Data Policy

Date Approved	24 June 2026		Version Number	24062026

Purpose and Context

This Data Policy explains how AbacusBio collects, uses, processes, stores, protects, and retains client data in connection with the provision of consulting and SaaS services.

The Client acknowledges and agrees that this Data Policy (available at abacusbio.com/data-policy/ and as updated from time to time) forms part of their Agreement with AbacusBio and governs the processing of Client data.

For the purposes of this policy, "AbacusBio" means AbacusBio Limited and its related entities, including AbacusBio International Limited (UK), AbacusBio Pty Limited (Australia), and AbacusBio Canada Limited, together forming the AbacusBio Group. The Client's engagement will be with a specific AbacusBio Group entity as identified in their Proposal or Agreement; however, the Client acknowledges and agrees that, in delivering the Services, Client data may be accessed and processed by authorised personnel across the AbacusBio Group, including personnel located in different jurisdictions, in accordance with this Data Policy.

Scope

This policy applies to all data processed by AbacusBio in connection with client engagements, including:

- Client-provided data
- Data generated through the delivery of services (including analytics and modelling outputs)
- Personal data relating to client personnel (e.g. name, email address, job title)
- Data processed through AbacusBio platforms (including SaaS solutions such as DTreo)

Roles and Responsibilities

3.1 Controller and Processor Roles

Depending on the nature of the engagement:

- The Client will typically act as **Data Controller**, and AbacusBio will act as **Data Processor** when processing data on the Client's behalf
- AbacusBio may act as an independent **Data Controller** where it determines the purposes and means of processing (e.g. use of proprietary datasets, benchmarking, internal analytics)

3.2 Client Responsibilities

The Client is responsible for:

- Ensuring that data provided to AbacusBio is collected lawfully
- Obtaining any necessary consents or authorisations
- Ensuring compliance with applicable data protection laws

Types of Data Processed

4.1 Personal Data

AbacusBio typically processes limited personal data relating to business contacts, including:

- Name
- Email address
- Job title
- Organisation

AbacusBio does not intentionally collect sensitive personal data unless expressly agreed.

4.2 Scientific, Operational and Proprietary Data

AbacusBio may process:

- Genetic, genomic, phenotypic and environmental data
- Farm, production and operational data
- Analytical outputs, modelling results, and derived datasets

Basis for Processing

AbacusBio processes data in accordance with globally recognised data protection principles, including:

- Contractual necessity
- Legitimate business interests (balanced against individual rights)
- Legal and regulatory obligations
- Consent (where required)
- Scientific and research purposes aligned with ethical standards

Data Use

AbacusBio uses client data solely for the purposes of:

- Delivering agreed services and outputs
- Performing analytics, modelling and reporting
- Operating and supporting platforms and tools
- Improving internal methodologies, tools and services
- Complying with legal and regulatory obligations

Data will not be used for purposes incompatible with the original purpose without appropriate authorisation.

Artificial Intelligence (AI)

7.1 Use of AI

AbacusBio may use artificial intelligence tools to support the delivery of services, including:

- Drafting and summarising content

- Supporting data analysis and modelling
- Assisting with coding and technical workflows

AI is used to support and enhance human expertise, not replace it.

7.2 AI Controls

AbacusBio applies strict governance to AI use:

- Only approved, enterprise-grade AI tools are used
- AI tools must be licensed, secure, and provisioned through AbacusBio
- All outputs are subject to human review before use

7.3 Use of Client Data in AI

- Client data is not entered into public or external AI tools unless explicitly authorised
- Personal, confidential, or proprietary data is treated as restricted
- AI tools are not used to train external models using client data

Data Sharing and Third Parties

AbacusBio may share data with:

- Group entities within AbacusBio
- Approved subcontractors and consultants
- Cloud service providers and software platforms

All third parties are subject to:

- Confidentiality obligations
- Data protection and security requirements
- Risk-based due diligence and ongoing oversight

AbacusBio does not sell client data.

Client-Directed Data Collection (Surveys and Stakeholder Engagement)

Where AbacusBio undertakes surveys, stakeholder engagement, or similar data collection activities on behalf of the Client (including through approved third-party tools):

- The Client is responsible for ensuring that all individuals (including stakeholders, participants, or respondents) are provided with appropriate privacy notices that comply with applicable data protection laws
- The Client is responsible for obtaining all necessary consents, permissions, and authorisations required to enable AbacusBio to collect, use, process, and store such data (including any personal data or personally identifiable information)
- The Client must ensure that such consents and notices are sufficient to cover the use of third-party tools and any cross-border data transfers that may occur as part of the Services

- AbacusBio will process such data solely in accordance with the Client's instructions and the Agreement, and will not be responsible for the content, adequacy, or legal compliance of any privacy notices or consent mechanisms implemented by the Client.

Data Storage and International Transfers

Cloud Infrastructure

AbacusBio operates a cloud-first model. Client Data is stored with trusted, enterprise-grade cloud and backup providers in secure, off-premise environments. Our primary hosting and backup locations are in Australia and the United States.

AbacusBio maintains an internal register of the cloud platforms and sub-processors used to deliver its services, including their hosting locations, and can provide relevant details to clients on request.

International Transfers

Due to AbacusBio's global operations, data may be accessed or transferred across jurisdictions.

AbacusBio ensures that appropriate safeguards are implemented, including:

- Contractual protections
- Transfers to jurisdictions with adequate protection where applicable
- Risk-based assessments of international transfers

Information Security

AbacusBio maintains a comprehensive Information Security Management framework designed to protect data confidentiality, integrity, and availability.

Key controls include:

- Role-based access control and least-privilege access
- Multi-factor authentication
- Encryption of data at rest and in transit
- Secure cloud infrastructure and network controls
- Endpoint security and device management
- Vulnerability management and patching
- Security monitoring and event logging
- Staff training and awareness

AbacusBio is working towards ISO/IEC 27001 and works with external cybersecurity advisors to continuously improve its security posture.

Data Retention and Deletion

Retention

Data is retained only for as long as necessary, including for:

- Duration of the engagement
- Delivery of services
- Legal, regulatory, or audit requirements

- Legitimate business purposes

Deletion

When data is no longer required, it is securely deleted or destroyed in accordance with its nature and sensitivity.

Clients may request return or deletion of data in accordance with contractual arrangements.

Individual Rights

Where applicable, AbacusBio supports the rights of individuals to:

- Access their personal data
- Request correction
- Request deletion
- Restrict or object to processing
- Request data portability

Requests will be handled in accordance with applicable laws.

Data Breach Management

AbacusBio maintains formal incident response procedures.

In the event of a data breach:

- The incident is investigated and contained
- Affected clients are notified where required
- Regulatory obligations are met
- Corrective actions are implemented

Contact and Governance

AbacusBio maintains internal governance structures for data protection, AI use, and cybersecurity.

Clients may contact AbacusBio regarding:

- Data protection enquiries
- Data access or deletion requests
- Security or AI use questions

The Data Protection Officer for AbacusBio is the Chief Operating Officer, Hannah Farr, who can be contacted at hfarr@abacusbio.com.

Policy Updates

This policy may be updated from time to time to reflect:

- Changes in law or regulation
- Changes in technology or services
- Improvements in internal practices

The most current version will apply.