

ARM HOLDING

PRIVACY POLICY

Website: <https://armholding.org>

Effective date: 30 July 2026

Last updated: 30 July 2026

Website operator: ARM Holding AU

1. Purpose and Scope

This Privacy Policy (the “Policy”) describes the personal data ARM collects, obtains, uses, discloses, stores and otherwise processes when individuals visit armholding.org, submit a corporate enquiry, request partnership or investor information, subscribe to communications, apply for a role, report a concern, or otherwise interact with the website or the controller identified below.

“Personal data” means information relating to an identified or identifiable individual and includes equivalent concepts such as personal information where applicable. “Processing” includes collecting, using, organising, storing, disclosing, transferring, analysing and deleting personal data.

The Website Terms of Use govern use of the website. The Cookies Policy provides detailed information about cookies and similar technologies. Service agreements govern products and transactions. Where a product-specific privacy notice conflicts with this Policy for that product, the more specific notice controls.

2. Who Is Responsible for Your Personal Data

The controller responsible for processing under this Policy is ARM Holding AU, an PTY LTD incorporated in Melbourne, Australia, registration number 26161065962, with registered office at Suite 2, Level 3, 480 Collins Street, Melbourne VIC 3000, Australia (“ARM”, “we”, “us” or “our”). Privacy enquiries may be sent to support@armholding.org.

This Policy forms part of the ARM privacy framework together with the Privacy Policy at <https://armholding.org/privacy-policy> and Website Terms of Use at <https://armholding.org/terms-of-use>.

An ARM affiliate or brand is not a controller merely by virtue of its appearance on the Website. Where personal data is shared within the ARM ecosystem, each recipient’s role as independent controller, joint controller or processor is identified in the relevant notice or agreement.

3. When This Policy Does Not Apply

This Policy does not govern a third-party website or a separately operated ARM-branded service that publishes its own privacy notice. It also does not govern personal data processed solely on behalf of an organisational customer where an ARM entity acts as processor; in that situation, the

customer controls the processing and its privacy notice applies, subject to the relevant data-processing agreement.

If your organisation provides access to an ARM service, direct privacy questions about your organisation's processing to that organisation. ARM will assist the controller as required by contract and law.

4. Personal Data We Collect

The data collected depends on how you interact with ARM. ARM collects only data that is necessary and proportionate for the stated purpose.

Category	Examples	Source
Identity and contact	Name, organisation, role, email, telephone, postal address and country	You; your organisation; authorised contacts
Enquiry and correspondence	Message content, partnership or investor interests, attachments, meeting requests and response history	You; correspondence participants
Newsletter and preferences	Email address, subscription status, topic choices, consent record and unsubscribe history	You; communications platform
Recruitment	CV, qualifications, employment history, portfolio, references, work-authorisation information and interview notes	You; referees; recruiters; public professional sources
Technical and usage	IP address, browser, device, operating system, timestamps, referring page, pages viewed, approximate location, identifiers and diagnostic/security events	Browser, device, hosting, security and analytics tools
Cookie and preference	Consent choices, theme/language settings and identifiers associated with cookies or similar technologies	Browser, consent platform and permitted vendors
Security and compliance	Reports, logs, suspected abuse, sanctions screening results and information required to establish or defend legal claims	You; systems; providers; authorities; public sources
Other submitted data	Feedback, event registration, press enquiry or other information voluntarily supplied	You or an authorised sender

The public Website does not request account credentials, payment-card data, private cryptographic keys, biometric identifiers, government identification, proof of address, health data or criminal-offence data through a general contact form. A feature that collects these data is governed by a specific notice, lawful basis, security controls, retention rule and, where required, a data-protection impact assessment.

5. Data We Receive from Other Sources

ARM may receive business contact data from your employer or organisation, event organisers, professional advisers, recruitment providers, service providers, publicly available professional profiles, corporate registries, sanctions lists and partners that lawfully refer an enquiry. ARM will respect source restrictions and provide any notice required when data was not obtained directly from you.

ARM does not purchase consumer profiles or combine Website data with data-broker records for advertising. Where such processing occurs, the relevant sources, categories, purposes, and opt-out rights are set out in <https://armholding.org/terms-of-use>.

6. Why We Use Personal Data and Our Legal Bases

Where a law requires a legal basis, ARM relies on the basis shown below. The applicable basis depends on the context and jurisdiction.

Purpose	Data typically used	Legal basis
Operate, deliver and secure the website	Technical, usage, security and preference data	Legitimate interests in operating and protecting the website; legal obligation where applicable; consent for non-essential technologies
Respond to enquiries and arrange discussions	Identity, contact, correspondence and organisation data	Steps requested before a contract; legitimate interests in business communications; consent where required
Evaluate partnerships, investors or corporate transactions	Contact, professional, correspondence and due-diligence data	Legitimate interests; pre-contract steps; legal obligations
Send newsletters and marketing	Contact, preferences, engagement and consent records	Consent where required; otherwise legitimate interests subject to objection and electronic-marketing law
Recruit and assess candidates	Identity, contact, recruitment and interview data	Pre-contract steps; legitimate interests; legal obligations.
Analyse and improve website performance	Usage, device, diagnostic and aggregated data	Consent where required for analytics; otherwise legitimate interests only where lawful and appropriately balanced
Prevent fraud, misuse and security incidents	Technical, security, correspondence and compliance data	Legitimate interests; legal obligations; establishment, exercise or defence of legal claims

Purpose	Data typically used	Legal basis
Comply with law and enforce rights	Relevant identity, correspondence, transaction and security data	Legal obligation; public interest where applicable; legitimate interests; legal claims

Where ARM relies on legitimate interests, it must document the purpose, necessity and balancing assessment. You may request information about the relevant assessment, subject to protection of confidential and third-party information.

Where processing relies on consent, you may withdraw consent at any time without affecting processing already carried out. Refusing optional data will not affect unrelated services. If data is required by law or to enter a contract, ARM will explain the consequence of not providing it.

7. Sensitive Personal Data

ARM does not intentionally collect sensitive or special-category data through the general website except where necessary, lawful and clearly disclosed. If you include such data in free text or an attachment when it is not requested, ARM may delete or restrict it.

Products involving identity verification, KYC, payments, custody, fraud prevention or regulated services may process government identifiers, financial information, biometric data, sanctions information or criminal-offence data. Those products require separate notices identifying the exact controller, categories, purposes, legal bases, recipients, retention, safeguards, rights and any automated decision-making.

8. Cookies, Analytics and Similar Technologies

ARM uses cookies, local storage and similar technologies for website operation, preferences, and security. The Cookies Policy at <https://armholding.org/cookies-policy> identifies the technologies, providers, purposes and durations and explains how to manage choices.

Where consent is required, ARM activates non-essential technologies only after consent and records or withdraws that choice in accordance with applicable law.

9. Marketing Communications

ARM may send corporate updates, event information or product news where permitted. Marketing messages will identify the sender and provide an unsubscribe method. You may opt out at any time by using the unsubscribe link or contacting support@armholding.org.

Opting out of marketing does not prevent service, security, legal or transactional communications. ARM retains a minimal suppression record to honour the opt-out.

10. How We Disclose Personal Data

ARM may disclose personal data only where necessary and lawful to:

- hosting, cloud, content-delivery, cybersecurity, analytics, consent-management, communications, recruitment, document-management and professional-service providers acting under contract;
- the ARM entity responsible for the enquiry or product, after its identity and role have been established and disclosed;
- professional advisers, auditors, insurers, banks and prospective transaction parties subject to appropriate confidentiality and due-diligence safeguards;
- courts, regulators, law-enforcement bodies and public authorities where disclosure is legally required or necessary to protect rights, safety and security; and
- a successor or purchaser in a merger, financing, reorganisation, insolvency, sale or transfer, subject to applicable notice and protection requirements.

ARM does not sell personal data or share it for cross-context behavioural advertising as defined by applicable United States state law.

11. Service Providers and Recipient Register

ARM discloses personal data to the following categories of recipients for the stated purposes. The identity and location of each provider are recorded in ARM's vendor register and disclosed below where required.

Recipient	Purpose	Location / Transfer
Website hosting provider	Website hosting, delivery and availability	Australia or other jurisdictions where the hosting infrastructure operates, subject to appropriate contractual and legal safeguards
Website security provider	Security, logging and abuse prevention	Australia or other jurisdictions where the provider operates, subject to appropriate contractual and legal safeguards
Google Analytics (Google LLC)	Website measurement where consented	United States and other countries where Google processes data, subject to Google's applicable international data transfer safeguards
Not Used	Enquiries and subscriptions	Not Applicable
Not Used	Recruitment and applications	Not Applicable

Recipient	Purpose	Location / Transfer
ARM Holding AU and its affiliated entities	Routing an enquiry to the responsible entity	Australia and other jurisdictions where the relevant ARM affiliate operates, acting as an independent controller or processor as applicable

12. International Transfers

Personal data may be processed outside your country when recipients or infrastructure are located elsewhere. ARM will make a restricted transfer only when a lawful mechanism and required safeguards are in place.

For transfers from the EEA, the United Kingdom, or Switzerland, safeguards may include an adequacy decision, approved Standard Contractual Clauses (SCCs), the UK International Data Transfer Agreement (IDTA) or International Data Transfer Addendum, or another legally recognised transfer mechanism, together with supplementary measures where required. Personal data may be transferred to jurisdictions in which ARM, its service providers, or affiliated entities operate, including Australia and other countries where website hosting, analytics, security, or support services are provided, subject to applicable data protection laws and appropriate safeguards.

You may request information about applicable safeguards by contacting support@armholding.org. ARM may redact confidential or third-party information.

13. Retention and Deletion

ARM retains personal data only for the periods below and longer only where a legal hold, statutory obligation or active dispute requires it. Data is deleted or anonymised when the applicable period ends.

Record	Retention period	Starting point
General enquiries	12 months	Closure of the enquiry
Partnership or investor enquiries	24 months	Last substantive contact or transaction end
Newsletter records	Until opt-out plus 24 months	Subscription or opt-out
Recruitment applications	12 months	Recruitment process closure
Security and access logs	12 months	Creation of the record
Cookie consent records	90 days	Consent choice or renewal

Record	Retention period	Starting point
Legal and compliance records	As required by applicable law or for seven (7) years, whichever is longer	Matter closure or statutory trigger

Backup copies are isolated from ordinary use and deleted after 90 days.

14. Security

ARM uses appropriate technical and organisational measures designed to protect personal data, taking account of processing risks. Measures must include, as appropriate, access control, least privilege, authentication, encryption in transit and at rest, secure development, logging, monitoring, vulnerability management, backups, incident response, provider due diligence, staff confidentiality and training.

No system is completely secure. If a personal data breach occurs, ARM will investigate, contain, document, and notify affected individuals or relevant authorities where required by applicable law. Report security concerns to support@armholding.org, not through a public form.

15. Your Privacy Rights

Depending on your location and the processing, you may have the right to:

- request access to and a copy of personal data;
- correct inaccurate or incomplete data;
- request deletion or restriction of processing;
- object to processing based on legitimate interests and object at any time to direct marketing;
- receive certain data in a structured, commonly used and machine-readable format and transmit it to another controller;
- withdraw consent at any time;
- not be subject to a decision based solely on automated processing that produces legal or similarly significant effects, where the right applies;
- appeal ARM's refusal of a request where applicable; and
- complain to a competent data-protection or privacy authority.

Rights are not absolute. ARM may refuse or limit a request where law permits and will explain the reason and available complaint or appeal route.

16. How to Exercise Your Rights

Submit a request through support@armholding.org or by post to Suite 2, Level 3, 480 Collins Street, Melbourne VIC 3000, Australia. Describe the privacy right you wish to exercise, the

relevant interaction, and your preferred response method. ARM will not require unnecessary personal data.

ARM may take proportionate steps to verify your identity and authority before processing a request. An authorised agent must provide written authorisation signed by the individual, together with evidence of the agent's identity and authority to act on the individual's behalf. ARM will respond within 30 days of receiving a verifiable request, unless a longer period is permitted by applicable law, in which case ARM will notify you of the extension and the reasons for it.

ARM will not discriminate against you for exercising a privacy right. A fee will be charged only where legally permitted, such as for a manifestly unfounded or excessive request.

17. Automated Decision-Making and Artificial Intelligence

The public website does not use automated decision-making or profiling that produces legal or similarly significant effects. ARM will not make a solely automated decision producing legal or similarly significant effects unless it has a lawful basis, provides the required information and safeguards, and offers human intervention, an opportunity to express a view, and a means to contest the decision where required.

ARM does not use Website enquiries, submissions, or user content to train or fine-tune AI models. Where personal data is used to develop or evaluate AI, the relevant privacy notice will specify the categories of data, purpose, legal basis, sources, retention, access, opt-out or objection rights, de-identification measures, and human oversight.

Product-specific AI features require separate, contextual disclosure of input processing, output review, model providers, data retention, training use, and material risks.

18. Children's Privacy

The website is not directed to children under 18 years of age. ARM does not knowingly collect children's personal data through the general website. If ARM learns that data was collected without required parental authorisation or another lawful basis, it will take appropriate steps to delete or restrict it.

Any product intended or likely to be accessed by children requires a separate age-appropriate design and privacy assessment, including age assurance, parental consent where required, default settings and child-friendly notices.

19. Australian and Regional Privacy Rights

19.1 Australian Privacy Framework

Where the Privacy Act 1988 (Cth) applies to ARM or the relevant processing, ARM handles personal information in accordance with that Act and the Australian Privacy Principles (APPs). This includes obligations concerning transparent management, collection, notice, use and disclosure, direct marketing, cross-border disclosure, security, access and correction.

19.2 Access and Correction in Australia

You may request access to personal information ARM holds about you and ask ARM to correct information that is inaccurate, out of date, incomplete, irrelevant or misleading. ARM will respond within the period required by law and will give written reasons and complaint information where access or correction is refused.

19.3 Direct Marketing

ARM uses personal information for direct marketing only where permitted by the Privacy Act 1988 (Cth), the Spam Act 2003 (Cth) and other applicable law. Every electronic marketing message provides the sender's identity and a functional unsubscribe method. ARM will action an unsubscribe request within the legally required period.

19.4 Overseas Disclosures

Before disclosing personal information to a recipient outside Australia, ARM takes the steps required by APP 8 and identifies the likely destination countries in section 12. Contractual or technical safeguards do not remove any accountability imposed by Australian privacy law.

19.5 Eligible Data Breaches

ARM maintains a data-breach response process. Where the Notifiable Data Breaches scheme applies and ARM has reasonable grounds to believe an eligible data breach has occurred, ARM will notify the Office of the Australian Information Commissioner and affected individuals in accordance with the Privacy Act 1988 (Cth).

19.6 Other Jurisdictions

Individuals outside Australia have the additional rights and complaint routes stated in "Not Applicable."

20. Regulatory and Law-Enforcement Requests

ARM may preserve or disclose personal data when required by valid law, legal process or a competent authority. ARM will review requests for legal validity, scope and proportionality, challenge inappropriate requests where reasonably available, and disclose only data reasonably required. ARM will notify the individual where permitted and appropriate.

21. Changes to This Policy

ARM may update this Policy when processing, technology, law, products or organisational arrangements change. The revised Policy will state its last-updated and effective dates. If a change materially affects individuals, ARM will provide additional notice or obtain consent where required.

22. Contact and Complaints

22.1 Contact ARM

Privacy questions, access or correction requests, and complaints may be submitted to support@armholding.org or by post to Suite 2, Level 3, 480 Collins Street, Melbourne VIC 3000, Australia. Data Protection Officer or Privacy Officer: Not Applicable.

22.2 Complaint Handling

ARM will acknowledge a privacy complaint, investigate it fairly, and provide a written outcome within 30 days of receiving the complaint, unless a longer period is permitted by applicable law. ARM may request information reasonably needed to investigate the complaint.

22.3 External Complaint

If you are not satisfied with ARM's response, or ARM does not respond within 30 days, you may lodge a complaint with the Office of the Australian Information Commissioner at <https://www.oaic.gov.au>. Where the complaint concerns a financial service, an approved external dispute resolution scheme such as the Australian Financial Complaints Authority may apply: Not Applicable.