Privacy Policy

Genetic Signatures Limited

ACN 095 913 205

1. Introduction

1.1. This Privacy Policy (the "**Policy**") outlines the commitment of Genetic Signatures Limited and its subsidiaries (collectively referred to as the "**Company**") to safeguarding the privacy of individuals whose Personal Information we collect, including our shareholders, employees, research partners, suppliers, contractors, and other stakeholders.

1.2. As a Company focused on the development and commercialisation of proprietary platform technology, the Company recognises the sensitivity of the information we handle we are committed to managing all Personal Information with the highest standards of confidentiality and integrity.

1.3. This Policy details how the Company collects, holds, uses, discloses, manages, protects, and otherwise handles your Personal Information in compliance with the **Australian Privacy Principles** under the **Privacy Act 1988 (Cth**) (as amended by the Privacy and Other Legislation Amendment Act 2024)**,** the **General Data Protection Regulation (EU) 2016/679** ("**GDPR**") applicable to individuals located in the European Economic Area ("**EEA**"), as well as relevant US privacy and data protection requirements.

2. Application

2.1. This Policy applies to all Personal Information collected by the Company, including:

(a) Employees, contractors, shareholders, and suppliers

(b) Research partners;

(c) Collaborators in clinical trials, observational studies, and commercial partnerships;

(d) Visitors to the Company's websites, digital platforms, and premises; and

(e) Individuals from the EEA in accordance with the GDPR, and individuals in the United States, in compliance with applicable US privacy laws and regulations.

2.2. Unless expressly stated otherwise, this Policy is binding across all entities controlled by or affiliated with the Company.

3. Definition of Personal Information

3.1. Personal Information is information or an opinion about you from which you can be reasonably identified:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not.

3.2. Personal Information is information that identifies you or could reasonably identify an individual, whether directly or indirectly, such as name, contact details, and records of dealings with the Company.

3.3. Sensitive information is a subset of Personal Information afforded additional protection. It includes health and genetic information, biometric data, racial or ethnic origin, religious beliefs, sexual orientation, criminal records, and membership of political, professional, or trade associations.

3.4. For the purposes of this Policy, references to Personal Information include Sensitive Information, unless specified otherwise.

4. Purpose of Collecting Personal Information

4.1. The Company collects Personal Information to:

(a) Develop, conduct, and commercialise the Company's technologies and products;

(b) Manage regulatory compliance obligations in Australia (including ASX listing rules), the United States, and the [[A under GDPR;

(c) Conduct clinical trials and research in collaboration with research partners;

(d) Communicate with investors, shareholders, suppliers, customers, and research collaborators;

(e) Administer employment, recruitment, workforce safety, payroll, and training;

(f) Facilitate website optimisation, product development, and business analytics;

(g) Comply with contractual, statutory, and regulatory requirements in all jurisdictions in which the Company operates**.**

4.2. The Company collects and processes Personal Information only where it is necessary, and we will inform individuals of the specific purpose at the time of collection, or as soon as practicable thereafter.

4.3. For job applicants, we may collect Personal Information from resumes, references, criminal background checks (with consent), publicly available professional profiles, pre-employment screening tests, and other employment-related information.

5. Types of Personal Information Collected

The categories of Personal Information collected may include**:**

5.1. **General Information**

(a) Full name, date of birth, gender;

(b) Residential address, email, and phone numbers;

(c) Identification details (passport, driver's licence, national ID);

(d) Tax file number (TFN) or equivalent in relevant jurisdictions;

(e) Financial information (e.g., banking details).

5.2. **Clinical Trial & Research Information**

(a) Health, genetic, and biomarker data collected during trials;

(b) Informed consent records;

(c) Research collaborator details.

5.3. **Technical and Website Data**

(a) IP addresses, device identifiers, and browsing history on the website.

(b) Cookies and analytics data for site optimisation.

5.4. Sensitive Information will only be collected where necessary, and where required explicit consent will be obtained in compliance with applicable privacy laws, including the Australian Privacy Act, GDPR, and relevant US regulations.

6. Personal Information Collection Method

6.1. The Company collects Personal Information directly from you, where practicable, through:

(a) Direct interactions (email, telephone, in-person meetings, forms);

(b) Participation in clinical trials;

(c) Recruitment processes;

(d) Website usage and digital platform engagement.

6.2. We may also collect Personal Information from third parties, including:

(a) Service providers (e.g., share registries, background check agencies);

(b) Research institutions or healthcare providers;

(c) Publicly available sources.

6.3. Information collected from third parties will be handled in accordance with this Policy and relevant legal frameworks.

6.4. For website visitors, data is collected via cookies, web beacons, and analytics tools. Cookies can be managed or disabled via browser settings. Cookie data linked to identifiable individuals will be treated as Personal Information.

6.5. Unsolicited Personal Information received will be assessed. If unnecessary, it will be de-identified or destroyed in accordance with our data handling procedures as detailed at section 7.3 below.

7. Storage and Security of Personal Information

7.1. The security of your personal information is of paramount importance to the Company and it takes reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification, or disclosure.

7.2. The Company implements robust security measures to safeguard Personal Information, including:

(a) Secure password-protected systems;

(b) Encryption protocols;

(c) Firewalls and intrusion detection systems;

(d) Physical security for hard copy records;

(e) Employee training on data handling and confidentiality.

7.3. Personal Information is retained only as long as necessary for operational, legal, or regulatory purposes. When no longer required, data is securely destroyed or anonymised.

8. Use and Disclosure of Personal Information

8.1. Personal Information will be used or disclosed solely for the purpose for which it was collected, unless:

(a) It is directly related to the primary purpose and within your reasonable expectations;

(b) Required for legal proceedings, fraud prevention, or regulatory compliance;

(c) Consent has been obtained;

(d) Required by applicable law or regulation in Australia, the US, or the EEA.

8.2. Disclosure may occur to:

(a) Regulatory bodies (e.g., ASX, ASIC, FDA, EMA);

(b) External advisors and service providers (e.g., IT, payroll, legal counsel);

(c) Research collaborators and clinical trial sites;

(d) Law enforcement or government agencies, where legally required.

8.3. Personal Information of individuals in the EEA will be processed in accordance with GDPR, including data minimisation, transparency, and the lawful basis for processing.

8.4. The Company does not engage in direct marketing without explicit consent. You may withdraw consent at any time by contacting us via the contact details below.

---

9. Cross-border Data Transfers

9.1. The Company may transfer Personal Information to recipients located outside Australia, including jurisdictions such as the United States and countries within the European Economic Area (EEA). Such transfers will only occur where:

(a) The recipient jurisdiction has laws that provide substantially similar protection to the Australian Privacy Act, or;

(b) The Company has implemented appropriate contractual safeguards, such as Standard Contractual Clauses (SCCs) under the GDPR, binding corporate rules, or other legally valid mechanisms to ensure adequate protection of your Personal Information.

9.2. The Company will also implement technical and organisational measures—including encryption, secure transmission protocols, and strict access controls—to protect Personal Information during and after any cross-border transfer, in compliance with Australian privacy laws, GDPR, and applicable U.S. privacy legislation.

---

10. Access, Correction and Further Information

10.1. You have the right to request access to your Personal Information held by the Company. Upon receiving a request, and subject to permitted exceptions under the Privacy Act or other applicable privacy laws (including GDPR and U.S. laws), the Company will provide access within a reasonable timeframe.

10.2. You also have the right to request the correction, updating, or deletion of your Personal Information if you believe it is inaccurate, incomplete, or outdated. The Company will take reasonable steps to promptly correct or update your information, or notify you if we are legally unable to do so.

10.3. If you have concerns about the Company's handling of your Personal Information, or if you believe that your privacy rights under this Policy have been breached, you may lodge a complaint by contacting the Company at the details provided below. Complaints will be treated seriously, handled confidentially, and investigated promptly.

10.4. If you are dissatisfied with the Company's response to your complaint, or if your complaint remains unresolved, you may escalate the matter to an external dispute resolution body or contact the Office of the Australian Information Commissioner (OAIC) at www.oaic.gov.au. Individuals located in the EEA may also contact their local data protection authority, while U.S. residents may lodge complaints with the relevant regulatory authority in their state.

11. Contact Information

11.1. All correspondence should be directed to the Company Secretary on:

Tel: +61 3 9692 7222

Email: michael.sapountzis@vistra.com

Mail: C/- Company Secretary – Genetic Signatures Limited
Level 11, Suite 2, 385 Bourke Street, Melbourne VIC 2000.

12. Notifiable Data Breach Protocol

12.1. The Company complies with the Office of the Australian Information Commissioner's (**OAIC**) Notifiable Data Breaches (**NDB**) scheme, as well as applicable data breach notification requirements under GDPR and relevant U.S. privacy laws. We are committed to ensuring transparency and accountability in the event of a data breach.

12.2. In the event of an actual or suspected data breach involving personal or sensitive information, the Company will promptly initiate a data breach response plan. This includes:

(a) Immediate containment and remediation to prevent further exposure.

(b) A risk assessment to evaluate the likelihood of serious harm to affected individuals.

(c) A forensic investigation to determine the cause and scope of the breach.

(d) Implementation of mitigation strategies to limit any potential impact.

12.3. If the breach is determined to meet the threshold for notification under applicable laws, we will:

(a) Promptly notify affected individuals, clearly outlining the nature of the breach, the types of information involved, the likely consequences, and recommended steps for individuals to protect themselves.

(b) Report the breach to the OAIC, and where relevant, other regulatory authorities (such as EU Supervisory Authorities under GDPR, or state regulators in the U.S.), in accordance with legal and regulatory obligations.

12.4. The Company's approach prioritises cybersecurity resilience, data protection, and continuous improvement. Following any breach, we will conduct a post-incident review to identify root causes, strengthen security controls, and implement corrective measures to safeguard against future incidents.

13. Policy Review and Amendments

13.1. This Policy cannot be amended without approval from the Company's Board

13.2. This Policy will be reviewed by our Board **every two years** or as often as may be required, to ensure it remains effective and meets the best practice standard and the needs of the Company.

13.3. This Policy will be available on the Company's website within a reasonable time after any such updates or amendments have been approved.