1. Introduction

The African Genomic Archive for Response & Insight (AGARI) is committed to the lawful processing of personal information in accordance with the Protection of Personal Information Act, 2013 (POPIA) of South Africa. Given our principle-based approach to governance, we also seek to be broadly compliant with similar and equivalent data protection laws like the EU General Data Protection Regulations, and others of relevance to regional data governance. This Privacy Policy explains how we collect, use, store, and protect your personal information when you use the AGARI platform.

2. Acceptance

By accepting our Policy, you are deemed to have read, understood, accepted, and agreed to be bound by all of its terms.

3. Information We Collect

We collect the following personal information:

- Name and contact information (email address)
- Organisation affiliation and role
- Account credentials (securely encrypted)
- Profile information (optional biography)

We collect the following information about how you use the platform, including:

- Login times and session duration
- Data access and download activities (for audit purposes)
- Platform interactions and feature usage.

4. Your Data Obligations

You may only send, input or upload your own personal information or other data where you are lawfully authorised to do so, which includes warranting as far as reasonably possible for the authenticity and accuracy of the data being provided. We generally do not accept or process the personal information of children when a data subject user is below the age of 18 (eighteen). If you have mistakenly uploaded or shared any data described above, please alert the system administrator immediately.

5. How We Use Your Information

We use your personal information for the following purposes:

- To provide and maintain the AGARI platform services
- To authenticate your identity and manage your account
- To communicate with you about your account and platform updates
- To enforce access controls and sharing policies
- To maintain audit logs for security and compliance purposes, and to maintain broader system security
- To complete necessary business functions like internal auditing, planning and reporting
- To comply with legal obligations and regulatory requirements

6. Lawful Basis for Processing

We process your personal information based on the following legal grounds:

- Consent: You have provided explicit consent for account creation and data processing through the user registration process
- Contractual necessity: Processing is necessary to provide the platform services you have requested or fulfil other relevant contractual obligations
- Legal obligation: We must comply with applicable laws and regulations
- Legitimate interests: Processing is necessary for a vital or legitimate interest of you or the responsible party (asserting a legitimate interest will always be determined balanced against data subject rights)

7. Data Sharing and Disclosure

We do not sell your personal information or exchange or share your data for commercial purposes. We may share your information:

- Within your organisation: Organisation administrators can view member information for management purposes
- Within our organisation: Other entities, arms or organisations within or related to our organisation may have data shared with them for the purposes of fulfilling a legitimate interest
- With your consent: When you explicitly authorise sharing
- Legal requirements: When required by law, court order, or regulatory authority
- Service providers: With trusted third-party service providers and affiliates who assist in platform operations, for the purposes of fulfilling our obligations to you among other purposes.

We will ensure all sharing is lawful, and supported by robust security, and is contractually protected.

8. Data Security

We implement appropriate technical, security and organisational measures to protect your personal information, including but not limited to:

- Encryption of data in transit and at rest
- Access controls and authentication mechanisms
- Regular security audits and vulnerability assessments
- Secure server environment
- Staff training on data protection and privacy
- Incident response and disaster recovery procedures

We will also ensure that all of our employees, third party service providers, divisions and partners (including their employees and third-party service providers) having access to your personal information are bound by appropriate and legally binding confidentiality obligations and process your personal information at standards equal to or higher than our own.

9. Your Data Rights

You have the following rights regarding your personal information *inter alia*:

- Right of access: Request a copy of the personal information we hold about you
- Right to correct and/or delete: Request the correction, destruction or deletion of your personal information if the personal information is inaccurate; irrelevant; excessive; out of date; incomplete; obtained unlawfully; or that we are no longer authorised to retain

- Right to object: Object, on reasonable grounds relating to your particular situation to the processing of your personal information
- Right to object to marketing: Object at any time to the processing of your personal information for purposes of direct marketing;
- Right to withdraw consent: Withdraw consent for processing where consent is the legal basis for processing.

10. Data Retention and Accuracy

We only retain your personal information for as long as necessary to fulfil the purposes outlined in this policy, unless a longer retention period is required or permitted by law or you have consented to a longer retention period.

We will try to keep the personal information we collect as accurate, complete and up to date as is necessary for the purposes defined in this policy. From time to time we may request you to update your personal information on the website. Please note that in order to better protect you and safeguard your personal information, we may take steps to verify your identity before granting you access to your account or making any corrections to your personal information.

11. International Data Transfers

AGARI operates primarily within South Africa. If data is transferred outside of South Africa, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- We will only transfer your personal information to countries that have been deemed to provide an adequate level of protection for personal information
- Standard contractual clauses approved by relevant data protection authorities will be used to advance protection

12. Changes to This Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in our practices or legal requirements. We will notify you of significant changes via email or platform notification. The "Last updated" date at the top of this policy indicates when it was last revised.

13. Contacts and Complaints

If you wish to enact any of your data rights as outlined in this Policy, or have any questions in relation to this Policy, please contact the system administrator who will refer you to the appropriate contact.

You have the right to make a complaint at any time to the South African data regulator's office (Information Regulator's Office of South Africa), and the relevant data protection authority to your data processing. We would, however, appreciate the chance to deal with your concerns before you approach any such relevant regulator, so please contact us in the first instance.