POPIA COMPLIANCE FRAMEWORK

VAYU COACHING TECHNOLOGIES (PTY) LTD

Version 1.0

1. PURPOSE AND SCOPE

1.1 Purpose

The purpose of this POPIA Compliance Framework ("Framework") is to establish the governance, policies, procedures, controls, and accountability measures adopted by VAYU Coaching Technologies (Pty) Ltd ("the Company") to ensure compliance with the Protection of Personal Information Act, 2013 (Act No. 4 of 2013) ("POPIA").

The Company recognises the constitutional right to privacy and is committed to ensuring that personal information is processed lawfully, reasonably, transparently, securely, and in accordance with applicable legislation.

This Framework provides the foundation for the Company's information governance programme and applies to all personal information processed by the Company in the course of conducting its business activities.

1.2 Scope

This Framework applies to:

- VAYU Coaching Technologies (Pty) Ltd;
- All directors, employees, contractors, consultants, and temporary workers acting on behalf of the Company;
- All business activities conducted by the Company;
- All websites, applications, software platforms, coaching programmes, digital products, and services operated by the Company;
- All personal information processed by the Company in physical or electronic form.

This Framework applies regardless of whether information is processed:

- Within South Africa;
- Outside South Africa;
- Through cloud-based systems;
- Through third-party service providers;
- Through artificial intelligence technologies;
- Through mobile applications;
- Through online platforms.

1.3 Business Activities Covered

This Framework applies to the Company's activities including:

- Life coaching;
- Executive coaching;
- Personal development coaching;
- AI-powered coaching services;
- Mobile application development;
- Digital content creation;
- Digital marketing services;
- Customer relationship management;
- Website operations;
- Subscription-based services;
- Platform administration;
- Artificial intelligence services.

1.4 Objectives

The objectives of this Framework are to:

- Protect the privacy rights of data subjects;
- Ensure compliance with POPIA;
- Promote responsible information governance;
- Establish accountability for information processing activities;
- Reduce information security risks;
- Support lawful business operations;
- Build trust with clients, users, partners, and stakeholders;
- Establish standards for the responsible use of artificial intelligence;
- Protect the confidentiality, integrity, and availability of information.

1.5 Relationship to Other Policies

This Framework should be read together with:

- PAIA Manual;
- Privacy Policy;
- Terms of Service;
- Coaching Services Agreement;
- Information Security Policies;
- Data Retention Schedule;
- Incident Response Procedures;
- Any other applicable governance documentation adopted by the Company.

Where inconsistencies arise, applicable legislation shall prevail.

---

2. GOVERNANCE STRUCTURE

2.1 Accountability

The Company acknowledges that accountability for compliance with POPIA ultimately rests with the Company and its leadership.

All individuals acting on behalf of the Company are responsible for handling personal information in accordance with this Framework and applicable legislation.

2.2 Information Officer

The Company has appointed an Information Officer responsible for overseeing compliance with POPIA and PAIA.

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

2.3 Responsibilities of the Information Officer

The Information Officer is responsible for:

- Monitoring compliance with POPIA;
- Monitoring compliance with PAIA;
- Maintaining the Company's PAIA Manual;
- Maintaining privacy governance documentation;
- Managing requests from data subjects;
- Managing requests for access to information;
- Monitoring information security practices;
- Coordinating breach response activities;
- Managing engagement with the Information Regulator;
- Monitoring third-party operators and service providers;
- Promoting awareness of privacy obligations;
- Reviewing compliance controls;
- Overseeing cross-border data transfers;
- Overseeing AI governance and responsible AI practices.

2.4 Employees and Contractors

All employees, contractors, consultants, service providers, and authorised users who process personal information on behalf of the Company must:

- Comply with this Framework;
- Protect confidential information;
- Follow information security requirements;
- Report suspected incidents;
- Participate in required training and awareness activities;
- Process personal information only for authorised purposes.

2.5 Governance Reviews

The Company shall periodically review:

- Compliance risks;
- Information processing activities;
- Security controls;
- Third-party operator arrangements;
- AI governance controls;
- Regulatory developments.

Reviews shall be conducted at least annually or more frequently where circumstances require.

3. POPIA CONDITIONS FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

3.1 Commitment to Lawful Processing

VAYU Coaching Technologies (Pty) Ltd ("the Company") is committed to ensuring that all processing of personal information complies with the conditions for lawful processing established under the Protection of Personal Information Act, 2013 ("POPIA").

The Company shall implement policies, procedures, controls, and governance measures designed to support compliance with each of these conditions.

3.2 CONDITION 1: ACCOUNTABILITY

The Company accepts responsibility for ensuring compliance with POPIA and for establishing appropriate governance structures to support lawful processing.

The Company shall:

- Maintain privacy governance documentation;
- Appoint an Information Officer;
- Monitor compliance activities;
- Maintain records of processing activities;
- Review privacy practices periodically;
- Investigate and address privacy risks;
- Maintain appropriate information security controls.

The Information Officer shall oversee the implementation and monitoring of this Framework.

3.3 CONDITION 2: PROCESSING LIMITATION

The Company shall process personal information lawfully, reasonably, and in a manner that does not infringe the privacy rights of data subjects.

The Company shall:

- Process information only where a lawful basis exists;
- Collect information directly from data subjects where reasonably practicable;
- Limit collection to information that is relevant and necessary;
- Avoid excessive collection of personal information;
- Avoid processing information for unlawful purposes;
- Respect the rights of data subjects.

Where consent is relied upon as a lawful basis, such consent shall be voluntary, specific, informed, and capable of being withdrawn.

3.4 CONDITION 3: PURPOSE SPECIFICATION

The Company shall collect personal information only for specific, explicitly defined, and lawful purposes.

Personal information may be processed for purposes including:

- Coaching services;
- Platform administration;
- User account management;
- Customer support;
- Subscription management;
- Marketing communications;
- Financial administration;
- Legal compliance;
- Information security;
- Product improvement;
- AI-assisted service delivery.

The Company shall communicate the purpose of collection to data subjects through appropriate notices, agreements, and policies.

3.5 CONDITION 4: FURTHER PROCESSING LIMITATION

The Company shall ensure that any further processing of personal information remains compatible with the purpose for which the information was originally collected.

When assessing compatibility, the Company shall consider:

- The relationship between the original purpose and the proposed purpose;
- The nature of the information;
- The consequences of further processing;
- The reasonable expectations of the data subject;
- Applicable legal requirements.

Personal information shall not be repurposed in a manner that would be unfair, unexpected, or unlawful.

3.6 CONDITION 5: INFORMATION QUALITY

The Company shall take reasonable steps to ensure that personal information is:

- Accurate;
- Complete;
- Relevant;
- Up to date;
- Not misleading.

Data subjects shall be encouraged to notify the Company of changes to their personal information.

The Company may periodically review information to improve data quality and accuracy.

3.7 CONDITION 6: OPENNESS

The Company is committed to transparency regarding its information processing activities.

The Company shall maintain:

- A PAIA Manual;
- A Privacy Policy;
- Appropriate privacy notices;
- Records of processing activities;
- Documentation relating to information governance.

Data subjects shall be informed regarding:

- What information is collected;
- Why information is collected;

- How information is used;
- Who information may be shared with;
- Their rights under applicable legislation.

3.8 CONDITION 7: SECURITY SAFEGUARDS

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

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

Security measures may include:

- Access controls;
- Password policies;
- Multi-factor authentication;
- Encryption;
- Secure cloud infrastructure;
- Monitoring and logging;
- Data backup procedures;
- Information security awareness measures.

The Company shall periodically assess security risks and implement improvements where necessary.

3.9 CONDITION 8: DATA SUBJECT PARTICIPATION

The Company recognises the rights of data subjects to participate in the management of their personal information.

Subject to applicable law, data subjects may request:

- Access to personal information;
- Correction of inaccurate information;

- Updating of information;
- Deletion of information where appropriate;
- Restriction of processing where applicable;
- Information regarding the processing of their personal information.

Requests shall be handled in accordance with the Company's PAIA Manual, Privacy Policy, and applicable legislation.

3.10 APPLICATION TO AI-ENABLED SERVICES

The Company acknowledges that artificial intelligence technologies may be utilised in connection with certain products, services, and platform features.

The Company shall apply the principles contained in this section to AI-enabled processing activities.

In particular, the Company shall seek to:

- Maintain transparency regarding AI usage;
- Minimise unnecessary personal information submitted to AI systems;
- Implement reasonable safeguards for AI-enabled services;
- Monitor AI-related risks;
- Maintain human oversight of critical business decisions;
- Avoid unfair or discriminatory processing practices;
- Ensure that AI technologies are used in a manner consistent with applicable legal and ethical obligations.

The Company recognises that AI-generated content may contain inaccuracies and should not be treated as a substitute for professional legal, financial, medical, psychological, or other regulated professional advice.

4. CATEGORIES OF DATA SUBJECTS AND PERSONAL INFORMATION PROCESSED

4.1 Purpose

The purpose of this section is to identify the categories of data subjects whose personal information may be processed by VAYU Coaching Technologies (Pty) Ltd ("the Company") and to provide an overview of the categories of personal information that may be collected, stored, used, disclosed, transferred, or otherwise processed.

The categories contained in this section are intended as a governance framework and may be updated from time to time as the Company's products, services, technologies, and operational requirements evolve.

4.2 CATEGORIES OF DATA SUBJECTS

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

Clients

Individuals receiving:

- Life coaching services;
- Executive coaching services;
- Personal development services;
- Consulting services;
- Digital services;
- Subscription-based services.

Prospective Clients

Individuals who:

- Request information;
- Complete enquiry forms;
- Schedule consultations;
- Attend discovery calls;
- Subscribe to newsletters;
- Engage with marketing campaigns.

Platform Users

Individuals who:

- Register user accounts;
- Access websites;
- Use mobile applications;
- Use digital platforms;
- Participate in AI-enabled services;
- Purchase subscriptions.

Employees

Current, former, and prospective employees of the Company.

Contractors and Consultants

Independent contractors, consultants, freelancers, developers, coaches, advisors, and service providers engaged by the Company.

Suppliers and Vendors

Representatives of suppliers, vendors, and service providers.

Business Partners

Representatives of strategic partners, affiliates, referral partners, and professional service providers.

Website Visitors

Individuals who access or interact with:

- Company websites;
- Landing pages;
- Digital content;
- Marketing assets.

4.3 CATEGORIES OF PERSONAL INFORMATION

Depending on the nature of the relationship with the Company, personal information processed may include the following categories.

Identity Information

The Company may process:

- Full names;
- Initials;
- Identity numbers;
- Passport numbers;
- Nationality;
- Date of birth;
- Gender;
- Photographs where voluntarily provided.

Contact Information

The Company may process:

- Email addresses;
- Telephone numbers;

- Mobile numbers;
- Physical addresses;
- Postal addresses;
- Emergency contact information where applicable.

Account Information

The Company may process:

- Usernames;
- User identifiers;
- Authentication information;
- Subscription details;
- Account preferences;
- Account status information.

Passwords shall not be stored in plain text and shall be protected using appropriate security controls.

Financial Information

The Company may process:

- Billing information;
- Invoicing information;
- Payment history;
- Transaction records;
- Banking details where necessary;
- Tax-related information.

The Company does not intentionally store full payment card information unless required and authorised through approved payment processing systems.

Employment Information

The Company may process:

- Employment history;
- Qualifications;
- Professional certifications;
- Curriculum vitae;
- Performance records;

- Payroll information;
- Contractor records.

Coaching Information

The Company may process:

- Coaching goals;
- Personal development objectives;
- Assessment responses;
- Progress records;
- Accountability records;
- Session summaries;
- Coaching communications;
- Coaching programme participation records.

The Company recognises that coaching information may contain highly personal and confidential information.

User-Generated Content

The Company may process content voluntarily created or submitted by users including:

- Journal entries;
- Notes;
- Reflections;
- Goal tracking information;
- Habit tracking information;
- Uploaded documents;
- Written submissions;
- Feedback submissions.

Communication Information

The Company may process:

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

- Customer service records.

Technical Information

The Company may process:

- IP addresses;
- Device identifiers;
- Browser information;
- Operating system information;
- Application usage information;
- Login history;
- Session information;
- Security logs.

Marketing Information

The Company may process:

- Newsletter subscriptions;
- Marketing preferences;
- Campaign engagement information;
- Event registrations;
- Webinar registrations;
- Lead generation information.

Artificial Intelligence Interaction Information

Where AI-enabled services are utilised, the Company may process:

- Prompt submissions;
- AI-generated responses;
- AI interaction history;
- AI usage analytics;
- AI feedback information;
- Service improvement information.

The Company seeks to minimise unnecessary personal information processed through AI-enabled services and applies appropriate governance measures to such processing.

4.4 SPECIAL PERSONAL INFORMATION

The Company does not intentionally seek to collect special personal information unless:

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

Special personal information may arise in the context of:

- Coaching engagements;
- Journal entries;
- User reflections;
- Goal-setting exercises;
- Voluntary disclosures made by clients or platform users.

Where such information is processed, additional safeguards may be applied to protect the rights and interests of affected individuals.

4.5 CHILDREN'S INFORMATION

The Company's products and services are primarily intended for adults.

The Company does not knowingly collect personal information relating to children unless:

- Authorised by applicable law;
- Authorised by a competent person;
- Necessary for lawful business purposes.

Where information relating to children is identified, the Company shall take appropriate steps to ensure compliance with applicable legal requirements.

4.6 DATA MINIMISATION

The Company shall seek to collect only the personal information reasonably necessary to:

- Deliver products and services;
- Fulfil contractual obligations;
- Meet legal obligations;
- Protect legitimate business interests;
- Improve products and services;
- Maintain information security.

The Company shall avoid excessive, unnecessary, or disproportionate collection of personal information.

5. LAWFUL BASES FOR PROCESSING PERSONAL INFORMATION

5.1 Purpose

The purpose of this section is to establish the lawful bases upon which VAYU Coaching Technologies (Pty) Ltd ("the Company") processes personal information.

The Company shall not process personal information unless a lawful basis exists in accordance with the Protection of Personal Information Act, 2013 ("POPIA") and any other applicable legislation.

The lawful basis relied upon may vary depending on the nature of the information, the purpose of processing, and the relationship between the Company and the data subject.

5.2 CONSENT

The Company may process personal information where the data subject has voluntarily provided informed and specific consent.

Examples include:

- Newsletter subscriptions;
- Marketing communications;
- Downloadable resources;
- Webinar registrations;
- Promotional campaigns;
- Testimonials;
- Certain optional platform features;
- Participation in surveys or research initiatives.

Where consent is relied upon:

- Consent shall be obtained through clear and lawful means;
- Consent shall not be misleading or deceptive;
- Records of consent may be maintained;
- Data subjects may withdraw consent at any time, subject to legal or contractual limitations.

Withdrawal of consent shall not affect processing that occurred prior to withdrawal.

5.3 CONTRACTUAL NECESSITY

The Company may process personal information where such processing is necessary to:

- Enter into a contract;
- Perform contractual obligations;
- Deliver agreed services;
- Provide platform functionality;
- Manage subscriptions;
- Process payments;
- Deliver coaching services;
- Provide customer support.

Examples include:

- Client onboarding;
- Coaching programme administration;
- User account management;
- Subscription management;
- Payment processing;
- Customer service activities;
- Platform authentication.

Failure to provide required information may affect the Company's ability to provide products or services.

5.4 LEGAL OBLIGATIONS

The Company may process personal information where required by law.

Examples include:

- Tax administration requirements;
- Financial recordkeeping obligations;
- Regulatory reporting obligations;
- Employment-related obligations;
- Anti-fraud activities;
- Responses to lawful requests from regulatory authorities;
- Court orders and legal proceedings.

The Company may disclose information where required by applicable legislation or lawful authority.

5.5 LEGITIMATE INTERESTS OF THE COMPANY

The Company may process personal information where such processing is reasonably necessary to pursue legitimate business interests and where the rights of data subjects are not unreasonably prejudiced.

Examples include:

- Information security activities;
- Fraud prevention;
- Risk management;
- Platform administration;
- Service improvement;
- Product development;
- Internal reporting;
- Business continuity planning;
- Analytics and performance monitoring;
- Customer relationship management.

Legitimate interest processing shall be assessed periodically to ensure fairness and proportionality.

5.6 LEGITIMATE INTERESTS OF DATA SUBJECTS

The Company may process personal information where processing is necessary to protect the legitimate interests of a data subject.

Examples may include:

- Protecting user accounts;
- Preventing unauthorised access;
- Assisting with account recovery;
- Responding to security incidents;
- Protecting personal information from misuse;
- Maintaining service continuity.

5.7 COACHING SERVICES

The Company provides coaching services that require the processing of personal information to facilitate personal development, accountability, coaching engagements, and related services.

Such processing is generally based upon:

- Contractual necessity;
- Legitimate interests;
- Consent where applicable.

Information provided during coaching engagements shall be treated as confidential, subject to applicable legal requirements and contractual obligations.

5.8 AI-ENABLED SERVICES

The Company may utilise artificial intelligence technologies as part of certain products, services, and platform features.

Processing associated with AI-enabled services may be based upon:

- Contractual necessity;
- Legitimate interests;
- Consent where required.

The Company shall seek to ensure that:

- AI processing supports legitimate business purposes;
- Data minimisation principles are applied;
- Appropriate safeguards are maintained;
- Users are informed where AI functionality forms part of a service.

The Company shall not rely exclusively upon automated processing for decisions that may materially affect an individual's rights, opportunities, or legal position without appropriate human oversight.

5.9 MARKETING ACTIVITIES

The Company may process personal information for marketing purposes where:

- Consent has been obtained;
- A lawful existing customer relationship exists;
- Processing is otherwise permitted by applicable legislation.

Marketing activities may include:

- Newsletters;
- Educational content;
- Product announcements;
- Event invitations;
- Promotional communications;
- Service updates.

Data subjects shall be provided with reasonable opportunities to opt out of marketing communications.

5.10 CROSS-BORDER PROCESSING

Where personal information is transferred internationally, the Company shall ensure that an appropriate lawful basis exists for such transfer.

The Company may transfer information internationally where:

- Necessary to perform services;
- Necessary to utilise cloud infrastructure;
- Necessary to utilise approved service providers;
- Required by law;
- Consent has been obtained where appropriate.

Reasonable steps shall be taken to ensure adequate protection of personal information.

5.11 SPECIAL PERSONAL INFORMATION

The Company shall apply additional care when processing special personal information.

Where required, the Company shall rely upon:

- Explicit consent;
- Applicable statutory authorisation;
- Contractual necessity;

- Other lawful grounds recognised by POPIA.

Additional safeguards may be implemented where special personal information is processed.

5.12 REVIEW OF PROCESSING ACTIVITIES

The Company shall periodically review its processing activities to ensure that:

- Appropriate lawful bases remain valid;
- Processing activities remain necessary;
- Data minimisation principles are applied;
- Privacy risks are appropriately managed.

Where a lawful basis no longer exists, the Company shall take appropriate steps to cease processing or identify an alternative lawful basis consistent with applicable legal requirements.

6. CONSENT MANAGEMENT AND PRIVACY NOTICES

6.1 Purpose

The purpose of this section is to establish the principles, controls, and procedures governing the collection, management, recording, and withdrawal of consent by data subjects.

VAYU Coaching Technologies (Pty) Ltd ("the Company") recognises that consent is an important lawful basis for processing personal information in certain circumstances and is committed to ensuring that consent is obtained and managed in a lawful and transparent manner.

6.2 PRINCIPLES OF CONSENT

Where consent is relied upon as the lawful basis for processing personal information, such consent shall be:

- Voluntary;
- Specific;
- Informed;
- Unambiguous;
- Freely given;
- Capable of being withdrawn.

The Company shall not obtain consent through misleading, deceptive, coercive, or unfair practices.

Consent shall not be bundled with unrelated purposes where separate consent options are reasonably practicable.

6.3 WHEN CONSENT IS REQUIRED

The Company may rely on consent for activities including:

- Newsletter subscriptions;
- Marketing communications;
- Promotional campaigns;
- Webinar registrations;
- Downloadable resources;
- Surveys and feedback programmes;
- Testimonials;
- Certain optional platform features;
- Research initiatives;
- Optional AI-powered functionality where appropriate.

The Company shall not rely on consent where another lawful basis more appropriately applies.

6.4 OBTAINING CONSENT

Consent may be obtained through various channels including:

- Website forms;
- Mobile applications;
- Electronic registration processes;
- Written agreements;
- Email confirmations;
- Digital acceptance mechanisms;
- Event registrations;
- Customer onboarding processes.

Examples of acceptable consent mechanisms include:

- Unticked checkboxes;
- Explicit opt-in selections;
- Written confirmations;
- Electronic acknowledgements.

Pre-ticked boxes shall not be relied upon as evidence of valid consent.

6.5 RECORDING OF CONSENT

Where reasonably practicable, the Company shall maintain records demonstrating:

- When consent was obtained;
- How consent was obtained;
- What information was provided at the time consent was obtained;
- What activities were authorised by the consent;
- Whether consent has subsequently been withdrawn.

Consent records may be retained for compliance, audit, and dispute-resolution purposes.

6.6 WITHDRAWAL OF CONSENT

Data subjects shall be entitled to withdraw consent at any time.

The Company shall make reasonable efforts to provide accessible mechanisms for withdrawing consent.

Examples may include:

- Unsubscribe links;
- Account settings;
- Email requests;
- Written requests;
- Customer support channels.

The withdrawal of consent shall not affect:

- Processing conducted before withdrawal;
- Processing required by law;
- Processing required for contractual obligations;
- Processing based on another lawful basis.

6.7 PRIVACY NOTICES

The Company shall provide privacy notices designed to inform data subjects regarding the processing of their personal information.

Privacy notices may be provided through:

- Websites;
- Mobile applications;
- Registration forms;
- Client agreements;
- Coaching agreements;
- Terms of Service;
- Privacy Policies;
- Marketing forms;

- User onboarding processes.

Privacy notices should be clear, understandable, and reasonably accessible.

6.8 CONTENT OF PRIVACY NOTICES

Where appropriate, privacy notices shall explain:

- The identity of the Company;
- Contact details of the Information Officer;
- Categories of information collected;
- Purpose of collection;
- Lawful basis for processing;
- Categories of recipients;
- Cross-border transfers where applicable;
- Data subject rights;
- Complaint procedures;
- Consequences of failing to provide information where applicable.

The Company shall seek to avoid unnecessarily complex or misleading privacy notices.

6.9 MARKETING CONSENT

Where consent is required for marketing communications, the Company shall:

- Obtain appropriate consent;
- Record consent where reasonably practicable;
- Respect opt-out requests;
- Maintain suppression lists where appropriate;
- Avoid sending communications after consent has been withdrawn.

Marketing preferences shall be respected and updated as promptly as reasonably practicable.

6.10 COACHING SERVICES

The Company recognises that coaching relationships frequently involve the voluntary disclosure of personal information.

Prior to the commencement of coaching services, clients shall be provided with:

- Information regarding the processing of personal information;
- Applicable privacy notices;
- Coaching agreements where appropriate;
- Information regarding confidentiality limitations.

Where coaching services involve optional activities requiring consent, such consent shall be obtained separately where appropriate.

6.11 AI-ENABLED SERVICES

Where AI-powered functionality forms part of a product or service, the Company shall seek to provide reasonable transparency regarding:

- The use of artificial intelligence;
- The nature of AI-assisted functionality;
- The role of human oversight where applicable;
- Limitations of AI-generated content;
- Applicable privacy considerations.

The Company may require users to acknowledge AI-related disclosures before accessing certain AI-enabled features.

6.12 CHILDREN AND DEPENDENT PERSONS

Where consent is required in relation to children or persons lacking legal capacity to provide consent, the Company shall take reasonable steps to obtain consent from an authorised competent person where required by law.

6.13 REVIEW OF CONSENT PRACTICES

The Company shall periodically review:

- Consent collection mechanisms;
- Privacy notices;
- Marketing practices;
- User onboarding processes;
- Platform registration processes;
- AI-related disclosures.

The purpose of such reviews shall be to ensure continued compliance with POPIA, transparency obligations, and recognised privacy best practices.

6.14 ACCOUNTABILITY

The Information Officer shall oversee the Company's consent management programme and shall ensure that reasonable measures are implemented to:

- Demonstrate compliance;
- Maintain appropriate records;
- Address privacy concerns;
- Support data subject rights;
- Improve transparency regarding information processing activities.

7. DATA SUBJECT RIGHTS AND REQUEST MANAGEMENT

7.1 Purpose

The purpose of this section is to establish the principles, procedures, and responsibilities governing the exercise of data subject rights and the management of requests relating to personal information processed by VAYU Coaching Technologies (Pty) Ltd ("the Company").

The Company recognises that individuals have rights regarding their personal information and is committed to facilitating the lawful exercise of those rights in accordance with the Protection of Personal Information Act, 2013 ("POPIA"), the Promotion of Access to Information Act, 2000 ("PAIA"), and any other applicable legislation.

7.2 DATA SUBJECT RIGHTS

Subject to applicable legal limitations and exceptions, data subjects may exercise the following rights.

Right of Access

A data subject may request confirmation regarding whether the Company holds personal information relating to them and may request access to such information.

Access requests shall be processed in accordance with:

- POPIA;
- PAIA;
- The Company's PAIA Manual;
- Applicable legal requirements.

Right to Correction

A data subject may request the correction, updating, or amendment of personal information that is:

- Inaccurate;
- Incomplete;
- Misleading;
- Outdated.

The Company may require reasonable evidence to support correction requests.

Right to Deletion

A data subject may request the deletion, destruction, anonymisation, or de-identification of personal information where:

- The information is no longer required;
- Processing is no longer lawful;
- Retention is no longer necessary;
- Applicable legal requirements permit deletion.

The Company may decline deletion requests where retention is required by law, contract, litigation requirements, regulatory obligations, or legitimate business interests.

Right to Object

A data subject may object to certain forms of processing where permitted by law.

Such objections may relate to:

- Direct marketing;
- Certain legitimate-interest processing activities;
- Other processing activities recognised by applicable legislation.

The Company shall consider such objections and respond in accordance with applicable legal requirements.

Right to Withdraw Consent

Where processing is based upon consent, a data subject may withdraw consent at any time.

Withdrawal shall not affect:

- Processing conducted before withdrawal;
- Processing based upon another lawful basis;
- Processing required by law;
- Processing required to fulfil contractual obligations.

Right to Complain

A data subject may lodge a complaint with:

- The Company's Information Officer;
- The Information Regulator;
- A court or tribunal where applicable.

The Company encourages data subjects to first engage with the Information Officer where appropriate to facilitate efficient resolution.

7.3 SUBMISSION OF REQUESTS

Requests relating to personal information should be submitted to the Information Officer.

Information Officer

Chris Roos

Founder, Chief Executive Officer, Director and Information Officer

Email:

chris.roos@vayulifecoaching.co.za

Compliance Email:

compliance@vayulifecoaching.co.za

Telephone:

+27 62 732 1090

Physical Address:

134 Ranger Road

Fish Hoek

Cape Town

7975

Western Cape

South Africa

7.4 VERIFICATION OF IDENTITY

Before acting on a request, the Company may require reasonable verification of identity.

Verification measures may include:

- Proof of identity;
- Verification of account ownership;
- Confirmation of contact details;
- Additional supporting documentation where appropriate.

The purpose of verification is to prevent unauthorised disclosure of personal information.

7.5 PROCESSING OF REQUESTS

Upon receipt of a request, the Company may:

1. Acknowledge receipt of the request;
2. Verify the identity of the requester;
3. Assess the scope of the request;
4. Determine whether additional information is required;
5. Consider applicable legal obligations;
6. Consult relevant stakeholders where necessary;
7. Issue a response.

Requests shall be handled fairly, consistently, and in accordance with applicable legislation.

7.6 RESPONSE TIMEFRAMES

The Company shall endeavour to respond to requests within the time periods prescribed by applicable legislation.

Response times may vary depending on:

- Complexity of the request;
- Volume of information involved;
- Third-party consultation requirements;
- Verification requirements;
- Legal considerations.

Where additional time is required, the requester shall be informed where appropriate.

7.7 REFUSAL OF REQUESTS

The Company may refuse requests where permitted by law.

Grounds for refusal may include:

- Protection of third-party privacy rights;
- Protection of confidential information;
- Protection of intellectual property;
- Protection of commercially sensitive information;
- Legal privilege;
- Security considerations;
- Regulatory restrictions;
- Other lawful grounds.

Detailed grounds for refusal are contained within the Company's PAIA Manual.

7.8 REQUESTS INVOLVING COACHING INFORMATION

The Company recognises that coaching engagements frequently involve highly personal and confidential information.

Where requests involve coaching-related information, the Company shall consider:

- Confidentiality obligations;
- Privacy rights;
- Contractual obligations;
- Third-party interests;
- Applicable legal requirements.

Special care shall be exercised when assessing requests involving coaching records.

7.9 REQUESTS INVOLVING AI-ENABLED SERVICES

Where requests relate to AI-generated content, AI interaction histories, or AI-assisted services, the Company shall assess:

- The nature of the information requested;
- The rights of the requester;
- Technical feasibility;
- Security considerations;
- Third-party rights;
- Applicable legal obligations.

The Company does not guarantee that all AI interactions are retained indefinitely and may apply applicable retention schedules.

7.10 INTERNAL ESCALATION

Where a request raises significant legal, privacy, security, or operational considerations, the Information Officer may escalate the matter for further review before a final decision is issued.

Such review may include consultation with:

- Legal advisors;
- Compliance specialists;
- Technology providers;
- Relevant service providers;
- Security specialists.

7.11 RECORDS OF REQUESTS

The Company shall maintain records of requests received, including:

- Date received;
- Nature of the request;
- Verification activities;
- Decisions made;
- Responses issued;
- Any corrective actions taken.

Such records may be retained for audit, compliance, governance, and dispute-resolution purposes.

7.12 NON-DISCRIMINATION

The Company shall not unfairly discriminate against any individual for exercising their rights under POPIA or PAIA.

The exercise of privacy rights shall not, in itself, result in adverse treatment, except where limitations arise due to the operational, legal, or contractual consequences of the request.

7.13 CONTINUOUS IMPROVEMENT

The Company shall periodically review:

- Request management procedures;
- Response processes;
- Data subject communications;
- Complaint handling mechanisms;
- Privacy governance controls.

The purpose of such reviews shall be to improve transparency, accountability, and the effective protection of personal information.

8. INFORMATION SECURITY AND TECHNICAL SAFEGUARDS

8.1 Purpose

The purpose of this section is to establish the information security principles, safeguards, responsibilities, and controls implemented by VAYU Coaching Technologies (Pty) Ltd ("the Company") to protect personal information and other confidential information against unauthorised access, disclosure, alteration, loss, destruction, misuse, or compromise.

The Company recognises that information security is a critical component of compliance with the Protection of Personal Information Act, 2013 ("POPIA"), and forms an essential part of responsible business operations.

8.2 SECURITY OBJECTIVES

The Company's information security programme is designed to protect:

Confidentiality

Ensuring information is accessible only to authorised individuals.

Integrity

Ensuring information remains accurate, complete, and protected against unauthorised modification.

Availability

Ensuring authorised users can access information and systems when required.

Accountability

Ensuring actions involving information can be traced, monitored, and reviewed where appropriate.

8.3 SECURITY GOVERNANCE

The Information Officer shall oversee information governance and privacy-related security matters.

Security responsibilities include:

- Risk identification;
- Security monitoring;
- Access management oversight;
- Incident management;
- Vendor security assessments;
- Compliance monitoring;
- Security awareness activities.

The Company may engage external specialists where additional expertise is required.

8.4 ACCESS CONTROL

Access to information shall be limited according to legitimate business requirements.

The Company shall seek to implement:

- Role-based access controls;
- Least-privilege principles;
- User authentication controls;
- Access approval procedures;
- Access review procedures;
- Access revocation procedures.

Individuals shall only be granted access to information necessary for authorised business purposes.

8.5 PASSWORD SECURITY

The Company shall maintain appropriate password security practices.

Where technically supported:

- Strong passwords shall be required;
- Password reuse should be discouraged;
- Password managers should be utilised;
- Shared passwords should be avoided;
- Default passwords should be changed promptly.

Passwords shall never be stored in plain text where secure alternatives are available.

8.6 MULTI-FACTOR AUTHENTICATION

Multi-factor authentication ("MFA") shall be enabled wherever reasonably practicable for:

- Google Workspace accounts;
- HubSpot accounts;
- Xero accounts;
- Payment platforms;
- Administrative systems;
- Cloud service providers;
- Domain management systems;
- AI service provider accounts.

Administrative accounts shall receive priority for MFA implementation.

8.7 DEVICE SECURITY

Devices used to access Company systems should be protected through appropriate security controls.

Such controls may include:

- Device passwords or biometrics;
- Operating system updates;
- Anti-malware protection;
- Screen locking;
- Encryption where available;
- Secure backups.

Lost or stolen devices containing Company information shall be reported as soon as reasonably practicable.

8.8 CLOUD SERVICES SECURITY

The Company utilises cloud-based services to support business operations.

Examples may include:

- Google Workspace;
- HubSpot;
- Xero;
- PayFast;
- OpenAI;
- Anthropic Claude;
- Future technology providers adopted by the Company.

The Company shall seek to utilise reputable providers that maintain reasonable security controls and privacy safeguards.

8.9 ENCRYPTION

Where reasonably practicable, the Company shall utilise encryption technologies to protect information during:

- Transmission;
- Storage;
- Backup activities;
- External communications.

The Company shall rely upon security controls provided by approved service providers where appropriate.

8.10 BACKUP AND RECOVERY

The Company shall maintain reasonable measures designed to support information recovery in the event of:

- System failure;
- Human error;
- Cybersecurity incidents;
- Data corruption;
- Accidental deletion.

Backup arrangements may include:

- Cloud-based backups;
- Service provider backup systems;
- Recovery procedures;
- Business continuity measures.

8.11 LOGGING AND MONITORING

Where technically feasible, the Company may maintain records relating to:

- Account access;
- Login activity;
- Administrative actions;
- Security events;
- Platform activity;
- System performance.

Monitoring activities shall be conducted in accordance with applicable legal requirements and legitimate business purposes.

8.12 SECURITY OF COACHING INFORMATION

The Company recognises that coaching information frequently contains highly personal and confidential information.

Additional care shall be taken when processing:

- Coaching notes;
- Client assessments;
- Goal-setting information;
- Accountability records;
- Session summaries;
- Journal entries;
- Personal reflections.

Access to such information shall be restricted to authorised individuals with a legitimate business need.

8.13 SECURITY OF AI-RELATED INFORMATION

Where AI-enabled services are utilised, the Company shall seek to implement reasonable safeguards relating to:

- Prompt submissions;
- AI-generated responses;
- User interaction data;
- Service provider access controls;
- Data minimisation practices;
- Monitoring of AI-related risks.

The Company shall seek to avoid unnecessary disclosure of personal information to AI service providers.

8.14 THIRD-PARTY SERVICE PROVIDERS

The Company may utilise third-party operators and service providers.

Reasonable steps shall be taken to:

- Assess service providers;
- Review privacy commitments;
- Review security controls;
- Maintain contractual protections where appropriate;
- Monitor provider performance.

Third-party operators shall only receive information reasonably necessary to perform authorised services.

8.15 PHYSICAL SECURITY

The Company shall implement reasonable measures designed to protect physical records and equipment.

Measures may include:

- Controlled access to work areas;
- Secure storage of records;
- Protection of devices;
- Secure disposal of documents;
- Visitor management practices where applicable.

8.16 SECURITY INCIDENT REPORTING

Any suspected or actual security incident should be reported to the Information Officer as soon as reasonably practicable.

Examples include:

- Unauthorised access;
- Loss of information;
- Theft of devices;
- Misdirected communications;
- Malware infections;
- Credential compromise;
- Unauthorised disclosure of personal information.

All incidents shall be assessed and investigated appropriately.

8.17 INFORMATION CLASSIFICATION

Information shall be classified according to its sensitivity and business impact.

The Company may utilise classifications including:

Public

Information intended for public release.

Internal

Information intended for internal business use.

Confidential

Information requiring restricted access.

Restricted

Highly sensitive information requiring enhanced protection.

Appropriate safeguards shall be applied based upon classification.

8.18 SECURITY AWARENESS

The Company shall promote security awareness among:

- Employees;
- Contractors;
- Consultants;
- Service providers where appropriate.

Security awareness activities may include:

- Privacy awareness;
- Password security guidance;
- Phishing awareness;
- AI usage guidance;
- Information handling procedures;
- Incident reporting requirements.

8.19 SECURITY REVIEWS

The Company shall periodically review:

- Security controls;
- Privacy safeguards;
- Access permissions;
- Service providers;
- AI-related risks;
- Emerging threats.

Reviews shall be conducted at least annually or more frequently where circumstances warrant.

8.20 CONTINUOUS IMPROVEMENT

Information security is an ongoing process.

The Company shall seek to continuously improve its security posture through:

- Risk assessments;
- Lessons learned from incidents;
- Technology improvements;
- Regulatory developments;
- Industry best practices;
- Periodic governance reviews.

The Company recognises that no security programme can eliminate all risk and therefore adopts a risk-based approach to information protection.

9. THIRD-PARTY OPERATORS, CLOUD SERVICES AND CROSS-BORDER DATA TRANSFERS

9.1 Purpose

The purpose of this section is to establish the governance principles, responsibilities, controls, and procedures relating to third-party operators, cloud service providers, software providers, artificial intelligence providers, and cross-border transfers of personal information.

VAYU Coaching Technologies (Pty) Ltd ("the Company") recognises that the use of third-party service providers is necessary for the delivery of its services and is committed to ensuring that personal information remains appropriately protected throughout the information processing lifecycle.

9.2 GOVERNING PRINCIPLES

The Company shall seek to ensure that:

- Personal information is shared only where necessary;
- Data minimisation principles are applied;
- Appropriate safeguards are implemented;
- Service providers are selected responsibly;
- Cross-border transfers are appropriately managed;
- Operators process information only for authorised purposes;
- Privacy and security obligations are respected.

The Company remains accountable for personal information processed on its behalf by third-party operators.

9.3 DEFINITION OF AN OPERATOR

For purposes of this Framework, an operator refers to any third party that processes personal information on behalf of the Company.

Examples may include:

- Cloud service providers;
- Software-as-a-Service providers;
- Customer relationship management providers;
- Payment processors;
- Artificial intelligence providers;
- Hosting providers;
- Analytics providers;
- Marketing service providers;
- Professional advisors.

9.4 CURRENT OPERATORS AND SERVICE PROVIDERS

The Company may utilise the following core service providers.

Google Workspace

Purpose:

- Email services;
- Document management;
- Collaboration;
- File storage;
- Calendar management;
- Business communications.

Potential Information Processed:

- Contact information;
- Communications;
- Documents;
- Business records;
- Client records.

HubSpot

Purpose:

- Customer relationship management;
- Lead management;
- Sales administration;
- Marketing communications;
- Customer support.

Potential Information Processed:

- Names;
- Contact details;
- Communication records;
- Lead information;
- Customer relationship information.

Xero

Purpose:

- Accounting;
- Invoicing;
- Financial administration;
- Tax administration;
- Financial reporting.

Potential Information Processed:

- Customer information;
- Supplier information;
- Financial transactions;
- Accounting records.

PayFast

Purpose:

- Payment processing;
- Subscription payments;
- Transaction administration.

Potential Information Processed:

- Customer information;
- Billing information;

- Transaction records.

The Company shall seek to avoid storing unnecessary payment information directly.

OpenAI

Purpose:

- AI-assisted coaching services;
- Content generation;
- Platform functionality;
- Productivity and operational support;
- User-facing AI features.

Potential Information Processed:

- User prompts;
- User responses;
- Interaction data;
- Service-related information.

The Company shall seek to minimise unnecessary personal information submitted to AI systems.

Anthropic Claude

Purpose:

- AI-assisted business operations;
- Research and content generation;
- Platform support functions;
- Internal productivity functions.

Potential Information Processed:

- Prompts;
- Responses;
- Operational information;
- Service-related information.

9.5 OPERATOR SELECTION CRITERIA

When selecting operators, the Company shall consider factors including:

- Reputation;
- Security capabilities;
- Privacy commitments;
- Regulatory compliance;
- Reliability;
- Business continuity considerations;
- Data protection practices;
- Contractual protections.

The Company shall seek to engage providers that maintain appropriate technical and organisational safeguards.

9.6 OPERATOR OBLIGATIONS

Where reasonably practicable, operators engaged by the Company should:

- Process information only on authorised instructions;
- Maintain confidentiality;
- Implement appropriate security measures;
- Notify the Company of relevant incidents;
- Comply with applicable legal requirements;
- Protect personal information from unauthorised access or disclosure.

The Company may rely upon service provider agreements, terms of service, privacy commitments, and other contractual arrangements to support these obligations.

9.7 CROSS-BORDER TRANSFERS

Personal information may be transferred to, processed in, stored in, backed up in, or accessed from jurisdictions outside South Africa.

Such transfers may occur where:

- Cloud services are utilised;
- Software providers operate internationally;
- AI providers process information internationally;
- Business continuity requirements necessitate distributed infrastructure;
- International service providers are engaged.

The Company shall seek to ensure that such transfers occur lawfully and with appropriate safeguards.

9.8 INTERNATIONAL PROCESSING ENVIRONMENTS

Depending upon the service provider utilised, personal information may be processed in jurisdictions including:

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

The precise location of processing may vary depending upon infrastructure configurations and service provider arrangements.

9.9 SAFEGUARDS FOR INTERNATIONAL TRANSFERS

The Company shall seek to implement reasonable safeguards including:

- Contractual protections;
- Service provider security commitments;
- Vendor due diligence;
- Access controls;
- Encryption technologies;
- Data minimisation practices;
- Ongoing provider reviews.

Cross-border transfers shall be assessed in light of applicable legal obligations and business requirements.

9.10 DATA MINIMISATION FOR THIRD-PARTY PROCESSING

The Company shall seek to disclose only the information reasonably necessary for a service provider to perform authorised services.

Where reasonably practicable, the Company shall:

- Limit access rights;
- Limit categories of information shared;
- Avoid unnecessary disclosure;
- Utilise anonymisation where appropriate;
- Utilise de-identification where appropriate.

9.11 ARTIFICIAL INTELLIGENCE PROVIDERS

The Company recognises that AI service providers present unique privacy, confidentiality, and governance considerations.

Accordingly, the Company shall seek to:

- Limit unnecessary personal information submitted to AI systems;
- Review provider privacy commitments;
- Monitor developments in AI regulation;
- Apply appropriate human oversight;
- Maintain transparency regarding AI-enabled processing;
- Periodically review AI-related risks.

The Company shall seek to ensure that AI-enabled processing remains consistent with POPIA principles and the Company's ethical obligations.

9.12 THIRD-PARTY RISK MANAGEMENT

The Company shall periodically review:

- Service provider relationships;
- Privacy commitments;
- Security controls;
- Incident histories;
- Regulatory developments;
- Emerging risks.

The purpose of such reviews is to support responsible governance and ongoing compliance.

9.13 TERMINATION OF OPERATOR RELATIONSHIPS

Where a relationship with an operator is terminated, the Company shall seek to ensure that:

- Access rights are removed;
- Data access is revoked where appropriate;
- Information is returned, deleted, or otherwise handled in accordance with contractual and legal requirements;
- Security risks are appropriately managed.

9.14 ACCOUNTABILITY

The Information Officer shall maintain oversight of:

- Third-party operator relationships;
- Cross-border processing activities;
- AI service provider governance;
- Privacy risks associated with outsourced processing activities.

The Company acknowledges that accountability for personal information cannot be outsourced and remains responsible for ensuring that information processed on its behalf receives appropriate protection.

10. ARTIFICIAL INTELLIGENCE GOVERNANCE AND RESPONSIBLE AI USE

10.1 Purpose

The purpose of this section is to establish the principles, controls, responsibilities, and governance measures governing the use of artificial intelligence ("AI") by VAYU Coaching Technologies (Pty) Ltd ("the Company").

The Company recognises the significant opportunities presented by AI technologies while also acknowledging the potential privacy, security, ethical, legal, and operational risks associated with their use.

The Company is committed to ensuring that AI technologies are used responsibly, transparently, ethically, and in a manner consistent with applicable legal requirements and the Company's values.

10.2 SCOPE

This section applies to:

- AI-powered coaching features;
- AI-assisted content generation;
- AI-assisted customer support;
- AI-assisted productivity tools;
- AI-enabled platform features;
- Internal AI usage by employees or contractors;
- Third-party AI service providers;
- Future AI technologies adopted by the Company.

10.3 AI GOVERNANCE PRINCIPLES

The Company shall seek to ensure that AI technologies are used in accordance with the following principles:

Transparency

Users should be informed where AI forms part of a product, service, feature, or interaction.

Accountability

The Company remains accountable for the implementation and governance of AI-enabled services.

Human Oversight

Appropriate human oversight shall be maintained for significant decisions, sensitive situations, and high-risk activities.

Privacy

AI usage shall remain consistent with POPIA and the Company's privacy obligations.

Fairness

The Company shall seek to reduce unfair bias and discriminatory outcomes where reasonably practicable.

Security

AI systems shall be incorporated into the Company's information security programme.

Data Minimisation

Only information reasonably necessary for authorised purposes should be processed through AI-enabled services.

10.4 PERMITTED USES OF AI

The Company may utilise AI technologies for purposes including:

- Coaching support;
- Goal-setting assistance;
- Reflection and journaling assistance;
- Habit formation support;
- Personal development guidance;
- Educational content generation;
- Customer support;
- Productivity enhancement;
- Research assistance;
- Content drafting;
- Service improvement;
- Platform functionality.

The Company reserves the right to expand or modify AI-enabled functionality over time.

10.5 PROHIBITED OR RESTRICTED USES OF AI

The Company shall seek to avoid utilising AI systems for:

- Unlawful activities;
- Deceptive activities;
- Discriminatory activities;
- Unauthorised surveillance;
- Processing activities prohibited by law;
- Activities that materially infringe the rights of individuals.

The Company shall not intentionally position AI-generated content as regulated professional advice.

10.6 HUMAN OVERSIGHT

The Company recognises that AI systems may produce inaccurate, incomplete, misleading, biased, or inappropriate outputs.

Accordingly:

- Human judgment shall remain important;
- Significant business decisions should not rely solely upon AI outputs;
- AI-generated information should be reviewed where appropriate;
- Human intervention may be required for sensitive situations.

The Company reserves the right to review, monitor, modify, or remove AI-generated content where necessary.

10.7 AI AND COACHING SERVICES

The Company may utilise AI to enhance coaching-related services.

AI may assist with:

- Reflection exercises;
- Goal clarification;
- Accountability support;
- Habit development;
- Educational content;
- Self-assessment activities;
- Personal development exercises.

However:

- AI is not a substitute for professional counselling;
- AI is not a substitute for psychotherapy;
- AI is not a substitute for psychiatric treatment;
- AI is not a substitute for medical advice;
- AI is not a substitute for legal advice;
- AI is not a substitute for financial advice.

Users remain responsible for exercising independent judgment regarding AI-generated content.

10.8 USER DISCLOSURES

Where AI functionality forms part of a service, the Company shall seek to provide reasonable disclosures regarding:

- The use of AI technologies;
- The role of AI within the service;
- The limitations of AI-generated content;
- The possibility of inaccuracies;
- The importance of independent judgment.

The Company may require acknowledgement of AI disclosures before access to certain features is granted.

10.9 AI INPUTS AND PROMPTS

Users may voluntarily submit information to AI-enabled services.

The Company shall seek to:

- Minimise unnecessary personal information processing;
- Promote responsible use of AI features;
- Implement appropriate privacy safeguards;
- Restrict access to authorised personnel where applicable.

Users are encouraged to exercise discretion when providing highly sensitive information through AI-enabled services.

10.10 AI OUTPUTS

AI-generated outputs may:

- Contain inaccuracies;
- Be incomplete;
- Become outdated;
- Reflect limitations of underlying technologies.

The Company makes no representation that AI-generated content will always be accurate, complete, reliable, or suitable for every circumstance.

AI-generated content should be considered informational in nature unless expressly stated otherwise.

10.11 FAIRNESS AND BIAS

The Company acknowledges that AI systems may exhibit bias arising from:

- Training data;
- System design;
- Model limitations;
- User inputs.

The Company shall seek to:

- Monitor AI-related risks;
- Reduce unfair bias where reasonably practicable;
- Review complaints relating to AI outputs;
- Promote fair and responsible AI usage.

The Company does not guarantee that all AI-generated outputs will be free from bias.

10.12 PRIVACY AND CONFIDENTIALITY

The use of AI technologies shall remain subject to:

- POPIA;
- This Framework;
- The Company's Privacy Policy;
- Information security requirements;
- Applicable contractual obligations.

Reasonable steps shall be taken to protect personal information processed through AI-enabled services.

10.13 THIRD-PARTY AI PROVIDERS

The Company may utilise third-party AI providers including, but not limited to:

- OpenAI;
- Anthropic;
- Future approved AI providers.

The Company shall seek to:

- Review provider privacy commitments;
- Review provider security controls;
- Assess provider suitability;
- Monitor developments affecting AI governance.

10.14 AI INCIDENTS

The Company shall investigate AI-related incidents where appropriate.

Examples may include:

- Privacy concerns;
- Security concerns;
- Harmful outputs;
- System failures;
- Significant inaccuracies;
- Complaints relating to AI functionality.

Corrective measures may be implemented where appropriate.

10.15 CONTINUOUS MONITORING AND REVIEW

The Company acknowledges that AI technologies continue to evolve rapidly.

Accordingly, the Company shall periodically review:

- AI governance practices;
- AI-related risks;
- Regulatory developments;
- Industry standards;
- User feedback;
- Service provider capabilities.

This section shall be reviewed and updated as AI technologies and regulatory expectations continue to develop.

10.16 ACCOUNTABILITY

The Information Officer shall maintain oversight of AI governance activities and shall seek to ensure that AI-enabled services operate in a manner consistent with:

- POPIA;
- Applicable laws;
- Ethical business practices;
- Information security requirements;
- The Company's commitment to responsible innovation.

The Company remains accountable for the governance of AI-enabled services deployed within its business operations.

11. DATA RETENTION, ARCHIVING AND SECURE DESTRUCTION

11.1 Purpose

The purpose of this section is to establish the principles, responsibilities, controls, and procedures governing the retention, archiving, deletion, destruction, anonymisation, and de-identification of information processed by VAYU Coaching Technologies (Pty) Ltd ("the Company").

The Company recognises that personal information should not be retained longer than is reasonably necessary and is committed to maintaining retention practices that support compliance with the Protection of Personal Information Act, 2013 ("POPIA"), applicable legislation, contractual obligations, and legitimate business requirements.

11.2 RETENTION PRINCIPLES

The Company shall seek to ensure that information is:

- Retained only for lawful purposes;
- Retained only for as long as reasonably necessary;
- Protected throughout its lifecycle;
- Reviewed periodically;
- Securely destroyed when no longer required.

The Company shall avoid indefinite retention unless there is a lawful justification for doing so.

11.3 GROUNDS FOR RETENTION

Information may be retained where necessary to:

- Fulfil contractual obligations;
- Deliver products or services;
- Comply with legal obligations;
- Meet tax requirements;
- Meet regulatory requirements;
- Resolve disputes;
- Defend legal claims;
- Support information security activities;
- Maintain business continuity;
- Protect legitimate business interests.

11.4 RECORD RETENTION SCHEDULE

The Company shall maintain a Record Retention and Destruction Schedule.

The current schedule is contained in Appendix C of this Framework and may be amended from time to time.

The schedule shall define:

- Categories of records;
- Applicable retention periods;
- Archiving requirements;
- Destruction requirements;
- Legal hold requirements.

11.5 ARCHIVING

Where information is no longer actively required but remains subject to retention obligations, the Company may archive such information.

Archived information may include:

- Historical client records;
- Historical coaching records;
- Financial records;
- Tax records;
- Compliance documentation;
- Contractual records;
- Platform records.

Archived information shall continue to receive appropriate protection.

11.6 COACHING RECORDS

The Company recognises that coaching records may contain highly confidential and sensitive personal information.

Retention of coaching records shall be guided by:

- Contractual obligations;
- Professional considerations;
- Legal requirements;
- Privacy considerations;
- Legitimate business needs.

Access to archived coaching records shall remain restricted to authorised persons.

11.7 PLATFORM USER INFORMATION

Information relating to users of the VAYU platform may be retained for purposes including:

- Account management;
- Subscription administration;
- Customer support;
- Security monitoring;
- Regulatory compliance;
- Dispute resolution;
- Product improvement.

Retention periods shall be governed by the Record Retention and Destruction Schedule.

11.8 USER-GENERATED CONTENT

User-generated content may include:

- Journal entries;
- Notes;
- Reflections;
- Goal-tracking records;
- Habit-tracking records;
- Assessment responses;
- Uploaded content.

The Company shall seek to provide reasonable retention controls while balancing:

- User expectations;
- Technical requirements;
- Security requirements;
- Legal obligations;
- Business continuity requirements.

11.9 AI INTERACTION RECORDS

The Company may retain certain AI-related records for purposes including:

- Service delivery;
- Quality assurance;
- Platform improvement;
- Security monitoring;
- Incident investigation;
- Compliance monitoring.

AI-related records shall be retained in accordance with approved retention schedules and applicable legal requirements.

The Company may anonymise or de-identify AI-related information where appropriate.

11.10 ANONYMISATION AND DE-IDENTIFICATION

Where reasonably practicable, the Company may:

- Remove identifiers;
- Aggregate information;
- Anonymise records;
- De-identify records.

Anonymised information may be retained for:

- Statistical purposes;
- Product improvement;
- Research activities;
- Security monitoring;
- Business intelligence.

Provided that such information can no longer reasonably be linked to an identifiable individual.

11.11 DELETION REQUESTS

Data subjects may request deletion of personal information where permitted by law.

Deletion requests shall be assessed in accordance with:

- POPIA;

- Applicable contractual obligations;
- Legal retention requirements;
- Regulatory obligations;
- Legitimate business interests.

The Company may refuse deletion requests where retention remains legally justified.

11.12 SECURE DESTRUCTION

Where information is no longer required, the Company shall seek to ensure that destruction occurs in a secure manner.

Methods may include:

Electronic Records

- Secure deletion;
- Permanent removal from active systems;
- Cryptographic destruction where appropriate;
- Deletion through approved service provider mechanisms.

Physical Records

- Shredding;
- Secure destruction services;
- Physical destruction methods designed to prevent reconstruction.

The objective of destruction is to prevent unauthorised access, recovery, reconstruction, or disclosure.

11.13 LEGAL HOLDS

The Company may suspend normal destruction processes where information is required for:

- Litigation;
- Regulatory investigations;
- Audits;
- Compliance reviews;
- Dispute resolution;
- Law enforcement requirements.

Such records shall be retained until the relevant matter has been resolved or the legal hold has been lifted.

11.14 RESPONSIBILITIES

The Information Officer shall oversee:

- Retention governance;
- Retention schedule maintenance;
- Destruction practices;
- Legal hold processes;
- Compliance reviews.

Employees, contractors, and authorised personnel shall comply with approved retention and destruction requirements.

11.15 PERIODIC REVIEW

The Company shall periodically review:

- Retention periods;
- Archiving practices;
- Destruction procedures;
- Legal requirements;
- Technology changes;
- Business requirements.

Reviews shall be conducted at least annually or more frequently where necessary.

11.16 CONTINUOUS IMPROVEMENT

The Company acknowledges that retention and destruction requirements may evolve over time.

Accordingly, retention practices shall be reviewed and refined periodically to ensure continued compliance with:

- POPIA;
- PAIA;
- Applicable legislation;
- Regulatory guidance;
- Industry best practices;
- Operational requirements.

The Company shall seek to maintain retention practices that balance privacy protection, legal compliance, operational efficiency, and responsible information governance.

12. PRIVACY INCIDENT, DATA BREACH AND SECURITY EVENT MANAGEMENT

12.1 Purpose

The purpose of this section is to establish the principles, responsibilities, procedures, and governance measures relating to the identification, reporting, investigation, management, containment, and resolution of privacy incidents, data breaches, and security events affecting VAYU Coaching Technologies (Pty) Ltd ("the Company").

The Company recognises that despite reasonable safeguards, security incidents may occur and is committed to responding promptly, responsibly, and in accordance with applicable legal requirements.

12.2 OBJECTIVES

The objectives of the Company's incident management programme are to:

- Protect personal information;
- Minimise harm to affected individuals;
- Contain security incidents;
- Restore affected systems and services;
- Preserve evidence where necessary;
- Meet legal and regulatory obligations;
- Improve future security controls;
- Promote accountability and transparency.

12.3 DEFINITIONS

Privacy Incident

Any event that may involve the inappropriate handling, disclosure, loss, alteration, misuse, or unauthorised access to personal information.

Examples include:

- Misdirected emails;
- Unauthorised disclosure;
- Improper access to records;
- Loss of confidential information.

Security Event

Any event that may affect the confidentiality, integrity, or availability of information, systems, devices, applications, or services.

Examples include:

- Malware infections;
- Unauthorised login attempts;
- Credential compromise;
- System failures;
- Suspicious network activity.

Data Breach

A confirmed incident involving:

- Unauthorised access;
- Unauthorised disclosure;
- Loss;
- Destruction;
- Alteration;
- Theft;

of personal information or other protected information.

12.4 INCIDENT REPORTING

All employees, contractors, consultants, and authorised users shall report suspected incidents as soon as reasonably practicable.

Incidents should be reported to:

Information Officer

Chris Roos

Email:
chris.roos@vayulifecoaching.co.za

Alternative Compliance Email:
compliance@vayulifecoaching.co.za

Telephone:
+27 62 732 1090

Prompt reporting is encouraged even where uncertainty exists regarding the nature or severity of the incident.

12.5 INCIDENT CATEGORIES

Incidents may include:

Privacy Incidents

- Accidental disclosure;
- Incorrect recipients;
- Loss of records;
- Unauthorised access to personal information.

Cybersecurity Incidents

- Malware;
- Phishing attacks;
- Credential compromise;
- Ransomware;
- Unauthorised system access.

Physical Security Incidents

- Lost devices;
- Stolen equipment;
- Unauthorised physical access;
- Loss of physical records.

Third-Party Incidents

- Service provider breaches;
- Cloud service incidents;
- Vendor security failures;
- AI provider incidents.

12.6 INITIAL RESPONSE

Upon becoming aware of an incident, the Company shall seek to:

1. Identify the nature of the incident;
2. Contain the incident where possible;
3. Protect affected information;
4. Assess immediate risks;
5. Preserve relevant evidence;
6. Initiate investigation procedures.

The Company shall act proportionately to the nature and severity of the incident.

12.7 INCIDENT INVESTIGATION

The Company shall investigate incidents to determine:

- What occurred;
- When the incident occurred;
- How the incident occurred;
- What information was affected;
- Who may have been affected;
- The extent of potential harm;
- Whether legal obligations are triggered.

Investigations may involve internal personnel, external advisors, technology providers, or other specialists where appropriate.

12.8 INCIDENT CLASSIFICATION

Incidents may be classified according to severity.

Low Severity

Minor incidents with limited impact and minimal risk.

Medium Severity

Incidents involving sensitive information, operational disruption, or elevated risk.

High Severity

Incidents involving significant personal information exposure, major operational impact, regulatory implications, or substantial reputational risk.

Classification may be revised as additional information becomes available.

12.9 DATA BREACH NOTIFICATION

Where required by applicable law, the Company shall notify:

- Affected data subjects;
- The Information Regulator;
- Relevant authorities where appropriate.

Notification decisions shall be based upon:

- Applicable legal requirements;
- Severity of the incident;
- Risk of harm;
- Nature of affected information.

The Company shall seek to provide notifications within a reasonable timeframe after becoming aware of a notifiable incident.

12.10 CONTENT OF NOTIFICATIONS

Where notification is required, the Company shall seek to provide information including:

- Description of the incident;

- Categories of information affected;
- Potential consequences;
- Steps already taken;
- Recommended actions for affected individuals;
- Contact details for further assistance.

Notification content may be adapted based upon the circumstances of the incident.

12.11 THIRD-PARTY INCIDENTS

Where incidents involve third-party operators, cloud providers, payment processors, AI providers, or other service providers, the Company shall seek to:

- Engage with the affected provider;
- Obtain relevant information;
- Assess risks;
- Determine notification requirements;
- Implement corrective measures.

The Company remains accountable for managing risks associated with third-party processing activities.

12.12 AI-RELATED INCIDENTS

AI-related incidents may include:

- Exposure of personal information;
- Inappropriate outputs;
- Biased outputs;
- Security vulnerabilities;
- Prompt injection attacks;
- Data leakage;
- Unauthorised access to AI systems.

Such incidents shall be investigated in accordance with this Framework and may require additional technical assessment.

12.13 EVIDENCE PRESERVATION

Where appropriate, the Company shall preserve relevant evidence relating to incidents.

Evidence may include:

- System logs;
- Communications;
- Screenshots;
- Audit records;
- Security alerts;
- Incident reports.

Evidence preservation supports:

- Investigations;
- Regulatory compliance;
- Legal proceedings;
- Root cause analysis.

12.14 CORRECTIVE ACTIONS

Following investigation, the Company may implement corrective actions including:

- Access control improvements;
- Policy updates;
- Security enhancements;
- Additional training;
- Vendor reviews;
- Technology changes;
- Process improvements.

Corrective actions shall seek to reduce the likelihood of recurrence.

12.15 INCIDENT RECORDS

The Company shall maintain records relating to incidents including:

- Date of occurrence;
- Nature of the incident;
- Information affected;
- Investigation findings;
- Actions taken;
- Notifications issued;
- Lessons learned.

Such records may be retained in accordance with the Company's retention requirements.

12.16 POST-INCIDENT REVIEW

Following significant incidents, the Company shall conduct a review to assess:

- Root causes;
- Effectiveness of the response;
- Areas for improvement;
- Additional controls required;
- Lessons learned.

The purpose of such reviews is to strengthen future resilience and improve governance.

12.17 CONTINUOUS IMPROVEMENT

The Company recognises that threat landscapes continue to evolve.

Accordingly, incident management procedures shall be reviewed periodically to ensure continued effectiveness and alignment with:

- POPIA;
- Information security best practices;
- Regulatory expectations;
- Industry developments;
- Business requirements.

The Company shall seek to continuously improve its ability to prevent, detect, respond to, and recover from privacy and security incidents.

13. TRAINING, AWARENESS AND ACCOUNTABILITY

13.1 Purpose

The purpose of this section is to establish the Company's approach to privacy awareness, information security awareness, accountability, and ongoing compliance education.

The Company recognises that compliance with POPIA is not solely dependent upon policies and technology but also upon the conduct, awareness, and accountability of individuals who process personal information.

13.2 GENERAL RESPONSIBILITIES

All employees, contractors, consultants, service providers, and authorised users who process information on behalf of the Company shall:

- Comply with this Framework;
- Protect personal information;
- Protect confidential information;
- Follow security requirements;
- Report suspected incidents;
- Cooperate with investigations;
- Respect privacy rights;
- Use information only for authorised purposes.

13.3 PRIVACY AWARENESS

The Company shall promote awareness regarding:

- POPIA requirements;
- Privacy obligations;
- Confidentiality requirements;
- Data subject rights;
- Information handling practices;
- Incident reporting procedures;
- AI governance requirements.

Awareness activities may be conducted through training sessions, written guidance, policy reviews, onboarding programmes, or other appropriate methods.

13.4 SECURITY AWARENESS

The Company shall promote awareness regarding:

- Password security;
- Multi-factor authentication;
- Phishing attacks;
- Social engineering risks;
- Secure information handling;
- Device security;
- Remote working practices;
- AI-related risks.

13.5 CONFIDENTIALITY OBLIGATIONS

Individuals with access to confidential information shall be expected to:

- Maintain confidentiality;
- Avoid unauthorised disclosures;
- Protect sensitive information;
- Comply with contractual obligations;
- Follow approved security procedures.

Confidentiality obligations may continue after termination of employment, engagement, or contractual relationships.

13.6 CONTRACTOR AND SERVICE PROVIDER AWARENESS

Where appropriate, contractors and service providers may be required to:

- Review applicable policies;
- Comply with privacy obligations;
- Comply with information security requirements;
- Maintain confidentiality;
- Report incidents promptly.

13.7 ACCOUNTABILITY

Each individual who processes personal information shall remain accountable for their actions and decisions relating to such information.

Failure to comply with applicable requirements may result in corrective action as provided for in this Framework.

13.8 REVIEW OF AWARENESS PROGRAMMES

The Company shall periodically review awareness initiatives to ensure that they remain relevant, effective, and aligned with evolving legal, operational, and technological requirements.

14. MONITORING, AUDITING AND COMPLIANCE REVIEWS

14.1 Purpose

The purpose of this section is to establish the monitoring, auditing, review, and assessment activities necessary to support ongoing compliance with POPIA and this Framework.

14.2 CONTINUOUS MONITORING

The Company shall seek to monitor:

- Information processing activities;
- Security controls;
- Access management practices;
- Data retention practices;
- Third-party operator relationships;
- AI governance activities;
- Privacy risks.

Monitoring activities shall be proportionate to the Company's size, operations, and risk profile.

14.3 COMPLIANCE REVIEWS

The Company shall conduct periodic compliance reviews to assess:

- Compliance with POPIA;
- Compliance with this Framework;
- Compliance with related policies;
- Effectiveness of controls;
- Emerging risks.

Reviews shall be conducted at least annually or more frequently where circumstances require.

14.4 RISK ASSESSMENTS

The Company shall periodically assess privacy and information security risks.

Risk assessments may consider:

- Operational risks;
- Technology risks;
- Third-party risks;
- AI-related risks;
- Regulatory risks;
- Reputational risks.

14.5 THIRD-PARTY REVIEWS

The Company shall periodically review key service providers and operators to assess:

- Privacy commitments;
- Security controls;
- Service performance;
- Regulatory developments;
- Risk exposure.

14.6 AI GOVERNANCE REVIEWS

The Company shall periodically review:

- AI-enabled services;
- AI-related risks;
- User feedback;
- AI governance controls;
- Regulatory developments affecting AI.

The purpose of such reviews is to promote responsible AI use and ongoing compliance.

14.7 CORRECTIVE ACTIONS

Where deficiencies are identified, the Company may implement:

- Process improvements;
- Policy updates;
- Additional controls;
- Training initiatives;
- Technical safeguards;
- Vendor management actions.

14.8 REPORTING

The Information Officer shall maintain appropriate records relating to:

- Compliance reviews;
- Risk assessments;
- Monitoring activities;
- Corrective actions;
- Significant findings.

Such records may be retained for governance and compliance purposes.

15. NON-COMPLIANCE, ENFORCEMENT AND DISCIPLINARY MEASURES

15.1 Purpose

The purpose of this section is to establish the Company's approach to addressing violations of this Framework, privacy obligations, information security requirements, and applicable legal obligations.

15.2 NON-COMPLIANCE

Non-compliance may include:

- Unauthorised access to information;
- Unauthorised disclosure of information;
- Failure to follow approved procedures;
- Failure to report incidents;
- Misuse of personal information;
- Breaches of confidentiality;
- Unauthorised use of AI systems;
- Failure to comply with security requirements.

15.3 INVESTIGATION OF BREACHES

The Company may investigate alleged breaches of:

- POPIA;
- This Framework;
- Related policies;
- Confidentiality obligations;
- Security requirements.

Investigations shall be conducted fairly and proportionately.

15.4 CORRECTIVE ACTION

Depending upon the circumstances, corrective action may include:

- Additional training;
- Coaching and guidance;
- Process improvements;
- Access restrictions;
- Policy reviews;
- Contractual remedies;
- Disciplinary action where applicable.

15.5 CONTRACTORS AND THIRD PARTIES

Contractors, consultants, and service providers who fail to comply with applicable obligations may be subject to:

- Remedial requirements;
- Contractual enforcement measures;
- Suspension of access;
- Termination of engagements where appropriate.

15.6 REPORTING OF SUSPECTED VIOLATIONS

Individuals are encouraged to report suspected violations promptly.

Reports shall be treated seriously and investigated appropriately.

15.7 FAIRNESS

The Company shall seek to ensure that enforcement activities are:

- Fair;
- Reasonable;
- Consistent;
- Proportionate;
- Legally compliant.

15.8 CONTINUOUS IMPROVEMENT

Lessons learned from compliance failures shall be utilised to improve governance, security, awareness, and operational controls.

16. REVIEW, APPROVAL AND DOCUMENT CONTROL

16.1 Purpose

The purpose of this section is to establish the governance arrangements relating to the maintenance, approval, review, and control of this Framework.

16.2 DOCUMENT OWNERSHIP

This Framework is owned by VAYU Coaching Technologies (Pty) Ltd.

The Information Officer shall be responsible for:

- Maintaining the Framework;
- Coordinating reviews;
- Managing updates;
- Monitoring implementation;
- Promoting compliance.

16.3 REVIEW FREQUENCY

This Framework shall be reviewed:

- At least annually; or
- Following significant legislative changes; or
- Following significant operational changes; or
- Following significant security incidents; or
- Following significant changes to AI-enabled services.

16.4 VERSION CONTROL

The Company shall maintain appropriate version control records including:

- Version number;
- Effective date;
- Review date;
- Summary of material amendments;
- Approval records.

16.5 DOCUMENT CONTROL REGISTER

Item	Details
Document Title	POPIA Compliance Framework
Document Owner	VAYU Coaching Technologies (Pty) Ltd
Responsible Officer	Information Officer
Current Version	1.0
Effective Date	_____
Review Date	_____
Classification	Internal Governance Document

16.6 APPROVAL

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

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

Approval

I hereby approve and adopt this POPIA Compliance Framework on behalf of VAYU Coaching Technologies (Pty) Ltd.

Signature:

Name:

Chris Roos

Date:

Version:

1.0

16.7 CONTINUED IMPROVEMENT

The Company recognises that privacy, information security, technology, artificial intelligence, and regulatory requirements continue to evolve.

Accordingly, this Framework shall be treated as a living governance document and shall be reviewed and updated as necessary to maintain ongoing compliance, operational effectiveness, and responsible business practices.