Biz M&A - Privacy Policy

29th June 2025

1. Purpose

This Privacy Policy establishes Biz m&a's framework for the ethical, compliant, and secure handling of personal information in accordance with the **Privacy Act 1993**. The purpose is to ensure that personal data is managed with integrity and in support of client trust, employee confidentiality, and legal compliance across all business functions, including sales, marketing, HR, and operations.

2. Scope

This policy applies to:

- All permanent and temporary employees, contractors, licensees, and agents of Biz m&a
- All client and employee personal data handled by the business, whether in physical or electronic form
- All business units involved in the collection, storage, use, processing, transfer, or destruction of personal information

3. Legal Framework

This policy is governed by the **Privacy Act 1993**, specifically its 12 Privacy Principles, and is supplemented by relevant data retention, tax, employment, and anti-money laundering legislation applicable in New Zealand.

4. Information Collection and Lawful Purpose

Biz m&a collects personal data for legitimate and specified business purposes. These include:

- Conducting property listings, sales, and lease transactions
- Verifying identity and client eligibility under AML/CFT obligations
- Managing employment and contractor relationships
- Providing property management and agency services
- Meeting compliance requirements of REINZ and other regulatory bodies

Requirements:

- Information must be collected directly from the individual where practical (Principle 2)
- The individual must be informed of:
    - The purpose of collection
    - The intended recipients
    - Their rights to access and correct data (Principle 3)

5. Data Use, Retention, and Disposal

Permitted Use

Personal information must be used only for its originally collected purpose, unless:

- The data subject consents to another use
- Required or permitted by law
- Necessary to prevent or mitigate serious threats to health or safety

Data Retention Guidelines

- Retain only for as long as required by law or business necessity (e.g. IRD, audit)
- Property listings with no sale or active agency must be destroyed after 90 days unless a risk factor or legal claim is identified
- Secure destruction procedures must be followed for paper and digital records

6. Access, Correction, and Accuracy

Individual Rights:

- Individuals have the right to access personal information held about them
- Requests must be acknowledged within 20 working days
- Individuals may request corrections; if declined, a statement of dispute must be appended

Accuracy Obligations:

- Staff must ensure that data recorded is accurate, complete, and up to date (Principle 8)
- Any known inaccuracies must be corrected with the individual's knowledge and consent

7. Data Security and Protection

Biz m&a must implement reasonable safeguards to protect personal data against:

- Unauthorised access or disclosure
- Loss, theft, or misuse
- Alteration or destruction

Examples of controls include:

- Password-protected systems and encrypted files
- Restricted access to client/employee records
- Secure file storage and disposal containers
- Role-based access control for sensitive data

8. Unique Identifiers and Record Indexing

Biz m&a may assign unique identifiers (e.g., client or staff ID numbers) only when operationally required and must not use them as substitutes for personally identifiable information.

- Identifiers must not be disclosed externally unless required in accounting or regulatory documentation
- All records must be indexed by name and property address to prevent confusion or misidentification

9. Responsibilities

Management / Licensees

- Maintain policy compliance and staff training programs
- Identify high-risk data processes and implement controls
- Ensure forms and contracts include proper disclosures and consents
- Establish secure access, storage, and disposal systems

Employees and Salespersons

- Collect information openly and with consent
- Verify that the individual understands the use and scope of data
- Avoid recording non-relevant or sensitive personal opinions
- Store data securely in-office and avoid unnecessary off-site storage
- Refer requests, complaints, or suspected breaches to the Privacy Officer

10. Third-Party Disclosures and Data Transfers

Disclosures to third parties (e.g., REINZ, auditors, solicitors, external agents) must be:

- Clearly authorised by the data subject, or
- Permitted under the Privacy Act (e.g., for legal enforcement, health/safety concerns, or public interest)

Internal transfers of personal information must follow documented procedures and include proper tracking and consent.

11. Data Subject Requests and Timeframes

Biz m&a must respond to formal access or correction requests within 20 working days.

If an extension is required:

- The individual must be notified with reasons
- The company must still act without undue delay

Redactions or formatting adjustments may be made where reasonable, but the justification must be documented and communicated.

12. Privacy Breach Protocol and Enforcement

Breach Reporting:

All actual or suspected breaches must be reported immediately to the Privacy Officer.

Investigation and Consequences:

Privacy breaches may lead to:

- Internal investigation and disciplinary action (up to dismissal)
- Formal complaint to the **Privacy Commissioner**
- Civil remedies (damages up to NZD $200,000)
- Public reprimand and remedial orders

13. Designated Privacy Officer

The **Office Manager** acts as Biz m&a's **Privacy Officer**, with responsibility to:

- Promote adherence to privacy principles
- Manage access and correction requests
- Liaise with the Privacy Commissioner during investigations
- Oversee training and compliance audits

14. Training and Awareness

All staff and contractors are required to undergo privacy training during onboarding and through regular refresher sessions. Training must cover:

- Collection and consent protocols
- Secure data handling
- Internal reporting of breaches and inquiries
- Role-based privacy responsibilities

15. Policy Review

This policy is reviewed annually or earlier if:

- Legislative changes occur
- New data-handling technologies or practices are implemented
- Significant privacy incidents are reported