ARAVANIS

Privacy Policy

Aravanis Insolvency Pty Ltd trading as Aravanis

Version 2.0 | 1 September 2026

Privacy commitment Aravanis manages personal information openly, lawfully and securely, with particular care for the sensitive financial and personal information obtained during insolvency administrations.

Entity	Aravanis Insolvency Pty Ltd trading as Aravanis
Document owner	Director
Privacy Officer	Andrew Aravanis
Privacy contact	Email : andrew@aravanis.com.au Tel: (02) 8985 5155
Website	www.aravanis.com.au
Approval status	Approved
Review	At least annually and on material legal, regulatory, technology or business change

Contents

1. Purpose and status
2. Scope and application
3. Privacy framework
4. Definitions
5. Kinds of personal information
6. How Aravanis collects information
7. Why information is collected, held, used and disclosed
8. Collection notices, anonymity and unsolicited information
9. Disclosure recipients and insolvency functions
10. Government identifiers and tax file numbers
11. Overseas access and disclosure
12. Information quality, security and retention
13. Data breaches
14. Access and correction
15. Privacy complaints
16. Websites, communications and direct marketing
17. Automated decision-making and artificial intelligence
18. Employee records and recruitment
19. Governance and responsibilities
20. Review, publication and related documents

Appendix A - APP compliance matrix
Appendix B - Privacy incident response checklist

1. Purpose and status

This Policy explains how Aravanis Insolvency Pty Ltd trading as Aravanis (Aravanis) manages personal information. Aravanis is committed to the Privacy Act 1988 (Cth), the Australian Privacy Principles (APPs), the Notifiable Data Breaches scheme and other applicable confidentiality, tax, employment, insolvency and records obligations.

The Policy supports open and transparent privacy management. It is intended to be made available free of charge in an appropriate form. It does not limit statutory powers or duties of a Registered Trustee or other officeholder, and it does not create a right to withhold information where production, use, disclosure or publication is required or authorised by law, court order or an administration duty.

2. Scope and application

This Policy applies to personal information handled by Aravanis in corporate operations, personal insolvency administrations, advisory engagements, recruitment and employment, stakeholder communications, websites, digital systems and dealings with regulators, courts, service providers and professional advisers. Each formal appointment may involve a separate legal capacity, purpose and record set.

3. Privacy framework

- Privacy Act 1988 (Cth) and the 13 Australian Privacy Principles
- Part IIIC of the Privacy Act, the Notifiable Data Breaches scheme
- Tax File Number Rule 2015 and taxation secrecy requirements where applicable
- Bankruptcy Act 1966, Bankruptcy Regulations 2021, Insolvency Practice Schedule (Bankruptcy) and Insolvency Practice Rules (Bankruptcy)
- Corporations Act 2001, Insolvency Practice Schedule (Corporations) and applicable regulations and rules
- court orders, warrants, statutory notices, registration conditions and professional obligations
- AFSA Inspector-General guidance and directions applicable to personal insolvency practitioners
- applicable employment, surveillance, anti-money laundering, cyber security and records laws

4. Definitions

Term	Meaning
Administration	A formal or informal personal insolvency or advisory engagement.
APP entity	An agency or organisation covered by the Privacy Act for the relevant act or practice.
Personal information	Information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information or opinion is true or not and whether it is recorded in a material form or not.
Sensitive information	Personal information of a kind given additional protection by the Privacy Act, including health, racial or ethnic origin, political, religious, professional or trade-association membership, sexual orientation or practices, criminal record, genetic or biometric information.
Registered Practitioner	A Registered Trustee or other externally appointed officeholder.
Privacy incident	Loss, unauthorised access, disclosure, alteration, misuse or interference involving personal information.
Eligible data breach	A breach meeting the statutory requirements in Part IIIC of the Privacy Act.

5. Kinds of personal information

Depending on the insolvency appointment and legal authority, Aravanis may collect and hold:

- identity and contact details, former names, date and place of birth, signatures, photographs and identity documents
- tax file numbers, Australian Business Numbers, government identifiers and registration details where lawfully required
- financial information, bank accounts, income, expenses, assets, liabilities, transactions, taxation, superannuation and insurance information
- employment, business, directorship, shareholding, trust, partnership, related-party and professional information
- claims, proofs of debt, creditor and debtor information, contracts, security interests, litigation and dispute information
- family, dependant, relationship and household information relevant to statutory duties or claims
- health, disability, hardship, criminal allegation or conviction, professional membership and other sensitive information where lawful and necessary
- communications, interview notes, complaints, recordings, affidavits, reports, evidence and investigation material
- device, account, access, log, security, website and communication metadata
- staff, applicant, contractor, referrer, supplier, professional adviser and stakeholder information
- information contained in books and records taken into possession or control, including information concerning customers, employees and third parties

6. How Aravanis collects information

Aravanis collects information in the following manner:

- directly from the individual, including forms, interviews, telephone calls, meetings, email, portals and correspondence
- from bankrupts, debtors, directors, officers, employees, creditors, claimants, relatives, representatives and counterparties
- from accountants, lawyers, financial advisers, lenders, insurers, valuers, agents and other service providers
- from AFSA, ASIC, the ATO, courts, tribunals, police, regulators and other government agencies
- through statutory notices, examinations, warrants, searches, investigations, litigation and compulsory production powers
- from public registers, insolvency registers, land and company searches, social media, websites and other public sources
- from books, records, devices, systems, premises and data controlled by an Administration
- automatically through websites, security systems, logs, cookies and approved business technology

7. Why information is collected, held, used and disclosed

Aravanis will generally use or disclose personal information for the primary purpose of an insolvency administrations, a related secondary purpose an individual would reasonably expect, with consent, or where required or authorised by law or another APP exception assessing, investigating, administering and finalising appointments and engagements.

- identifying, securing, realising and distributing assets and investigating affairs and transactions
- adjudicating claims, convening meetings, reporting to creditors and paying dividends or distributions
- exercising statutory powers, complying with duties and responding to courts, regulators and lawful notices
- detecting, investigating, preventing and reporting fraud, offences, misconduct, conflicts, threats and security incidents
- communicating with stakeholders and verifying identity, authority and entitlement
- obtaining legal, accounting, valuation, technology, insurance, recovery, sale and other professional services
- managing staff, contractors, recruitment, training, workplace safety, payroll and benefits
- operating, securing, auditing and improving systems, premises, websites and services
- meeting insurance, risk, governance, taxation, AML/CTF, records and professional obligations

- establishing, exercising or defending legal or equitable claims and preserving privilege

.

8. Collection notices, anonymity and unsolicited information

8.1 Collection and notification

At or before collection, or as soon as practicable afterwards, Aravanis will take reasonable steps to notify the individual of relevant APP 5 matters, including identity and contact details, circumstances of collection, legal authority or consequences if information is not provided, purposes, usual recipients, access and correction, complaints and likely overseas disclosures.

8.2 Anonymity and pseudonymity

Where practicable and lawful, individuals may interact anonymously or using a pseudonym. This option may not be available where Aravanis is required or authorised by law to deal with an identified individual, or where identification is impracticable for the relevant function, claim, appointment or security requirement.

8.3 Unsolicited information

If Aravanis receives unsolicited personal information, it will determine whether the information could lawfully have been collected. If not, and if lawful and reasonable, Aravanis will destroy or de-identify it. Records subject to statutory retention, legal hold, privilege, court process or administration duties will not be destroyed merely because they were unsolicited.

9. Disclosure recipients and insolvency functions

Subject to authority, need and confidentiality, recipients may include:

- creditors, debtors, bankrupts, directors, officers, employees, claimants and their representatives
- AFSA, the Inspector-General in Bankruptcy, ASIC, the ATO, AUSTRAC, police, courts, tribunals and other regulators or government bodies
- banks, secured creditors, insurers, brokers, auctioneers, agents, valuers, investigators, debt collectors and asset-recovery providers
- lawyers, accountants, tax advisers, experts, auditors, reviewers and professional bodies
- technology, cloud, communications, storage, cyber security, e-signature, printing, mailing and records providers
- purchasers or prospective purchasers of assets or businesses, subject to lawful data minimisation, confidentiality and sale arrangements
- related bodies, subcontractors and administrative service providers supporting Aravanis

Statutory reports, notices, meeting materials, court documents, registers and public insolvency records may include personal information where required or authorised. Aravanis will avoid unnecessary inclusion and apply lawful redaction or access restrictions where appropriate.

10. Government identifiers and tax file numbers

Aravanis will not adopt a government-related identifier as its own identifier except where permitted. Government identifiers and tax file numbers will be collected, used, disclosed, stored and destroyed only as authorised by law. Access will be restricted, and tax file numbers will not be used to establish identity where that is prohibited.

11. Overseas access and disclosure

Aravanis may use service providers whose personnel, support functions or systems are located outside Australia. Current locations must be verified against the vendor register and contracts, and the countries in which overseas recipients are likely to be located will be identified where practicable.

Before disclosing personal information overseas, Aravanis will take reasonable steps required by APP 8 to ensure the recipient does not breach the APPs. Depending on the arrangement, Aravanis may remain accountable for an overseas recipient's acts or practices. Controls may include due diligence, data-location review, contractual privacy and security terms, access limits, encryption, incident notification, audit rights and exit arrangements.

12. Information quality, security and retention

12.1 Quality

Aravanis will take reasonable steps to ensure personal information it collects, uses and discloses is accurate, up to date, complete and relevant, having regard to the purpose. Allegations, estimates, disputed claims and third-party statements will be identified appropriately rather than represented as established fact.

12.2 Security

Aravanis keeps personal information in a third-party CRM platform with industry benchmarks for encryption, authentication and other data storage and security protocols. Staff are also trained and reminded of their obligations with regard to personal information and limit access to personal information by requiring the use of passwords and in certain circumstances, two-factor authentication

- governance, documented responsibilities, privacy-by-design and periodic risk assessment
- role-based access, least privilege, authentication, logging and privileged-access controls
- approved systems, encryption, secure transfer, protected backups and recovery testing
- physical security, clean-desk controls, secure printing, transport and disposal
- supplier due diligence, contractual controls, access review and incident obligations
- staff training, confidentiality obligations, phishing and social-engineering controls
- prompt reporting, containment, investigation, remediation and lessons learned

12.3 Retention and destruction

Personal information will be retained for the period required by insolvency legislation, court orders, taxation, employment, insurance, limitation, professional, contractual and records obligations. When no longer required for a permitted purpose, and no legal hold or statutory reason applies, Aravanis will take reasonable steps to destroy or de-identify it. Administration records will

follow the applicable retention schedule. The retention schedule, not this public Policy, should contain verified record classes and periods.

13. Data breaches

A suspected privacy or security incident must be reported immediately through the approved incident channel. Aravanis will contain the incident, preserve evidence, assess affected information and individuals, evaluate serious harm, remediate where possible and document decisions.

Where Aravanis has reasonable grounds to suspect an eligible data breach, it will conduct a reasonable and expeditious assessment and take all reasonable steps to complete it within the statutory assessment period. If an eligible data breach is established, Aravanis will prepare the required statement, notify the Australian Information Commissioner and notify affected individuals as soon as practicable, subject to statutory exceptions. Other regulators, courts, insurers, clients or appointment stakeholders may also require notification.

14. Access and correction

An individual may request access to, or correction of, personal information Aravanis holds by contacting the Privacy Officer. Aravanis may verify identity and authority, consult relevant officeholders and respond within the periods required by law. Access may be refused or limited where an APP exception or another law applies, including where access would unreasonably affect another person's privacy, reveal commercially sensitive evaluative information, prejudice an investigation, relate to legal proceedings, reveal intentions in negotiations, be unlawful, or compromise privilege or confidentiality.

If access or correction is refused, Aravanis will generally give written reasons and available complaint mechanisms, unless unreasonable or unlawful. If corrected information was previously disclosed, Aravanis will take reasonable steps to notify relevant recipients where required and requested.

15. Privacy complaints

Aravanis take complaints about privacy very seriously.

1. Contact the Privacy Officer using the details on the cover page and provide the relevant matter, information, dates, people and outcome sought.
2. Aravanis will acknowledge, assess and investigate the complaint, maintain confidentiality and manage conflicts. The complainant may be asked for further information or authority.
3. Aravanis will keep you updated on the progress of the investigations.
4. Aravanis will provide a written outcome within a reasonable period, subject to complexity, legal restrictions and external processes.

If dissatisfied, an individual may complain to the Office of the Australian Information Commissioner. Complaints about the conduct or decisions of a Registered Trustee may also have separate AFSA, statutory review, court or professional pathways. AFSA does not replace the OAIC for Privacy Act complaints, and the OAIC does not determine the merits of an insolvency administration decision.

16. Websites, communications and direct marketing

Aravanis websites and systems may collect technical information such as IP address, browser, device, pages visited, cookies and security logs. Website notices will describe material analytics and cookie practices. Third-party websites are governed by their own policies.

Aravanis will only use personal information for direct marketing where permitted by APP 7 and other applicable laws. Marketing communications will identify Aravanis and provide a simple means to opt out. Information obtained under statutory powers or from an Administration will not be repurposed for marketing without lawful authority.

17. Automated decision-making and artificial intelligence

Aravanis may use approved technology to assist document review, search, triage, transcription, fraud detection, workflow, risk analysis or drafting. Workers remain responsible for professional judgement, verification, confidentiality and statutory decisions. Personal information must not be entered into unapproved public artificial-intelligence services.

18. Employee records and recruitment

Aravanis handles applicant, employee, contractor and former-worker information for recruitment, engagement, payroll, benefits, performance, training, security, WHS, insurance, investigations and legal obligations. The employee-records exemption may apply to some acts or practices directly related to a current or former employment relationship and an employee record, but Aravanis will still apply appropriate confidentiality, security, access control and fair-handling standards.

19. Governance and responsibilities

Aravanis Director will be responsible for the governance of this Policy:

- the Director oversees material privacy risk, incidents and remediation
- the Director ensures appropriate resources, accountability and escalation
- the Privacy Officer administers this Policy, complaints, access and correction, privacy impact assessments and data-breach coordination
- Registered Practitioners ensure appointment-specific authority, confidentiality, records, reporting and stakeholder controls
- system and information owners maintain access, security, retention and vendor controls
- all workers collect the minimum necessary information, use approved systems, verify recipients and report incidents immediately

20. Review, publication and related documents

This Policy will be reviewed at least annually and earlier following a material legal, regulatory, technology, vendor, data-flow or business change, a serious incident, audit finding, complaint trend or identified control weakness. The public version will be freely available, normally on the Aravanis website, and available in an appropriate alternative form on request.