ACIEM

Privacy Policy

Version: 2.1
May 2024

Revision History

Revision	Approved by	Date	Comments
V 1.0	Roger Dean	17 November 2017	Version 1 of Aciem Privacy Policy document (update from Aimia policy).
V 1.1	Roger Dean	10 June 2022	Updated Aciem location and branding elements
V 2.0	Roger Dean	20 March 2023	Updated Privacy Policy
V 2.1	Roger Dean	27 May 2024	Updated responsibilities

What is Data Privacy and Personal Information

Data Privacy governs how personal information is collected, used, stored, and managed.

Personal information is information about an identifiable individual and covers both information that is simply about them (e.g., height) and information that may identify them (e.g., name). The information does not need to name the individual, as long as they are identifiable in other ways (e.g., their home address).

Privacy Principles from 2020 Privacy Act

The following Privacy Principles from the Privacy Act of 2020 are relevant to Aciem's current business activities, and must be followed:

- 5: Storage and security of information
    - Aciem will ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse, or disclosure of personal information. If Aciem has a serious privacy breach, it will notify the Office of the Privacy Commissioner as soon as possible (within 72 hours).
- 9: Limits on retention of personal information
    - Aciem will not keep personal information for longer than it is required for the purpose it may lawfully be used.
- 10: Use of personal information
    - Aciem will only use personal information for the purpose it was collected
- 11: Disclosing personal information
    - Aciem will only disclose personal information for the purpose for which it was originally collected or obtained.

Additional privacy principles may become relevant if Aciem's business activities change.

Aciem Data Privacy Principles

Aciem's Data Privacy Policy has been developed in accordance with Aciem's Values of being smart, credible, energetic, and proactive in all that we do.

- **Smart**
    - Data protection is an integral part of Aciem's business, and of the smart systems and processes that we use to protect and manage our loyalty solutions.
- **Credible**
    - Aciem is committed to handling customers' and clients' personal information with the highest level of confidentiality, security, and integrity.
- **Energetic**
    - Aciem is transparent, open, and honest with customers about how we safeguard their data privacy and provides our customers with information in a timely manner.
- **Proactive**
    - Aciem uses industry-recognised monitoring and alerting tools to actively manage and protect the data we safeguard on behalf of our customers and in compliance with all applicable privacy regulations.

Policy Statements

- Data protection and the protection of customer personally identifiable information (PII) will be considered a critical aspect of any system or process design.
- Personally identifiable information will be protected from unauthorised access, modification, or deletion.
- All Aciem employees will be expected to follow data privacy good practice and to protect the privacy of all personal information
- Any breach in our data protection will be treated as a serious incident. We will inform any impacted customers in a transparent and timely manner if any such breach were to occur.

Guidelines

Classification

Information received from customers will be considered and treated as PII by default, unless otherwise marked.

Rationale
This ensures that a default level of protection is applied to all customer information and decreases the likelihood that PII is not provided with adequate protection.

Implications
Customer information is to be encrypted in transit and at rest wherever possible.

Customer information is not to be sent via email

Hard copies of customer information are to be kept secured when not in use, not to be left unattended, and to be disposed of securely via shredding when no longer required.

Design

All new or changes to IT systems and/or processes must explicitly consider data privacy as part of their design.

Rationale
This ensures that the data privacy integrity of a system or process is maintained throughout the change process.

Implications
All new or changes to IT systems must include data privacy requirements in their design

All new or changes to IT systems and/or processes must undergo a data privacy review by the IT Manager or the Managing Director, IT, prior to implementation.

Employee Training

All Aciem employees must understand and acknowledge their accountabilities to protect the privacy of personal information

Rationale
This ensures that employees do not accidentally breach data privacy through a lack of knowledge regarding the appropriate way to protect the information

Implications
All Aciem employees must undergo annual training on privacy matters.

Aciem must audit the annual training records to ensure that training has been completed.

Third Parties

Aciem must ensure that any contract with a third party includes appropriate data privacy clauses. Aciem must ensure that the third party fulfills their security and data privacy accountabilities as specified in any contract.

Rationale
This ensures that data privacy controls are not 'set and forget' but are actively monitored over their lifetime.

Implications
Aciem must audit or otherwise check third party compliance with data privacy contract clauses at least annually.

Data Privacy Breaches

All breaches or suspected breaches must be immediately reported and managed as a serious incident.

Rationale
Fast reporting allows an incident to be contained and managed as successfully as possible.

Implications
All privacy breaches are to be reported to management as soon as possible.

Related Documents

- IT Security Policy – for further information on the technical controls used to secure data privacy
- Remote Working Policy
- Data Classification Policy
- Staff Handbook – for further information on disciplinary procedures
- Incident Management Procedures

Accountabilities

Managing Directors

- Maintain overall accountability for data handling, storage, processing, and protection
- Approve data privacy policy
- Ensure sufficient funding is available and assigned for recommended data protection initiatives
- Manage all incidents relating to the compromise of data privacy

Managing Director, IT

- Develop, implement, and maintain all IT security policies and procedures required to maintain data privacy
- Encourage a security-focused culture among IT staff

Managing Director, Client Services

- Be the point of contact for customers in the event of a privacy breach
- Encourage a security-focused culture among Client Services staff

Managing Director, Operations

- Implement and maintain processes that protect PII from physical access, e.g., physical protection of offices, shredding of paper containing PII, etc.
- Encourage a security-focused culture among Operations staff

Privacy and Data Protection Officer

- Develop and implement company data protection strategy
- Maintain currency and relevancy of data privacy policy and procedures. This includes reviewing the policy and procedures whenever there are any changes to:
    - the privacy laws and regulations
    - customer solutions that have the potential to impact on privacy.
- Ensure that all company employees and data subjects are informed about and understand their rights, obligations, and responsibilities regarding data protection
- Provide expert advice about the interpretation and application of data protection rules, and complete Data Protection Impact Assessments as required
- Monitor and provide reporting on data privacy compliance
- Monitor company compliance with all data protection rules and regulations, and highlight any non-compliance for remediation
- Maintain comprehensive records of all data processing activities conducted by the company, and the purpose of these activities
- Maintain a living inventory of all PII stored by the company
- Respond to any data protection queries, complaints or incidents

Manager, IT

- Implement required IT initiatives as directed to ensure compliance with data protection rules and regulations
- Act as directed to contain and/or manage any data privacy breach

All Staff

- Complete training on data privacy and security as required
- Report any breaches or suspected breaches immediately
- Abide by all company policies and procedures regarding data privacy

Noncompliance

Failure to abide by this policy may result in disciplinary action, up to and including immediate termination of employment with Aciem.

Suite 303/Building C
100 Parnell Road
Parnell
Auckland 1052

aciem.co.nz