

THE CHIRANDU GROUP

www.chirandu.com

PRIVACY NOTICE

Version: 1.0 **Effective Date:** 9 June 2026 **Classification:** Public

Responsible Party (POPIA): The Chirandu Group (Pty) Ltd

Registered address: Johannesburg, Republic of South Africa

The Chirandu Group is a South African-headquartered institution. We are accordingly subject to the Protection of Personal Information Act 4 of 2013 ("POPIA") as our primary data protection framework, with supplementary obligations arising under the laws of jurisdictions in which we operate or from which we receive personal information.

This Privacy Notice describes how The Chirandu Group (Pty) Ltd and its subsidiaries (collectively, "the Group", "we", "us", or "our") collect, use, retain, disclose, and protect personal information in connection with www.chirandu.com and associated digital services, products, and communications (the "Digital Properties"), and in the course of our commercial, research, and institutional relationships.

We are committed to processing personal information lawfully, fairly, and transparently, and to respecting the dignity and privacy of every person whose information we hold. This Notice is reviewed at least annually and whenever material changes to our processing activities occur.

1. Who We Are: Responsible Party and Group Structure

The Responsible Party for the purposes of POPIA, and the Data Controller for the purposes of the GDPR and UK GDPR in respect of processing activities described in this Notice, is:

The Chirandu Group (Pty) Ltd, trading as The Chirandu Group

Registration number: [to be inserted] **Registered office:** Johannesburg, Republic of South Africa

The Group comprises the following operating entities, each of which may act as a responsible party or operator (as defined in POPIA) in respect of specific processing activities:

- **Chirandu Botanica (Pty) Ltd** -- Research, development, and applied botanical science
- **Chirandu Institute (Pty) Ltd** -- Strategic intelligence and advisory services
- **Chirandu AI (Pty) Ltd** -- MBEU platform and technology development
- **Chirandu Capital (Pty) Ltd** -- Capital and corporate finance (currently dormant)

Where a subsidiary entity acts as a separate responsible party in respect of a specific processing activity, you will be informed of its identity and contact details at the point of collection. Intra-group data sharing is governed by binding intra-group agreements that impose obligations equivalent to those under POPIA.

Information Officer (POPIA s.55): The Group has designated a duly registered Information Officer as required under POPIA.

Email: kudzai@moyochiranduholdings.com

Website: www.chirandu.com

2. Applicable Legal Framework

Our processing of personal information is governed primarily by POPIA, which establishes the conditions for the lawful processing of personal information in South Africa. In addition, because we engage with commercial partners, research collaborators, and website visitors located in other jurisdictions, supplementary obligations arise as follows:

- **European Union and EEA:** Where we process personal information of individuals located in the EU or EEA, the EU General Data Protection Regulation (Regulation (EU) 2016/679, "GDPR") applies as a supplementary framework to the extent that our processing falls within its territorial scope (Article 3 GDPR).
- **United Kingdom:** Where we process personal information of individuals located in the United Kingdom, the UK GDPR and Data Protection Act 2018 apply on an equivalent basis.
- **Zimbabwe:** Processing activities involving personal information of individuals located in Zimbabwe are subject to the Cyber and Data Protection Act [Chapter 12:07] (2021) and Regulations issued thereunder.
- **Other jurisdictions:** We monitor applicable data protection requirements in jurisdictions with which we have material commercial engagement and apply the standards of the most protective applicable law where those standards exceed the baseline established by POPIA.

The conditions for lawful processing under POPIA (section 11) serve as the baseline for all processing activities. Where the GDPR, UK GDPR, or other applicable law imposes more stringent requirements in respect of a specific data subject or processing activity, those requirements are applied in addition to and not in substitution for POPIA compliance.

Jurisdiction-specific supplements to this Notice are available on request for data subjects located in the EU/EEA, UK, Zimbabwe.

3. Personal Information We Collect

We collect only the personal information that is adequate, relevant, and not excessive in relation to the purposes for which it is collected or subsequently processed, in accordance with the minimality condition under section 10 of POPIA (and the equivalent data minimisation principle under the GDPR).

3.1 Information You Provide Directly

- Identity and professional data: full name, job title, professional designation, company or institutional affiliation, and business registration details
- Contact data: business email address, telephone number, postal address, and other contact information provided in the course of enquiry or engagement
- Communication and correspondence data: the content of messages, proposals, enquiries, and responses exchanged with the Group through any channel
- Commercial and transactional data: information provided in connection with partnership applications, licensing enquiries, collaboration proposals, or commercial negotiations, including regulatory compliance documentation and counterparty identification materials
- Event and engagement data: information provided in connection with attendance at Group-hosted or co-hosted events, industry forums, or presentations

3.2 Information Collected Automatically

- Technical data: IP address, browser type and version, operating system, device identifiers, and network metadata
- Usage data: pages visited, time on page, navigation paths, referral source, and clickstream behaviour
- Cookie and tracking data: information collected through cookies and analogous technologies as further described in Section 9 of this Notice

3.3 Information Obtained from Third Parties

- Referral data: contact and background information provided by third parties who refer you to the Group, where you have consented to such referral or the referring party has a lawful basis for disclosure
- Publicly available professional data: information from public registers, professional directories, or published materials, where relevant to a commercial or research engagement
- Due diligence data: information obtained from credit reference agencies, regulatory compliance screening tools, or public enforcement databases in the course of counterparty qualification, where the Group has a legitimate interest or legal obligation to conduct such checks

We do not seek to collect special personal information (as defined in section 26 of POPIA, including information concerning health, race, ethnicity, religious beliefs, or biometric data) through our Digital Properties or in the ordinary course of our institutional activities. Should any specific engagement require the processing of special personal information, a separate, express consent will be sought and a supplementary notice provided.

4. Lawful Grounds for Processing and Purposes

Section 11 of POPIA requires that personal information be processed on at least one of the following grounds: (a) consent of the data subject; (b) necessity for the performance of a contract; (c) compliance with a legal obligation; (d) protection of the legitimate interests of the data subject; (e) necessity for the performance of a public law duty; or (f) pursuit of the legitimate interests of the responsible party or a third party. The Group relies on grounds (a), (b), (c), and (f) in the context of its processing activities, as set out in the register below.

Where the GDPR applies, the corresponding lawful bases under Article 6 GDPR are identified alongside each processing purpose.

Purpose: Responding to and managing commercial enquiries, partnership proposals, collaboration requests, and licensing discussions

Lawful basis: *POPIA s.11(1)(b): necessary for the performance of a contract or pre-contractual steps. GDPR Art. 6(1)(b).*

Purpose: Conducting counterparty qualification, commercial due diligence, and intellectual property risk assessment, including evaluation under the Group's formal intake protocol

Lawful basis: *POPIA s.11(1)(f): pursuit of the legitimate interests of the responsible party. GDPR Art. 6(1)(f). Legitimate interest: protection of proprietary botanical intelligence assets and assessment of counterparty suitability prior to disclosure.*

Purpose: Administering existing commercial, licensing, and research agreements, including compliance with obligations arising under the Nagoya Protocol, the National Environmental Management: Biodiversity Act (NEMBA), and applicable Access and Benefit-Sharing frameworks

Lawful basis: *POPIA s.11(1)(b): necessary for the performance of a contract. POPIA s.11(1)(c): compliance with a legal obligation. GDPR Art. 6(1)(b) and 6(1)(c).*

Purpose: Sending institutional communications, research publications, and commercial correspondence relevant to an established relationship with the Group

Lawful basis: *POPIA s.11(1)(f): pursuit of the legitimate interests of the responsible party (developing and maintaining commercial relationships). GDPR Art. 6(1)(f). For direct marketing communications, consent (POPIA s.11(1)(a); GDPR Art. 6(1)(a)) where required.*

Purpose: Operating, maintaining, securing, and improving the Digital Properties and associated technology infrastructure

Lawful basis: *POPIA s.11(1)(f): pursuit of the legitimate interests of the responsible party. GDPR Art. 6(1)(f). Legitimate interest: provision of a secure and functional online presence.*

Purpose: Complying with applicable legal and regulatory obligations, including record-keeping, regulatory reporting, enforcement of contractual rights, and responding to lawful governmental or regulatory requests

Lawful basis: *POPIA s.11(1)(c): compliance with a legal obligation. GDPR Art. 6(1)(c).*

Purpose: Conducting internal analytics and business intelligence to support the Group's strategic development and institutional mission

Lawful basis: *POPIA s. 11(1)(f): pursuit of the legitimate interests of the responsible party. GDPR Art. 6(1)(f). Data used in aggregated or pseudonymised form where feasible.*

Where processing is based on consent, you may withdraw that consent at any time by contacting the Information Officer. Withdrawal does not affect the lawfulness of processing carried out prior to withdrawal, nor does it affect processing conducted on other lawful grounds.

Where the Group relies on its legitimate interests as a ground for processing, a legitimate interests assessment has been conducted. Copies are available on written request to the Information Officer.

5. Disclosure of Personal Information

The Group does not sell, rent, or otherwise make personal information available to third parties for their own commercial purposes. Disclosure to third parties occurs only in the circumstances and subject to the safeguards described below.

5.1 Operators (Service Providers)

We engage operators (as defined in POPIA section 1) to perform functions on our behalf, including IT infrastructure and hosting, document management, legal, financial, and tax advisory services, and communications platforms. Operators process personal information solely on the Group's instructions under written operator agreements that impose obligations at least equivalent to those under POPIA, including confidentiality and security requirements.

5.2 Professional Advisors

Personal information may be disclosed to legal counsel, auditors, accountants, and other professional advisors engaged by the Group to the extent necessary for the provision of their services. Such parties are subject to professional confidentiality obligations and, where applicable, statutory secrecy obligations.

5.3 Commercial Counterparties

In the course of negotiating or performing commercial agreements, limited personal information (such as contact details and professional credentials of relevant representatives) may be disclosed to counterparties on a strictly need-to-know basis. Such disclosures are subject to appropriate confidentiality obligations. The Group's counterparty qualification protocol governs the conditions and sequencing of any such disclosure.

5.4 Regulatory and Governmental Authorities

Personal information may be disclosed to the Information Regulator of South Africa, other competent supervisory authorities, courts, arbitral tribunals, law enforcement agencies, or governmental bodies where required or permitted by applicable law, including in response to binding legal process or to establish, exercise, or defend legal claims.

5.5 Corporate Transactions

In the event of a merger, acquisition, restructuring, or disposal of all or a material part of the Group's assets or business, personal information may be disclosed to relevant counterparties and their advisors under binding confidentiality arrangements. Affected data subjects will be notified if the transaction results in a material change to the basis or manner of processing.

6. Cross-Border Transfers of Personal Information

Section 72 of POPIA prohibits the transfer of personal information about a data subject to a third party in a foreign country unless the recipient is subject to a law, binding corporate rules, or a binding agreement that provides an adequate level of protection substantially equivalent to the conditions for the lawful processing of personal information as set out in POPIA.

The Group operates across multiple jurisdictions including South Africa, Zimbabwe, and engages service providers and advisors located in various countries. Where personal information is transferred outside South Africa, we ensure that one or more of the following safeguards is in place prior to transfer:

- The recipient jurisdiction has been determined to provide an adequate level of protection by the Information Regulator or under applicable South African law
- A binding agreement is in place between the Group and the recipient that incorporates data protection obligations substantially equivalent to POPIA, including the conditions for lawful processing, security obligations, and data subject rights
- Where the GDPR or UK GDPR applies to the transfer, Standard Contractual Clauses approved by the European Commission or the UK Information Commissioner (as applicable) are incorporated into the relevant agreement
- The transfer falls within a permissible derogation under section 72(1) of POPIA or an equivalent provision under applicable law, such as necessity for the performance of a contract at the data subject's request

Data subjects who wish to receive further information regarding the safeguards applicable to a specific cross-border transfer, or to obtain a copy of the relevant transfer mechanism, may submit a written request to the Information Officer.

7. Retention and Destruction of Personal Information

The Group retains personal information only for as long as is necessary to fulfil the purposes for which it was collected, or for such longer period as is required by applicable law, including the record-keeping requirements of the Companies Act 71 of 2008, the Prescription Act 68 of 1969, and applicable tax and regulatory instruments. Retention periods are reviewed periodically and adjusted to reflect changes in law, regulatory guidance, or operational requirements.

The following indicative retention periods apply:

- **Commercial, contractual, and licensing records:** 7 (seven) years from the end of the relevant commercial relationship, in accordance with statutory limitation periods.
- **Pre-contractual correspondence and enquiry records:** 3 (three) years from the date of last substantive engagement, unless a commercial relationship is subsequently established.
- **Compliance, due diligence, and counterparty qualification records:** As required by applicable law and the Group's counterparty risk management framework, which may extend to 10 (ten) years in regulated contexts.
- **Access and Benefit-Sharing and Nagoya Protocol records:** As required by applicable biodiversity and benefit-sharing legislation, which may impose extended mandatory retention obligations.
- **Website analytics and technical log data:** Up to 26 (twenty-six) months in aggregated or pseudonymised form, following which data is deleted or further anonymised.
- **Direct marketing and communications records:** Until withdrawal of consent or exercise of the right to object, or until the relationship to which the communications relate has concluded, whichever is earlier.

At the expiry of the applicable retention period, personal information is securely deleted, anonymised, or physically destroyed in a manner that prevents reconstruction. Operators and third-party processors are required to apply equivalent destruction standards under their contractual obligations to the Group. Certificates of destruction are obtained where appropriate.

8. Rights of Data Subjects

POPIA confers the following rights on data subjects in respect of personal information held by a responsible party. Equivalent or additional rights arise under the GDPR and UK GDPR for data subjects located in the EU/EEA and United Kingdom respectively. We are committed to facilitating the exercise of these rights promptly and without obstruction.

8.1 Right of Access (POPIA s.23; GDPR Art. 15)

You have the right to request confirmation of whether the Group holds personal information about you, and if so, to receive a copy of that information together with details of the purposes of processing, the categories of information held, recipients to whom it has been disclosed, the applicable retention period, and the source of the information where it was not collected directly from you.

8.2 Right to Correction or Deletion (POPIA s.24; GDPR Arts. 16, 17)

You have the right to request that we correct personal information that is inaccurate, misleading, or out of date, and that we delete personal information that is no longer necessary for the purposes for which it was collected, that has been unlawfully obtained, or in respect of which continued retention is not authorised by applicable law. The right to deletion is subject to statutory exceptions, including where retention is required for the establishment, exercise, or defence of legal claims.

8.3 Right to Object (POPIA s.11(3); GDPR Art. 21)

You have the right to object at any time to the processing of your personal information on grounds relating to your particular situation, where the processing is based on legitimate interests. We will comply with such an objection unless we are able to demonstrate compelling legitimate grounds that override your interests, rights, and freedoms, or that the processing is necessary for the exercise or defence of legal claims. You have an absolute right to object to processing for direct marketing purposes, and we will cease such processing immediately on receipt of your objection.

8.4 Right to Restriction of Processing (GDPR Art. 18)

Where the GDPR applies, you have the right to request that we restrict processing of your personal information in certain circumstances, including while the accuracy of the information is contested, where processing is unlawful and you prefer restriction to deletion, or while your objection is being assessed.

8.5 Right to Data Portability (GDPR Art. 20)

Where the GDPR applies and processing is based on consent or contractual necessity and carried out by automated means, you have the right to receive your personal information in a structured, commonly used, and machine-readable format and to transmit it to another controller.

8.6 Rights in Relation to Automated Decision-Making

The Group does not currently subject data subjects to decisions based solely on automated processing that produce legal or similarly significant effects. Should we introduce such processing, we will update this Notice accordingly and implement the safeguards required by applicable law.

8.7 Right to Withdraw Consent

Where processing is based on your consent, you may withdraw it at any time by contacting the Information Officer. Withdrawal does not affect the lawfulness of processing prior to withdrawal.

8.8 Right to Lodge a Complaint

You have the right to lodge a complaint with the relevant supervisory or regulatory authority if you believe that the Group has processed your personal information in a manner that does not comply with applicable law. The relevant authorities are:

- **South Africa:** Information Regulator (South Africa) | www.justice.gov.za/inforeg | inforeg@justice.gov.za
- **EU / EEA:** The data protection authority in your member state of habitual residence, place of work, or location of the alleged infringement
- **United Kingdom:** Information Commissioner's Office (ICO) | www.ico.org.uk
- **Zimbabwe:** Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)

We welcome the opportunity to resolve concerns directly before you approach a supervisory authority. Please contact the Information Officer in the first instance.

To exercise any of the rights described above, please submit a written request to the Information Officer using the contact details in Section 11. We may verify your identity before processing your request. We aim to respond within 30 days of receipt, extendable by a further 30 days where the complexity or volume of requests warrants it, with notice to you.

9. Cookies and Tracking Technologies

The Digital Properties use cookies and analogous technologies (including pixel tags, web beacons, and session tracking tools) to support functionality, security, and improvement of our online presence. We deploy the following categories:

- **Strictly necessary cookies:** Essential to the operation of the Digital Properties and to maintaining session security. These cannot be disabled without impairing core functionality.
- **Functional cookies:** Enable enhanced features such as language preferences and region-specific content. Disabling these may impair certain non-essential features.
- **Analytics and performance cookies:** Collect anonymised or pseudonymised data regarding visitor interaction with our Digital Properties to enable performance measurement and improvement. Where analytics tools are used, IP anonymisation is applied prior to processing.
- **Communications and targeting cookies:** Where deployed, these enable measurement of the effectiveness of Group communications. Such cookies are only activated with your prior consent, obtained through the cookie consent interface on your first visit.

You may manage your cookie preferences at any time through the cookie settings tool accessible in the footer of our Digital Properties, or by configuring your browser settings. A full Cookie Policy, including the names, durations, and providers of all deployed cookies, is available at www.chirandu.com/cookies.

10. Security of Personal Information

The Group implements appropriate technical and organisational measures to safeguard personal information against loss, damage, unauthorised access, unlawful processing, and any other form of compromise, as required by section 19 of POPIA. These measures are commensurate with the nature, sensitivity, and volume of personal information processed and the risks associated with its processing, and include:

- Role-based access controls ensuring personal information is accessible only to personnel with a documented operational need
- Encryption of personal information in transit using TLS 1.2 or higher, and at rest where technically feasible and proportionate to the risk
- Network and infrastructure security controls, including firewalls and periodic vulnerability assessments of systems that process personal information
- Contractual security obligations imposed on all operators, requiring standards at least equivalent to the Group's own, with periodic compliance oversight
- Staff awareness measures, including procedural controls to ensure personnel who handle personal information understand their obligations under POPIA and Group policy

- Documented incident response procedures for detecting, assessing, containing, and reporting security compromises involving personal information

In the event of a security compromise involving personal information, the Group will notify the Information Regulator and affected data subjects as required under section 22 of POPIA and equivalent provisions of applicable law, including within 72 hours under the GDPR where applicable. Notification will include the nature of the compromise, the categories of personal information affected, the remedial measures taken or proposed, and the contact details of the Information Officer.

No security programme can guarantee absolute protection against all threats. You are encouraged to use trusted networks when accessing the Digital Properties and to notify the Information Officer promptly if you become aware of any suspected unauthorised access to personal information held by the Group.

11. Contact Details and Submission of Requests

All data subject rights requests, privacy enquiries, objections, and complaints should be directed to the Group's Information Officer:

Information Officer, The Chirandu Group

Email: kudzai@moyochiranduholdings.com

Website: www.chirandu.com

Postal address: Johannesburg, Republic of South Africa

Requests submitted by email will receive an acknowledgement within 3 (three) business days. We will endeavour to resolve all requests within 30 (thirty) days of receipt, subject to any extensions permitted by applicable law. We may request reasonable evidence of identity before processing a data subject rights request in order to prevent unauthorised disclosure.

The Group maintains a register of data subject requests in compliance with its accountability obligations under section 8 of POPIA.

12. Amendments to This Notice

The Group reserves the right to amend this Notice at any time to reflect changes in applicable law, regulatory guidance, technological developments, or its processing activities. The version number and effective date at the head of this Notice will be updated with each revision.

Where changes are material (meaning they substantively alter your rights or the manner in which we process your personal information), advance notice will be provided through a prominent announcement on the Digital Properties and, where we hold your contact information, by direct communication no fewer than 10 (ten) business days prior to the change taking effect.

Non-material amendments (including typographical corrections, clarifications, and administrative updates) will be published without advance notice. Your continued use of the Digital Properties following publication of an updated Notice constitutes acknowledgement of the revised terms. Prior versions of this Notice are available on request from the Information Officer.

13. Governing Law and Jurisdiction

This Notice is governed by and construed in accordance with the laws of the Republic of South Africa, with POPIA as the primary applicable data protection instrument. Nothing in this Notice limits or restricts the rights of data subjects under the law of any other jurisdiction in which they are located,

nor does it preclude any data subject from seeking relief before a competent supervisory authority or court in their jurisdiction of residence.

Disputes arising from this Notice that cannot be resolved through the Group's internal complaints process are subject to the jurisdiction of the courts of the Republic of South Africa, without prejudice to any data subject's right to approach the Information Regulator or a competent supervisory authority in their own jurisdiction.

This Notice does not constitute legal advice and does not create any contractual rights or obligations beyond those expressly stated herein.

Indigenous by origin. Global by design.

The Chirandu Group | Johannesburg, South Africa | www.chirandu.com
Version 1.0 | Effective 9 June 2026 | Governed by the laws of the Republic of South Africa