Policy Document - Privacy and Data

Comprehensive Policy on Privacy, Data Integrity, and Compliance

Company: RME Solutions Technology

Effective Date: 21/02/2024

Introduction

At RME Solutions Technology, we are committed to upholding the highest standards of privacy, data protection, and business information integrity. As a managed services provider and consultancy serving businesses, educational institutions, and government entities, we recognise that trust, legal compliance, and the security of information are paramount for our stakeholders. This policy outlines our approach to safeguarding personal and business information, ensuring compliance with Australian and international standards, and maintaining the confidence of our clients, partners, and the wider community.

Scope

This Policy applies to all personal and business information that RME Solutions Technology collects, uses, discloses, stores, or otherwise handles in the course of its business activities. It covers information relating to clients, employees, contractors, suppliers, and visitors, and applies across all jurisdictions in which we operate. The policy addresses compliance with Australian Privacy Principles (APPs), the Privacy Act 1988, the General Data Protection Regulation (GDPR), PCI DSS, and other relevant global standards.

Definitions

- Personal Information: Any information or opinion about an identified individual, or an individual who is reasonably identifiable (e.g. names, addresses, emails, dates of birth, financial details).
- Business Information: Confidential or proprietary information relating to RME Solutions Technology or its clients, not limited to but including contracts, strategies, and commercial data.
- APPs: The Australian Privacy Principles, a set of 13 principles under the Privacy Act 1988 regulating the handling of personal information in Australia.

- GDPR: The General Data Protection Regulation, governing the protection of personal data of individuals in the European Union and European Economic Area.
- PCI DSS: Payment Card Industry Data Security Standard, a global standard for securing payment card information.
- Data Subject: The individual whose personal information is processed.
- Data Controller: The organisation determining the purposes and means of processing personal information.
- Data Processor: The organisation processing personal information on behalf of a data controller.
- Data Breach: Unauthorised access, disclosure, or loss of personal information likely to result in serious harm.
- DPO: Data Protection Officer, responsible for overseeing data protection strategy and compliance.
- Privacy Officer: Designated company representative handling privacy matters and compliance.

Unless otherwise defined, terms used in this policy have the meanings given in the relevant legislation or regulatory guidance.

Legal and Regulatory Compliance

Australian Privacy Principles (APPs) and Privacy Act 1988

RME Solutions Technology fully complies with the Privacy Act 1988 and the APPs, which regulate the entire lifecycle of personal information: from collection, use, and disclosure, to storage, security, access, and disposal. We implement procedures to ensure that all obligations under the APPs are met, including those relating to open management, consent, direct marketing, cross-border disclosure, and security.

General Data Protection Regulation (GDPR)

Where applicable, we comply with the GDPR, particularly when offering services to, or processing data of, individuals in the EU or EEA. Our privacy practices reflect GDPR principles such as lawfulness, fairness, transparency, data minimisation, purpose limitation, accuracy, storage limitation, integrity, confidentiality, and accountability.

PCI DSS and Payment Security

For online payments, we integrate with Stripe, adhering to PCI DSS requirements to protect cardholder data. Stripe's hosted fields and SDKs ensure payment information is

handled directly by PCI DSS–validated servers, minimising our compliance burden and enhancing user security. We maintain ongoing PCI compliance and review our protocols in line with transaction volume and regulatory changes.

Global Standards and Other Laws

We monitor and adapt to privacy laws in all jurisdictions where we operate, including but not limited to CCPA, PIPEDA, PDPA, and emerging legislation. Our policies are regularly reviewed to ensure ongoing alignment with global best practices.

Principles of Data Handling

- Lawfulness, Fairness, and Transparency: Data is processed lawfully, fairly, and in a transparent manner.
- Purpose Limitation: Information is collected for specified, explicit, and legitimate purposes only.
- Data Minimisation: Only information necessary for the stated purpose is collected and processed.
- Accuracy: Reasonable steps are taken to ensure information is accurate, up-to-date, and complete.
- Integrity and Confidentiality: Appropriate security measures are in place to protect data from misuse, interference, loss, unauthorised access, modification, or disclosure.
- Accountability: We demonstrate compliance through documentation, regular reviews, and cooperation with regulators.

These principles guide every aspect of our data handling, from system design to daily operations.

Roles and Responsibilities

- Privacy Officer: Oversees compliance with privacy legislation, responds to inquiries and complaints, and coordinates privacy training.
- Data Protection Officer (DPO): (where required) Advises on data protection obligations, monitors compliance, and serves as the contact point for authorities and data subjects.
- All Staff: Must follow this policy and participate in privacy and security training relevant to their roles.
- Third Parties: Contractors, vendors, and partners must adhere to equivalent privacy and security standards as outlined in our agreements.

Roles are clearly defined to ensure consistent, responsible data handling across all levels.

Data Protection by Design and Default

We embed privacy into our products, services, and processes from the outset, following the privacy by design and default approach. This includes conducting privacy impact assessments for new initiatives, minimising data collection, and ensuring privacy-friendly default settings.

Data Collection, Use, and Disclosure

- Consent: We obtain informed consent before collecting, using, or disclosing personal information, except where exceptions apply under law.
- Notification: Individuals are informed at or before collection about the purposes, legal basis, consequences of non-provision, and rights regarding their information.
- Direct Marketing: Personal information is not used for direct marketing unless permitted by law and consent is provided. Opt-out mechanisms are always available.
- Cross-Border Transfers: Data is only transferred overseas where appropriate protections exist or with explicit consent.
- Government Identifiers: Government-related identifiers (e.g. TFN, Medicare number) are not adopted or used except as required by law.

We ensure individuals remain informed and in control of their information throughout its lifecycle.

Data Retention and Disposal

- Retention: Personal and business information is retained only as long as necessary for legal, regulatory, or operational purposes.
- Secure Disposal: Information no longer required is securely destroyed or de-identified, in accordance with legal requirements and industry best practice.

We periodically review our data holdings and disposal processes to prevent unnecessary retention.

Integrity and Security Measures

- Technical Safeguards: Encryption, firewalls, access controls, and secure payment gateways are employed to protect information.
- Organisational Measures: Staff training, regular audits, and incident response plans are in place to ensure ongoing security.
- Breach Response: In the event of a data breach, affected individuals and the Office of the Australian Information Commissioner (OAIC) will be notified in accordance with the Notifiable Data Breaches scheme.

We take a proactive approach to integrity and security, regularly updating our safeguards to address emerging threats.

Additional Policies and Notices

- Cookies and Tracking: Our website uses cookies and similar technologies for functionality and analytics. Users are informed and given control over their preferences.
- Marketing Communications: Recipients can opt out of marketing communications at any time using provided mechanisms.
- Office Visits: Visitors to our offices may be subject to security monitoring for safety and compliance. Privacy notices are displayed onsite.

We are committed to transparency regarding all data collection methods and uses.

Access, Correction, and Participation

- Access: Individuals may request access to their personal information held by us, subject to certain exceptions under law.
- Correction: Inaccurate, out-of-date, incomplete, or misleading information will be corrected upon request.
- Complaints and Requests: Mechanisms are in place for individuals to lodge complaints, make inquiries, or request correction or deletion of their information.

Requests are handled promptly, transparently, and in accordance with applicable law.

Enforcement and Accountability

We monitor and review our privacy and data integrity practices regularly. Staff are trained on compliance requirements, and we cooperate fully with regulators, including the OAIC and international authorities where required. Breaches of this policy may result in disciplinary action or termination of contracts.

Contact Information

For questions, requests, or complaints regarding this policy or our data handling practices, please contact:

Privacy Officer / Data Protection Officer

RME Solutions Technology

Email: privacy@rmesolutions.com.au

All correspondence will be responded to in a timely and respectful manner.

References and Further Reading

- Australian Privacy Principles | OAIC
- Privacy Act 1988 (Cth)
- General Data Protection Regulation (GDPR)
- PCI DSS Compliance
- Privacy Laws of the World – Australian Privacy Foundation
- Data protection regulation around the world - Thales

This policy may be updated from time to time to reflect changes in law, business practices, or stakeholder expectations. Please refer to our website for the most current version.