
- Compensation for Occupational Injuries and Diseases Act, 1993 (Act No. 130 of 1993)

Examples of records:

- Employment contracts
- Payroll records
- Leave records
- Performance records
- Recruitment documentation

Information and Data Protection Records

- Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)
- Protection of Personal Information Act, 2013 (Act No. 4 of 2013)
- Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)

Examples of records:

- Privacy notices
- Consent records
- Data processing records
- Information access requests
- Information security records

Consumer and Commercial Records

Where applicable:

- Consumer Protection Act, 2008 (Act No. 68 of 2008)

Examples of records:

- Client agreements
- Service agreements
- Customer communications
- Complaints records
- Refund records

Intellectual Property Records

- Copyright Act, 1978 (Act No. 98 of 1978)
- Trade Marks Act, 1993 (Act No. 194 of 1993)

Examples of records:

- Intellectual property registrations
- Trademark documentation
- Copyright-protected materials
- Brand assets

Electronic Communications and Digital Platform Records

- Electronic Communications and Transactions Act, 2002 (Act No. 25 of 2002)

Examples of records:

- Electronic communications
- Website records
- Application records
- Digital transaction records
- Electronic agreements

The Company may retain additional records as required by any other legislation applicable to its operations from time to time.

8. CATEGORIES OF RECORDS HELD BY THE COMPANY

The Company creates, receives, processes, stores, and maintains records in physical and electronic form in the ordinary course of business.

Access to these records may be subject to the provisions of PAIA, POPIA, contractual obligations, confidentiality requirements, and any other applicable legislation.

The categories below are intended as a general guide and do not guarantee that a particular record exists or will be accessible upon request.

8.1 Corporate Governance Records

The Company may maintain records relating to:

- Company registration documents
- Memorandum of Incorporation (MOI)
- Shareholder records
- Director records
- Board and management resolutions
- Corporate governance policies
- Statutory registers
- Regulatory filings
- Annual returns
- Compliance documentation
- Licences and registrations

8.2 Financial and Accounting Records

The Company may maintain records relating to:

- Financial statements
- Accounting records
- Tax returns
- VAT records (where applicable)
- Bank statements
- Invoices
- Payment records
- Expense records
- Audit records
- Budgets and forecasts
- Cash flow records
- Supplier payments
- Merchant account transactions
- Subscription revenue records

8.3 Human Resources Records

Where applicable, the Company may maintain records relating to:

- Employment applications
- Curriculum vitae
- Employment contracts
- Contractor agreements
- Performance records
- Leave records
- Payroll records
- Training records
- Disciplinary records
- Termination records
- Occupational health and safety records

8.4 Client and Coaching Records

The Company may maintain records relating to coaching clients, including:

- Coaching agreements
- Client onboarding documentation
- Identity verification information
- Assessment questionnaires
- Discovery session records
- Goal-setting documentation
- Progress reports
- Accountability records
- Coaching notes
- Session summaries
- Scheduling records
- Communication records
- Payment records
- Client feedback and testimonials

The Company recognises that coaching relationships frequently involve confidential and sensitive personal information. Access to such information may be restricted in accordance with applicable law.

8.5 Prospective Client and Lead Records

The Company may maintain records relating to prospective clients and business leads, including:

- Contact information
- Discovery call records
- Lead generation records
- Marketing campaign responses
- Website enquiry forms
- Consultation requests
- Sales correspondence
- CRM records

8.6 Customer and User Records

The Company may maintain records relating to users of its websites, applications, digital platforms, products, and services, including:

- User account information
- Registration records
- Subscription information
- Login activity
- User preferences
- Service usage records
- Customer support interactions
- Product feedback
- Billing information
- Communication history

8.7 Technology Platform Records

The Company develops and operates digital platforms and may maintain records including:

- User account records
- Platform activity records
- Application usage analytics
- Feature usage data
- Technical support requests
- Error logs
- System monitoring information
- Security monitoring records
- Application performance records
- Software development documentation
- System architecture documentation
- Technical specifications

8.8 User-Generated Content Records

The Company may maintain records created or submitted by users, including:

- Journal entries
- Written reflections
- Goal tracking information
- Habit tracking information
- Uploaded content
- Responses to assessments
- Notes created within the platform
- Coaching-related submissions
- Feedback submissions

8.9 Artificial Intelligence Interaction Records

Where AI-powered services are used, the Company may maintain records including:

- AI interaction logs
- Prompt submissions
- AI-generated responses
- Conversation history
- Usage analytics
- Feedback regarding AI-generated content
- System monitoring information

The Company does not guarantee that all AI-generated content is permanently retained and reserves the right to establish retention limits for operational, legal, security, and technical purposes.

8.10 Marketing and Communications Records

The Company may maintain records relating to marketing activities, including:

- Marketing campaigns
- Newsletter subscriptions
- Mailing lists
- Website analytics
- Advertising performance data
- Social media interactions
- Content engagement data
- Event registrations
- Promotional communications
- Lead generation activities

8.11 Supplier and Service Provider Records

The Company may maintain records relating to suppliers, contractors, and service providers, including:

- Service agreements
- Supplier onboarding documentation
- Invoices
- Payment records
- Contact information
- Due diligence records
- Compliance documentation

8.12 Legal and Compliance Records

The Company may maintain records relating to:

- Contracts and agreements
- Legal opinions
- Litigation records
- Complaints and dispute records
- PAIA requests
- POPIA compliance documentation
- Information security documentation
- Regulatory correspondence
- Compliance audits
- Risk management records

8.13 Information Security Records

The Company may maintain records relating to:

- Access control logs
- Security incident reports
- Vulnerability assessments
- Security monitoring records
- Data breach investigations
- Backup and recovery records
- Information security policies
- Cybersecurity controls and procedures

9. PROCESSING OF PERSONAL INFORMATION IN TERMS OF POPIA

9.1 Introduction

VAYU Coaching Technologies (Pty) Ltd recognises the constitutional right to privacy and is committed to processing personal information lawfully, reasonably, transparently, and securely in accordance with the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) ("POPIA").

The Company processes personal information only where such processing is necessary for legitimate business purposes, contractual obligations, legal obligations, consent-based activities, or the legitimate interests of the Company and its data subjects.

9.2 Categories of Data Subjects

The Company may process personal information relating to the following categories of data subjects:

Clients

Individuals receiving coaching, consulting, digital services, or related professional services from the Company.

Prospective Clients

Individuals who enquire about services, request consultations, subscribe to communications, or engage with the Company's marketing activities.

Platform Users

Individuals who create accounts, access, or use the Company's websites, applications, digital platforms, products, or services.

Employees

Current, former, and prospective employees of the Company.

Contractors and Service Providers

Independent contractors, consultants, suppliers, and service providers engaged by the Company.

Business Partners

Individuals representing strategic partners, affiliates, referral partners, and professional service providers.

Website Visitors

Individuals who visit the Company's websites or interact with online content.

9.3 Categories of Personal Information Processed

Depending on the nature of the relationship with the data subject, the Company may process:

Identification Information

- Full names
- Identity numbers
- Passport numbers
- Date of birth
- Gender
- Nationality

Contact Information

- Telephone numbers
- Mobile numbers
- Email addresses
- Physical addresses
- Postal addresses

Account Information

- Usernames
- Passwords (stored in encrypted or hashed form where applicable)
- Account preferences
- Subscription information

Financial Information

- Banking details
- Billing information
- Payment history
- Transaction records

Employment Information

- Employment history
- Qualifications
- Curriculum vitae
- Performance-related records

Coaching and Development Information

- Personal goals
- Assessments
- Coaching responses
- Reflection exercises
- Progress tracking information
- Personal development records
- Accountability records

Platform Usage Information

- Device information
- Browser information
- Operating system information
- IP addresses
- Login activity
- Usage analytics
- Feature interaction data

User-Generated Content

- Journal entries
- Written reflections
- Notes
- Uploaded content
- Goal tracking data
- Habit tracking information

Communication Information

- Email correspondence
- Contact form submissions
- Support requests
- Survey responses
- Feedback submissions

Special Personal Information

The Company does not intentionally collect special personal information unless such information is voluntarily provided by the data subject and is reasonably necessary for the provision of coaching, support services, legal compliance, or platform functionality.

Where special personal information is processed, appropriate safeguards will be implemented in accordance with POPIA.

9.4 Purpose of Processing Personal Information

The Company may process personal information for the following purposes:

Service Delivery

- Delivering coaching services
- Delivering consulting services
- Managing client relationships
- Providing customer support
- Administering subscriptions

Platform Operation

- Creating and managing user accounts
- Authenticating users
- Providing platform functionality
- Maintaining system security
- Monitoring platform performance

Personal Development and Coaching Support

- Tracking goals and progress
- Delivering coaching programmes
- Facilitating accountability processes
- Providing personalised experiences

Artificial Intelligence Services

- Generating AI-assisted coaching responses
- Providing AI-driven guidance and recommendations
- Improving user experiences
- Monitoring platform effectiveness

Business Administration

- Billing and invoicing
- Financial reporting
- Record keeping
- Regulatory compliance
- Risk management

Marketing and Communication

- Sending newsletters
- Delivering educational content
- Promoting products and services
- Conducting market research
- Measuring marketing effectiveness

Legal and Regulatory Compliance

- Meeting statutory obligations
 - Responding to lawful requests
 - Exercising legal rights
 - Defending legal claims
-

9.5 Recipients of Personal Information

Personal information may be disclosed to authorised third parties where necessary to conduct business operations.

Such recipients may include:

Professional Advisors

- Accountants
- Auditors
- Legal advisors
- Compliance consultants

Technology Service Providers

- Cloud hosting providers
- Software providers
- Analytics providers
- CRM providers
- Payment processors

Financial Institutions

- Banks
- Payment gateways
- Financial service providers

Regulatory Authorities

- SARS
- CIPC
- Information Regulator
- Courts and tribunals
- Law enforcement agencies where legally required

Personal information will not be sold to third parties.

9.6 International Transfer of Personal Information

The Company may utilise technology platforms, cloud-based systems, and service providers located outside South Africa.

Personal information may therefore be transferred to, processed in, or stored in jurisdictions outside South Africa.

Examples of such service providers may include:

- Google Workspace
- OpenAI
- Anthropic Claude
- HubSpot
- Xero
- Other cloud infrastructure providers utilised from time to time

Where cross-border transfers occur, the Company will take reasonable steps to ensure that appropriate safeguards are implemented and that personal information receives an adequate level of protection consistent with applicable legal requirements.

9.7 Security Safeguards

The Company implements reasonable technical and organisational measures designed to protect personal information against:

- Loss
- Misuse
- Unauthorised access
- Unauthorised disclosure
- Alteration
- Destruction

Such measures may include:

- Access controls
- Password protection
- Multi-factor authentication
- Encryption technologies
- Secure cloud storage
- Security monitoring
- Employee and contractor confidentiality obligations
- Regular software updates
- Data backup procedures

No electronic transmission or storage method can be guaranteed to be completely secure, and the Company cannot guarantee absolute security.

9.8 Retention of Personal Information

Personal information will be retained only for as long as necessary to:

- Fulfil the purpose for which it was collected
- Meet contractual obligations
- Comply with legal and regulatory requirements
- Resolve disputes
- Enforce agreements

The Company may securely destroy, anonymise, or de-identify personal information when retention is no longer required.

9.9 Rights of Data Subjects

Subject to applicable law, data subjects may have the right to:

- Request access to personal information
- Request correction of inaccurate information
- Request deletion of information where legally permissible
- Object to certain forms of processing
- Withdraw consent where processing is consent-based
- Lodge complaints with the Information Regulator

Requests relating to personal information should be directed to the Information Officer using the contact details contained in this Manual.

10. REQUEST PROCEDURE FOR ACCESS TO RECORDS

10.1 Right of Access

In accordance with the Promotion of Access to Information Act, 2000 ("PAIA"), any person may request access to records held by the Company.

Access to records will be granted where:

- The requirements of PAIA have been satisfied;
- No lawful grounds for refusal apply; and
- Any applicable fees have been paid.

The submission of a request does not automatically entitle the requester to access the requested record.

Each request will be assessed on its own merits in accordance with PAIA and any other applicable legislation.

10.2 Submission of Requests

Requests for access to records must be submitted to the Information Officer using the prescribed PAIA Request for Access Form (Form 2) as published by the Information Regulator.

The completed request form, together with any supporting documentation, must be submitted to:

Information Officer

Chris Roos

Founder, Chief Executive Officer, Director and Information Officer

Email:

chris.roos@vayulifecoaching.co.za

Physical Address:

134 Ranger Road

Fish Hoek

Cape Town

7975

Western Cape

South Africa

General Compliance Email:

compliance@vayulifecoaching.co.za

10.3 Required Information

The requester must provide sufficient information to enable the Company to:

- Identify the requester;
- Verify the identity of the requester where necessary;
- Identify the record being requested;
- Determine the form of access required;
- Determine whether any third parties may be affected by the request;
- Communicate with the requester regarding the request.

Where a request is made on behalf of another person, proof of authority to act on behalf of that person may be required.

10.4 Description of the Requested Record

Requesters should provide as much detail as possible regarding the requested record, including:

- The nature of the record;
- The subject matter of the record;
- The approximate date of the record;
- The individuals or departments likely to hold the record;
- Any reference numbers, account numbers, or identifiers where applicable.

Failure to provide sufficient information may delay the processing of the request.

10.5 Processing of Requests

Upon receipt of a valid request, the Company will:

1. Review the request;
2. Determine whether the requested record exists;
3. Consider whether access may lawfully be granted;
4. Determine whether third-party consultation is required;
5. Calculate any applicable fees;
6. Notify the requester of the outcome.

The Company reserves the right to request additional information where necessary to process a request.

10.6 Timeframes

The Company will endeavour to respond to requests within the time periods prescribed by PAIA.

The Information Officer will notify the requester:

- Whether access has been granted;
- Whether access has been refused;
- Whether additional information is required;
- Whether an extension is necessary.

Where permitted by law, the response period may be extended if:

- The request involves a large volume of records;
- Additional searches are required;
- Consultation with third parties is necessary;
- The circumstances otherwise justify an extension.

The requester will be informed of any extension and the reasons for it.

10.7 Form of Access

Where access is granted, records may be provided in a form reasonably determined by the Company, including:

- Inspection of physical records;
- Electronic copies;
- Printed copies;
- Email delivery;
- Other reasonable formats where available.

The Company is not required to create new records in response to a request where no such record already exists.

10.8 Requests Involving Personal Information

Where a request involves personal information relating to another individual, the Company may require additional verification and may refuse access where disclosure would unreasonably infringe the privacy rights of another person.

Requests for personal information will be evaluated in accordance with both PAIA and POPIA.

10.9 Third-Party Records

Where a requested record contains information relating to a third party, the Company may be required to:

- Notify the affected third party;
- Provide the third party with an opportunity to make representations;
- Consider any objections received before making a final decision.

This process may affect the timeframe for responding to the request.

10.10 Internal Records and Confidential Information

Certain records may contain:

- Confidential commercial information;
- Proprietary methodologies;
- Intellectual property;
- Trade secrets;
- Coaching methodologies;
- AI system information;
- Software development information;
- Security-related information.

Access to such records may be restricted where permitted by law.

10.11 Notification of Outcome

The Information Officer will notify the requester in writing of:

- The decision reached;
 - Any applicable fees;
 - The manner in which access will be provided;
 - Any grounds for refusal where access is denied;
 - Any rights available to challenge the decision.
-

10.12 Availability of Forms

The prescribed PAIA request forms are available from:

- The Information Regulator of South Africa;
- The Company's compliance contact details listed in this Manual;
- The Company's websites where applicable.

Requesters are encouraged to use the latest version of the prescribed forms available from the Information Regulator.

11. PRESCRIBED FEES AND PAYMENT REQUIREMENTS

11.1 General Principles

The processing of requests for access to records may be subject to the payment of fees as prescribed under the Promotion of Access to Information Act, 2000 ("PAIA") and any regulations issued thereunder.

Applicable fees may include:

- Request fees;
- Access fees;
- Reproduction fees;
- Search and preparation fees;
- Postage or delivery costs where applicable.

The Information Officer will notify the requester of any fees payable before access is granted where such fees are legally applicable.

11.2 Request Fee

Where permitted by PAIA, a requester may be required to pay a prescribed request fee before a request is processed.

The request fee is intended to cover the administrative costs associated with receiving and evaluating the request.

Certain categories of requesters may be exempt from paying a request fee in accordance with applicable legislation.

11.3 Access Fee

Where access to a record is granted, the requester may be required to pay an access fee.

Access fees may be charged for:

- Searching for records;
 - Retrieving records;
 - Preparing records for disclosure;
 - Reproducing records;
 - Providing copies of records;
 - Converting records into accessible formats where reasonably possible.
-

11.4 Deposits

Where the anticipated cost of processing a request exceeds the threshold prescribed by law, the Company may require the payment of a deposit before continuing with the processing of the request.

The requester will be informed of:

- The estimated cost;
- The amount of the required deposit;
- The basis upon which the deposit has been calculated.

Processing of the request may be suspended until the required deposit has been paid.

11.5 Method of Payment

Any fees payable in respect of a request must be paid using a payment method approved by the Company.

Payment instructions will be communicated to the requester in writing by the Information Officer.

11.6 Updated Fee Schedules

The Company does not publish fixed fee amounts within this Manual because the prescribed fees may be amended by regulation from time to time.

Requesters are encouraged to consult:

- The latest PAIA Regulations;
- The Information Regulator; or
- The Information Officer

for the most current fee schedule applicable at the time of the request.

11.7 Refunds

Any refunds relating to overpayments or incorrectly calculated fees will be dealt with in accordance with applicable law and the Company's administrative procedures.

11.8 No Guarantee of Access

Payment of a request fee, access fee, or deposit does not guarantee that access to the requested record will be granted.

All requests remain subject to the provisions of PAIA and any applicable grounds for refusal.

12. GROUNDS FOR REFUSAL OF ACCESS TO RECORDS

12.1 General Principles

The right of access to information is subject to the limitations and grounds for refusal provided for in the Promotion of Access to Information Act, 2000 ("PAIA").

The Company reserves the right to refuse access to records where such refusal is permitted or required by law.

Each request will be assessed on its own merits, taking into consideration the rights of the requester, the rights of affected third parties, the Company's legal obligations, and the public interest where applicable.

12.2 Protection of Personal Information of Third Parties

The Company may refuse access to records where disclosure would involve the unreasonable disclosure of personal information relating to a third party.

This may include, but is not limited to:

- Identity numbers
- Contact information
- Financial information
- Health-related information
- Employment information
- Coaching records
- Assessment results
- Personal development records
- Journaling content
- User-generated content
- Platform activity records

The privacy rights of data subjects will be protected in accordance with PAIA and POPIA.

12.3 Protection of Confidential Third-Party Information

The Company may refuse access to records containing confidential information supplied by a third party where disclosure could reasonably be expected to:

- Breach a duty of confidence;
- Prejudice the commercial interests of the third party;
- Reveal confidential business information;
- Disclose proprietary information;
- Compromise contractual obligations.

This may include information relating to clients, suppliers, contractors, service providers, business partners, consultants, and technology vendors.

12.4 Commercial Information of the Company

The Company may refuse access to records where disclosure could reasonably be expected to prejudice its commercial interests.

Such records may include:

- Business plans;
 - Strategic plans;
 - Financial forecasts;
 - Pricing methodologies;
 - Revenue models;
 - Market research;
 - Sales strategies;
 - Partnership strategies;
 - Growth strategies;
 - Acquisition plans;
 - Investment information;
 - Competitive analyses;
 - Internal management reports.
-

12.5 Trade Secrets and Proprietary Information

The Company may refuse access to records containing trade secrets or proprietary information.

Such information may include:

- Proprietary business processes;
- Internal operating methodologies;
- Commercial know-how;
- Proprietary systems;
- Internal frameworks;
- Proprietary documentation;
- Competitive intelligence.

Disclosure of such information may materially prejudice the Company's ability to compete within the marketplace.

12.6 Intellectual Property

The Company may refuse access to records containing intellectual property owned by, licensed to, or otherwise controlled by the Company.

This includes, but is not limited to:

- Coaching frameworks;
- Coaching methodologies;
- Assessment systems;
- Educational programmes;
- Training materials;
- Written content;
- Research materials;
- Course materials;
- Workbooks;
- Guides;
- Digital products;
- Branding assets;
- Trademarks;
- Copyright-protected works;
- Proprietary documentation.

The existence of a record does not grant any right to reproduce, distribute, modify, publish, commercialise, or otherwise exploit the intellectual property contained therein.

12.7 Technology and Software Systems

The Company develops and operates digital products and technology platforms.

Access may be refused where disclosure could reasonably reveal:

- Source code;
- Software architecture;
- System design documentation;
- Database structures;
- API configurations;
- Platform infrastructure;
- Technical specifications;
- Development roadmaps;
- Product development records;
- Proprietary algorithms;
- Technical implementation methodologies.

The Company is under no obligation to disclose information that could compromise the confidentiality or commercial value of its technology assets.

12.8 Artificial Intelligence Systems and Related Information

The Company may utilise artificial intelligence technologies in the provision of products and services.

Access may be refused where disclosure could reveal:

- AI implementation methodologies;
- Prompt engineering methodologies;
- Internal AI workflows;
- Model configurations;
- Proprietary AI processes;
- System instructions;
- Evaluation frameworks;
- Performance optimisation methods;
- Internal testing procedures;
- AI governance documentation where disclosure would compromise security or commercial interests.

The Company reserves the right to protect information necessary to maintain the integrity, security, effectiveness, and commercial value of its AI-enabled services.

12.9 Information Security and Cybersecurity

The Company may refuse access to records where disclosure could reasonably be expected to compromise information security.

Such information may include:

- Security policies;
- Access control procedures;
- Authentication mechanisms;
- Security architecture;
- Network configurations;
- Encryption methodologies;
- Vulnerability assessments;
- Penetration testing results;
- Incident response procedures;
- Disaster recovery procedures;
- Backup and recovery systems;
- Security monitoring records.

Disclosure of such information could expose the Company, its clients, or its users to security risks.

12.10 Coaching and Client Confidentiality

The Company provides professional coaching services that frequently involve the disclosure of sensitive personal information.

Access may be refused where disclosure would:

- Breach coaching confidentiality;
- Reveal confidential client information;
- Expose coaching records relating to third parties;
- Disclose assessments relating to third parties;
- Reveal sensitive personal development information;
- Compromise the privacy rights of current or former clients.

The Company places significant importance on preserving trust and confidentiality within coaching relationships.

12.11 Legally Privileged Records

The Company may refuse access to records subject to legal professional privilege.

This includes communications between the Company and its legal advisors where such communications are protected by law.

12.12 Records Relating to Legal Proceedings

Access may be refused where the requested records relate to existing, anticipated, or reasonably contemplated legal proceedings and disclosure would prejudice the Company's legal position.

12.13 Frivolous, Vexatious, or Manifestly Unreasonable Requests

The Company reserves the right to rely upon any applicable provisions of PAIA in relation to requests that are:

- Frivolous;
- Vexatious;
- Repetitive;
- Intended to harass;
- Manifestly unreasonable;
- Intended to disrupt the Company's operations.

Each request will be considered individually and fairly.

12.14 Information Not Held by the Company

The Company cannot provide access to records that:

- Do not exist;
- Cannot reasonably be located;
- Have been lawfully destroyed;
- Are not under the control of the Company.

The Company is not required to create new records in response to a request.

12.15 Public Interest Override

Notwithstanding any grounds for refusal contained in this Manual, the Company acknowledges that access may be granted where required by the public interest provisions of PAIA.

Any such determination will be made in accordance with the applicable provisions of PAIA and any other relevant legislation.

13. REMEDIES AVAILABLE TO REQUESTERS

13.1 General

The Company is committed to processing requests for access to information fairly, reasonably, and in accordance with the requirements of the Promotion of Access to Information Act, 2000 ("PAIA") and the Protection of Personal Information Act, 2013 ("POPIA").

Where a requester is dissatisfied with a decision made by the Company regarding a request for access to records or the processing of personal information, the requester may exercise the remedies available under applicable law.

13.2 No Internal Appeal Process

As a private body, the Company does not maintain a formal internal appeal procedure in respect of decisions taken under PAIA.

Any decision made by the Information Officer regarding a request for access to records shall constitute the Company's final internal decision.

Nothing in this Manual prevents a requester from seeking any remedies available under PAIA, POPIA, or any other applicable legislation.

13.3 Complaints Relating to Personal Information

A data subject who believes that the Company has processed personal information in a manner that is inconsistent with POPIA may lodge a complaint with the Information Regulator.

Examples may include concerns relating to:

- Collection of personal information;
- Processing of personal information;
- Accuracy of personal information;
- Security of personal information;
- Access to personal information;
- Correction or deletion requests;
- Cross-border transfers of personal information.

The Company encourages individuals to first raise concerns directly with the Information Officer where appropriate so that issues may be resolved efficiently and amicably.

13.4 Information Regulator

The Information Regulator is the independent authority responsible for monitoring and enforcing compliance with PAIA and POPIA in South Africa.

A requester or data subject may lodge a complaint with the Information Regulator where they believe their rights under PAIA or POPIA have been infringed.

Information Regulator (South Africa)

Website:

<https://www.justice.gov.za/inforeg/>

General Enquiries:

enquiries@inforegulator.org.za

Complaints:

PAIAComplaints@inforegulator.org.za

POPIAComplaints@inforegulator.org.za

The contact details of the Information Regulator may change from time to time, and requesters are encouraged to consult the Information Regulator's official website for the most current information.

13.5 Judicial Remedies

A requester who remains dissatisfied after exhausting any applicable remedies may apply to a court of competent jurisdiction for appropriate relief as provided for under PAIA.

The court may consider:

- Whether access should be granted;
- Whether a refusal was lawful;
- Whether procedural requirements were followed;
- Whether any rights protected under PAIA or POPIA have been infringed.

Any legal proceedings must be conducted in accordance with applicable legislation and court procedures.

13.6 Good Faith Resolution

The Company supports the resolution of disputes in a constructive and cooperative manner.

Before initiating formal complaints or legal proceedings, requesters are encouraged to engage with the Information Officer to clarify concerns, provide additional information where necessary, and explore practical solutions that may resolve the matter efficiently.

Nothing in this section limits any rights available to a requester under PAIA, POPIA, or any other applicable law.

14. AVAILABILITY OF THIS MANUAL

14.1 Publication of the Manual

This Manual is made available in accordance with Section 51 of the Promotion of Access to Information Act, 2000 ("PAIA").

The Manual is intended to assist members of the public in understanding:

- The records held by the Company;
 - The manner in which access to records may be requested;
 - The Company's processing of personal information;
 - The rights available under PAIA and POPIA.
-

14.2 Availability on Company Websites

The latest version of this Manual shall be made available on the Company's websites, where applicable, including:

- vayu.coach
- vayulifecoaching.co.za
- vayulifecoaching.online

The Company reserves the right to publish the Manual on additional websites, portals, or digital platforms under its control from time to time.

14.3 Availability at the Company's Offices

A copy of this Manual shall be made available for inspection at the Company's registered offices during normal business hours, subject to reasonable administrative arrangements.

Physical Address:

134 Ranger Road
Fish Hoek
Cape Town
7975
Western Cape
South Africa

14.4 Requesting a Copy

Any person may request a copy of this Manual by contacting the Information Officer using the contact details contained in this Manual.

The Company may provide the Manual in electronic format where reasonably practicable.

14.5 Language

This Manual has been prepared in English.

The Company may, at its discretion, make translated versions available. In the event of any inconsistency between versions, the English version shall prevail.

14.6 No Limitation of Rights

The availability of this Manual does not limit any rights afforded to requesters under PAIA, POPIA, or any other applicable legislation.

Nothing contained in this Manual shall be interpreted as limiting or excluding any rights or obligations established by law.

15. REVIEW, MAINTENANCE AND UPDATING OF THIS MANUAL

15.1 Ongoing Review

The Company recognises that its operations, technologies, legal obligations, and information processing activities may change over time.

Accordingly, this Manual shall be reviewed periodically to ensure continued compliance with:

- Promotion of Access to Information Act, 2000 (PAIA);
 - Protection of Personal Information Act, 2013 (POPIA);
 - Applicable regulations;
 - Information Regulator guidance;
 - Other relevant legislation.
-

15.2 Amendments

The Company reserves the right to amend, revise, replace, update, or withdraw portions of this Manual at any time where necessary to:

- Reflect changes in legislation;
 - Reflect changes in business operations;
 - Reflect changes in technology platforms;
 - Reflect changes in information processing activities;
 - Improve clarity or administrative efficiency;
 - Address regulatory requirements.
-

15.3 Version Control

The Information Officer shall be responsible for maintaining:

- The current version of the Manual;
 - Historical versions where appropriate;
 - Records of material amendments;
 - Publication of updated versions.
-

15.4 Review Frequency

The Company intends to review this Manual at least annually.

Additional reviews may be conducted where:

- Significant regulatory changes occur;
 - New products or services are introduced;
 - Material changes occur to the Company's information processing activities;
 - Information security requirements change;
 - New technology platforms are adopted.
-

15.5 Continued Validity

The most recent published version of this Manual shall supersede all previous versions and shall remain effective until replaced by a subsequent version.

16. APPROVAL, ADOPTION AND EFFECTIVE DATE

This PAIA Manual has been prepared in accordance with Section 51 of the Promotion of Access to Information Act, 2000 and incorporates relevant information concerning the Company's obligations under the Protection of Personal Information Act, 2013.

The Company is committed to transparency, accountability, lawful information governance, and the protection of personal information.

This Manual has been approved and adopted by the Information Officer of VAYU Coaching Technologies (Pty) Ltd.

Company Details

Company Name:

VAYU Coaching Technologies (Pty) Ltd

Registration Number:

2026/430224/07

Information Officer

Name:

Chris Roos

Position:

Founder, Chief Executive Officer, Director and Information Officer

Email:

chris.roos@vayulifecoaching.co.za

Telephone:

+27 62 732 1090

Document Control

Document Title:

PAIA Manual

Version:

1.0

Effective Date:

Review Date:

Approval

I hereby confirm that this Manual has been approved and adopted on behalf of VAYU Coaching Technologies (Pty) Ltd and shall remain in force until amended or replaced.

Name:

Chris Roos

Position:

Founder, Chief Executive Officer, Director and Information Officer

Signature:

Date:

APPENDIX A

INFORMATION REGULATOR OF SOUTH AFRICA

The Information Regulator is the independent authority established to monitor and enforce compliance with the Promotion of Access to Information Act, 2000 ("PAIA") and the Protection of Personal Information Act, 2013 ("POPIA").

Individuals who believe that their rights under PAIA or POPIA have been infringed may lodge a complaint with the Information Regulator.

General Contact Details

Information Regulator (South Africa)

Physical Address:

JD House
27 Stiemens Street
Braamfontein
Johannesburg
2001
South Africa

Postal Address:

P.O. Box 31533
Braamfontein
Johannesburg
2017
South Africa

Telephone:

+27 (0)10 023 5200

Website:

www.inforegulator.org.za

General Enquiries

Email:

enquiries@inforegulator.org.za

PAIA Complaints

Email:

PAIAComplaints@inforegulator.org.za

POPIA Complaints

Email:

POPIAComplaints@inforegulator.org.za

Functions of the Information Regulator

The Information Regulator is responsible for, among other things:

- Monitoring compliance with PAIA;
- Monitoring compliance with POPIA;
- Investigating complaints;
- Promoting public awareness regarding information rights;
- Issuing guidance and codes of conduct;
- Enforcing compliance where appropriate.

The contact details above may change from time to time. Individuals are encouraged to verify the latest information via the Information Regulator's official website.

APPENDIX B

PAIA REQUESTS, FORMS AND ACCESS PROCEDURES

Purpose

This Appendix provides guidance regarding the prescribed forms and procedures required for requesting access to records held by VAYU Coaching Technologies (Pty) Ltd.

Prescribed Form

Requests for access to records must be submitted using the prescribed PAIA Request for Access to Record Form (Form 2).

The current prescribed form is published by the Information Regulator and may be updated from time to time.

Requesters are responsible for ensuring that they use the most recent version of the prescribed form.

Information Required from Requesters

A requester should provide sufficient information to enable the Company to:

- Identify the requester;
- Verify the requester's identity;
- Locate the requested record;
- Determine the form of access requested;
- Communicate effectively with the requester;
- Determine whether third-party consultation is required.

The requester should provide as much detail as reasonably possible regarding the requested records.

Submission of Requests

Completed requests may be submitted to:

Information Officer

Chris Roos

Founder, Chief Executive Officer, Director and Information Officer

Email:

chris.roos@vayulifecoaching.co.za

Alternative Compliance Email:

compliance@vayulifecoaching.co.za

Physical Address:

134 Ranger Road

Fish Hoek

Cape Town

7975

Western Cape

South Africa

Telephone:

+27 62 732 1090

Verification Requirements

The Company may request additional information or documentation to verify:

- The identity of the requester;
- Authority to act on behalf of another person;
- Ownership of the requested information;
- Entitlement to access the requested records.

Failure to provide sufficient verification may result in delays or refusal of access where permitted by law.

Processing of Requests

Upon receipt of a valid request, the Company will:

1. Review the request;
 2. Determine whether the requested records exist;
 3. Consider applicable legal requirements;
 4. Assess any grounds for refusal;
 5. Consult affected third parties where required;
 6. Notify the requester of the outcome.
-

Response Timeframes

The Company will process requests within the time periods prescribed by PAIA.

Where legally permissible, an extension may be required due to:

- Volume of records;
- Complexity of the request;
- Third-party consultation requirements;
- Operational constraints permitted by law.

The requester will be informed of any extension and the reasons for it.

Applicable Fees

Requesters may be required to pay fees prescribed by PAIA regulations.

These may include:

- Request fees;
- Access fees;
- Reproduction fees;
- Search and preparation fees;
- Delivery costs.

Current fees are determined by applicable legislation and regulations and may change from time to time.

Grounds for Refusal

Access may be refused in circumstances permitted by PAIA, including but not limited to:

- Protection of personal information;
- Protection of confidential information;
- Protection of trade secrets;
- Protection of intellectual property;
- Protection of commercial information;
- Protection of information security systems;
- Legal privilege;
- Other lawful grounds contained in PAIA.

Full details are contained in Section 12 of this Manual.

Complaints and Remedies

Where a requester is dissatisfied with a decision relating to a request, the requester may:

- Contact the Information Officer for clarification;
- Lodge a complaint with the Information Regulator;
- Exercise any legal remedies available under PAIA or POPIA.

Further details are contained in Section 13 of this Manual.

Availability of Forms

The latest prescribed PAIA forms may be obtained from:

- The Information Regulator;
- The Company's websites, where made available;
- The Information Officer upon request.

Requesters are encouraged to use the latest official forms published by the Information Regulator.

APPENDIX C

RECORD RETENTION AND DESTRUCTION SCHEDULE

1. PURPOSE

This Record Retention and Destruction Schedule establishes the periods for which VAYU Coaching Technologies (Pty) Ltd ("the Company") may retain records in accordance with:

- The Promotion of Access to Information Act, 2000 (PAIA);
- The Protection of Personal Information Act, 2013 (POPIA);
- The Companies Act, 2008;
- The Tax Administration Act, 2011;
- Other applicable legislation;
- Legitimate business requirements.

Records shall not be retained indefinitely unless there is a lawful basis for doing so.

Where records are no longer required, they may be securely deleted, destroyed, anonymised, or de-identified.

2. CORPORATE GOVERNANCE RECORDS

Record Category	Retention Period
Company registration documents	Permanent
Memorandum of Incorporation (MOI)	Permanent
Shareholder records	Permanent
Director resolutions	Permanent
Statutory registers	Permanent
Annual returns	Permanent
Regulatory filings	Permanent
Compliance records	Minimum 7 years

3. FINANCIAL AND ACCOUNTING RECORDS

Record Category	Retention Period
Annual financial statements	Minimum 7 years
General ledger records	Minimum 7 years
Bank statements	Minimum 7 years
Tax returns	Minimum 7 years
Supporting tax documentation	Minimum 7 years
Invoices issued	Minimum 7 years
Supplier invoices	Minimum 7 years
Payment records	Minimum 7 years
Merchant account transaction records	Minimum 7 years
Expense records	Minimum 7 years
Budget and forecast records	Minimum 5 years

4. HUMAN RESOURCES RECORDS

Record Category	Retention Period
Employment contracts	Duration of employment plus 5 years
Payroll records	Minimum 5 years
Leave records	Minimum 5 years
Performance records	Duration of employment plus 3 years
Disciplinary records	Duration of employment plus 3 years
Recruitment records	12 months after conclusion of recruitment process
Contractor agreements	Duration of agreement plus 5 years

5. CLIENT AND COACHING RECORDS

Record Category	Retention Period
Coaching agreements	7 years after termination
Client onboarding records	7 years after termination
Session summaries	7 years after termination
Progress records	7 years after termination
Assessment results	7 years after termination
Accountability records	7 years after termination
Client communications	7 years after termination
Client payment records	7 years after termination
Client feedback and testimonials	Until consent is withdrawn or no longer required

Confidential Coaching Information

Coaching records may contain highly personal information.

Where retention is no longer required, records should be securely destroyed or anonymised to protect client privacy.

6. PROSPECTIVE CLIENT AND LEAD RECORDS

Record Category	Retention Period
Website enquiries	24 months
Discovery call records	24 months
Lead records	24 months
Consultation requests	24 months
CRM records for inactive leads	24 months
Marketing enquiries	24 months

The Company may retain records for longer where consent has been obtained or a legitimate business purpose exists.

7. PLATFORM USER RECORDS

Record Category	Retention Period
User account information	Duration of account plus 24 months
Subscription records	7 years
Billing records	7 years
Login records	24 months
Support requests	5 years
User preferences	Duration of account
Product usage records	24 months
Customer service records	5 years

8. USER-GENERATED CONTENT

Record Category	Retention Period
Journal entries	Duration of account plus 24 months
Goal tracking records	Duration of account plus 24 months
Habit tracking records	Duration of account plus 24 months
Notes created by users	Duration of account plus 24 months
Uploaded content	Duration of account plus 24 months
Assessment responses	Duration of account plus 24 months

The Company may offer users the ability to delete certain content directly through the platform, subject to operational and legal limitations.

9. ARTIFICIAL INTELLIGENCE INTERACTION RECORDS

Record Category	Retention Period
AI interaction logs	Up to 24 months
Prompt submissions	Up to 24 months
AI-generated responses	Up to 24 months
AI usage analytics	Up to 36 months
AI performance monitoring records	Up to 36 months
AI incident records	Minimum 5 years

The Company reserves the right to anonymise AI-related data for research, quality assurance, security, product improvement, and statistical purposes where legally permissible.

10. MARKETING AND COMMUNICATION RECORDS

Record Category	Retention Period
Newsletter subscriptions	Until unsubscribe or 24 months of inactivity
Marketing campaign records	5 years
Advertising performance records	5 years
Website analytics records	36 months
Social media campaign records	5 years
Event registration records	3 years

11. LEGAL AND COMPLIANCE RECORDS

Record Category	Retention Period
Contracts and agreements	7 years after termination
Legal opinions	Permanent where appropriate
Litigation records	10 years after conclusion
Complaints records	5 years
PAIA requests	5 years
POPIA complaints	5 years
Information security investigations	5 years
Regulatory correspondence	7 years

12. INFORMATION SECURITY RECORDS

Record Category	Retention Period
Security incident reports	5 years
Vulnerability assessments	5 years
Penetration testing reports	5 years
Access control logs	24 months
Security monitoring logs	24 months
Backup records	According to backup schedule
Disaster recovery records	5 years

13. DESTRUCTION OF RECORDS

Where records are no longer required:

- Electronic records may be securely deleted;
 - Physical records may be shredded or securely destroyed;
 - Personal information may be anonymised or de-identified;
 - Destruction shall occur in a manner designed to prevent unauthorised access, reconstruction, or disclosure.
-

14. LEGAL HOLDS

Notwithstanding the retention periods contained in this Schedule, the Company may retain records for longer where:

- Required by law;
- Required for litigation;
- Required for investigations;
- Required by regulatory authorities;
- Necessary to establish, exercise, or defend legal rights;
- Necessary to protect the legitimate interests of the Company or affected parties.

Such records shall be retained until the relevant matter has been resolved.

APPENDIX D

THIRD-PARTY OPERATORS, CLOUD SERVICES AND INTERNATIONAL DATA TRANSFERS

1. PURPOSE

This Appendix provides additional information regarding third-party service providers, software platforms, cloud services, operators, and international data transfers utilised by VAYU Coaching Technologies (Pty) Ltd ("the Company").

The Company may engage reputable third-party service providers to assist with the delivery of services, operation of technology platforms, administration, communications, accounting, marketing, analytics, customer relationship management, artificial intelligence services, and other legitimate business activities.

The use of third-party providers does not diminish the Company's obligations under the Protection of Personal Information Act, 2013 ("POPIA").

2. THIRD-PARTY OPERATORS

The Company may utilise the following categories of operators and service providers:

Financial Service Providers

- Banking institutions
- Payment processors
- Merchant service providers
- Accounting service providers

Technology Service Providers

- Cloud hosting providers
- Software providers
- Infrastructure providers
- Analytics providers
- Security providers

Marketing and CRM Providers

- Customer relationship management platforms
- Email marketing providers
- Advertising platforms
- Analytics platforms

Artificial Intelligence Service Providers

- Generative AI providers
- Natural language processing providers
- Machine learning service providers
- AI-assisted productivity tools

Professional Service Providers

- Accountants
 - Auditors
 - Legal advisors
 - Compliance consultants
 - Business consultants
-

3. CURRENT CORE SERVICE PROVIDERS

The Company currently utilises or may utilise the following service providers as part of its operations.

Google Workspace

Purpose:

- Business email
- Document storage
- File sharing
- Collaboration
- Calendar management
- Productivity services

Categories of Information Potentially Processed:

- Names
 - Email addresses
 - Contact information
 - Documents
 - Communications
 - Business records
-

OpenAI

Purpose:

- AI-powered coaching functionality
- Content generation
- User support
- Productivity assistance
- AI-assisted platform features

Categories of Information Potentially Processed:

- User prompts
- User responses
- Coaching interactions
- Platform-generated content
- Operational information

The Company does not intentionally submit unnecessary personal information to AI systems.

Anthropic Claude

Purpose:

- AI-assisted content generation
- Business operations
- Research assistance
- Coaching support functionality
- Administrative productivity

Categories of Information Potentially Processed:

- Prompts
- Responses
- Business information
- Operational information

The Company seeks to minimise unnecessary personal information when using AI service providers.

HubSpot

Purpose:

- Customer relationship management
- Lead management
- Sales management
- Marketing communications
- Customer support

Categories of Information Potentially Processed:

- Names
 - Contact details
 - Communication history
 - Lead information
 - Customer records
-

Xero

Purpose:

- Accounting
- Financial management
- Invoicing
- Tax administration
- Financial reporting

Categories of Information Potentially Processed:

- Customer information
 - Supplier information
 - Financial transactions
 - Invoices
 - Accounting records
-

PayFast

Purpose:

- Payment processing
- Transaction management
- Subscription payments
- Financial administration

Categories of Information Potentially Processed:

- Payment information
 - Customer details
 - Transaction records
 - Billing information
-

4. CROSS-BORDER TRANSFERS OF PERSONAL INFORMATION

The Company may transfer personal information to service providers located outside the Republic of South Africa or whose infrastructure operates across multiple jurisdictions.

Such transfers may occur where:

- Cloud services are utilised;
- Software-as-a-Service (SaaS) platforms are utilised;
- International technology providers are engaged;
- Data processing activities require international infrastructure;
- Business continuity or operational requirements necessitate such transfers.

The Company will take reasonable steps to ensure that personal information transferred internationally receives an appropriate level of protection consistent with applicable legal requirements.

5. COUNTRIES AND JURISDICTIONS

Personal information may be processed, stored, backed up, transmitted, or accessed in jurisdictions including, but not limited to:

- South Africa
- United States of America
- European Union Member States
- Australia
- United Kingdom
- Other jurisdictions utilised by service providers from time to time

The precise location of processing may vary depending on the infrastructure and service providers in use.

6. SAFEGUARDS FOR INTERNATIONAL TRANSFERS

Where personal information is transferred internationally, the Company may rely on:

- Contractual safeguards;
- Vendor security commitments;
- Industry-standard security controls;
- Encryption technologies;
- Access controls;
- POPIA-compliant processing arrangements;
- Other reasonable technical and organisational measures.

The Company seeks to engage service providers that maintain appropriate security and privacy standards.

7. DATA MINIMISATION

The Company is committed to the principle of data minimisation.

Where possible, the Company seeks to:

- Limit the personal information shared with third parties;
 - Avoid unnecessary disclosure of sensitive information;
 - Restrict access to authorised personnel only;
 - Use anonymised or de-identified information where appropriate.
-

8. CHANGES TO SERVICE PROVIDERS

The Company's technology stack, operational requirements, and service providers may change from time to time.

Accordingly:

- Additional operators may be appointed;
- Existing operators may be replaced;
- New cloud services may be adopted;
- Additional AI providers may be utilised.

The Company reserves the right to update this Appendix to reflect such changes.

9. RESPONSIBILITY AND ACCOUNTABILITY

While the Company may engage third-party operators, VAYU Coaching Technologies (Pty) Ltd remains responsible for ensuring that personal information is processed in accordance with applicable legal requirements.

The Company will take reasonable steps to ensure that operators acting on its behalf maintain appropriate safeguards for the protection of personal information.

APPENDIX E

CATEGORIES OF PERSONAL INFORMATION AND LAWFUL BASIS FOR PROCESSING

1. PURPOSE

This Appendix provides an overview of the categories of personal information processed by VAYU Coaching Technologies (Pty) Ltd ("the Company"), the purposes for which such information is processed, and the lawful basis upon which such processing occurs.

The Company processes personal information in accordance with the Protection of Personal Information Act, 2013 ("POPIA"), applicable contractual obligations, legal obligations, and legitimate business requirements.

The categories listed below are intended as a general guide and may be updated from time to time as the Company's products, services, and operations evolve.

2. CLIENT AND COACHING INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
Full Name	Client identification	Contractual necessity
Contact Details	Communication and service delivery	Contractual necessity
Physical Address	Billing, administration, legal compliance	Contractual necessity / Legal obligation
Date of Birth	Identity verification where required	Legitimate interest
Coaching Goals	Coaching service delivery	Contractual necessity
Coaching Assessments	Personal development support	Contractual necessity
Progress Tracking Information	Coaching service delivery	Contractual necessity
Accountability Records	Coaching programme administration	Contractual necessity
Session Notes	Coaching service delivery	Contractual necessity
Client Communications	Service administration	Contractual necessity
Payment Records	Financial administration	Legal obligation / Contractual necessity
Testimonials	Marketing and social proof	Consent

3. PROSPECTIVE CLIENT INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
Name	Lead management	Legitimate interest
Email Address	Responding to enquiries	Legitimate interest
Telephone Number	Consultation scheduling	Legitimate interest
Discovery Call Information	Assessment of service suitability	Legitimate interest
Website Enquiry Information	Responding to enquiries	Legitimate interest
Marketing Preferences	Marketing administration	Consent

4. PLATFORM USER INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
Name	Account administration	Contractual necessity
Email Address	Account creation and communication	Contractual necessity
Username	Platform functionality	Contractual necessity
Password Credentials	Authentication and security	Contractual necessity
Subscription Information	Subscription administration	Contractual necessity
User Preferences	Personalisation	Contractual necessity
Login History	Security and fraud prevention	Legitimate interest
Account Activity	Platform functionality	Contractual necessity

5. USER-GENERATED CONTENT

Category of Information	Purpose of Processing	Lawful Basis
Journal Entries	Platform functionality	Contractual necessity
Reflections and Notes	Coaching support	Contractual necessity
Goal Tracking Information	Personal development support	Contractual necessity
Habit Tracking Information	Platform functionality	Contractual necessity
Assessment Responses	Coaching and development support	Contractual necessity
Uploaded Content	Platform functionality	Contractual necessity

6. AI INTERACTION INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
AI Prompt Submissions	AI-assisted service delivery	Contractual necessity
AI Responses	Service functionality	Contractual necessity
AI Usage Analytics	Product improvement	Legitimate interest
AI Performance Data	Service quality and optimisation	Legitimate interest
AI Feedback Information	Service improvement	Legitimate interest

The Company seeks to minimise the submission of unnecessary personal information to AI service providers and implements reasonable safeguards when utilising AI technologies.

7. WEBSITE VISITOR INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
IP Address	Security and analytics	Legitimate interest
Device Information	Platform optimisation	Legitimate interest
Browser Information	Technical functionality	Legitimate interest
Website Usage Information	Analytics and performance monitoring	Legitimate interest
Cookie Data	Website functionality and analytics	Consent where required

8. MARKETING INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
Email Address	Newsletter distribution	Consent
Marketing Preferences	Preference management	Consent
Campaign Engagement Data	Marketing effectiveness analysis	Legitimate interest
Event Registration Information	Event administration	Contractual necessity
Webinar Registration Information	Event administration	Contractual necessity

9. FINANCIAL INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
Billing Information	Financial administration	Contractual necessity
Transaction Records	Financial administration	Legal obligation
Payment Information	Payment processing	Contractual necessity
Tax Information	Tax compliance	Legal obligation
Accounting Records	Financial reporting	Legal obligation

10. EMPLOYEE AND CONTRACTOR INFORMATION

Category of Information	Purpose of Processing	Lawful Basis
Identity Information	Employment administration	Contractual necessity
Contact Information	Employment administration	Contractual necessity
Qualifications	Recruitment and engagement	Contractual necessity
Employment History	Recruitment and engagement	Contractual necessity
Payroll Information	Employment administration	Legal obligation
Performance Records	Human resource management	Legitimate interest
Contractor Information	Contract administration	Contractual necessity

11. SPECIAL PERSONAL INFORMATION

The Company does not intentionally collect special personal information unless:

- The information is voluntarily provided by the data subject;
- Processing is required for service delivery;
- Processing is authorised by law;
- Explicit consent has been obtained where required.

Where special personal information is processed, additional safeguards may be implemented in accordance with POPIA.

Examples may include:

- Information relating to wellbeing;
 - Information disclosed during coaching engagements;
 - Information voluntarily disclosed by users in journals, reflections, assessments, or AI interactions.
-

12. RECIPIENTS OF PERSONAL INFORMATION

Personal information may be disclosed to authorised recipients including:

- Accountants and auditors;
- Legal advisors;
- Payment processors;
- Banking institutions;
- Cloud service providers;
- Customer relationship management providers;
- Artificial intelligence service providers;
- Regulatory authorities where legally required;
- Technology service providers supporting the Company's operations.

Such disclosures are limited to what is reasonably necessary for the relevant purpose.

13. DATA MINIMISATION PRINCIPLE

The Company seeks to collect and process only the personal information reasonably required to:

- Deliver services;
- Operate its technology platforms;
- Meet legal obligations;
- Protect legitimate business interests;
- Improve products and services.

The Company does not intentionally collect excessive personal information.

14. CHANGES TO PROCESSING ACTIVITIES

The categories of personal information processed by the Company may change as products, services, technologies, and operational requirements evolve.

This Appendix may be amended from time to time to reflect such changes and to ensure ongoing compliance with applicable legal requirements.