PRIVACY & COMPLIANCE

NGO Data Governance & Privacy Framework

A Comprehensive Framework for Not-for-Profit Organisations in Aotearoa New Zealand and Australia

Version 1.0 | 2025 Edition | AmplifyData.org.nz

Privacy Act 2020 | Data Classification | Māori Data Sovereignty | Breach Response | Consent Management | RACI Matrix | Policy Templates

Published by AmplifyData.org.nz • Contact@AmplifyData.org.nz

Table of Contents

18 sections covering data governance, privacy compliance, and practical templates

roduction to Data Governance for NGOs

ata governance matters and the regulatory landscape for not-for-profit organisations

Why Data Governance Matters for Not-for-Profits

Not-for-profit organisations hold some of the most sensitive data in our communities — information about vulnerable beneficiaries, donor financial details, volunteer personal information, and programme outcomes that can reveal intimate details about people's lives.

Why NGOs Need Data Governance

- **Trust is your most valuable asset** — Donors, beneficiaries, and communities trust you with sensitive data
- **Regulatory compliance is mandatory** — Privacy laws apply equally to NGOs
- **Funding requirements demand it** — Government contracts require data protection
- **Ethical obligations** — You serve vulnerable communities
- **Operational efficiency** — Good governance improves decision-making

Consequences of Poor Data Governance

- Privacy Commissioner investigations and penalties
- Loss of donor trust and funding
- Reputational damage in your community
- Legal liability for board members and staff
- Breach of funding agreements
- Harm to the people you serve

The Regulatory Landscape

New Zealand

- Privacy Act 2020 (13 IPPs)
- Health Information Privacy Code 2020
- Charities Act 2005
- Incorporated Societies Act 2022
- Te Tiriti o Waitangi obligations

Australia

- Privacy Act 1988 (13 APPs)
- Notifiable Data Breaches Scheme
- ACNC Governance Standards
- State health records legislation
- My Health Records Act 2012

Cross-Border

- GDPR (EU donors/beneficiaries)
- Trans-Tasman data flows
- International partner sharing

a Governance Framework Overview

ur-layer framework for comprehensive data governance in your organisation

Framework Structure

Layer 1	**Governance & Accountability** — Board oversight, data governance roles, risk management, performance reporting
Layer 2	**Policies & Standards** — Privacy policy, data classification, consent management, retention schedule, breach response
Layer 3	**Processes & Procedures** — Data collection, access management, quality management, third-party management, training
Layer 4	**Technology & Tools** — CRM/database systems, security controls, backup and recovery, audit and monitoring

The Seven Pillars of NGO Data Governance

PRINCIPLE	DESCRIPTION	APPLICATION
Accountability	Clear ownership and responsibility for data	Designated data stewards, board oversight
Transparency	Open about data practices	Privacy notices, annual reporting
Integrity	Data is accurate, complete, and reliable	Data quality processes, validation
Security	Protected from unauthorised access	Access controls, encryption, training
Consent	Collected and used with proper authority	Consent management, opt-in/opt-out
Purpose Limitation	Used only for stated purposes	Data minimisation, use restrictions
Cultural Respect	Honours cultural values and sovereignty	Māori data sovereignty, community protocols

Privacy Act 2020 Compliance

tanding and implementing the 13 Information Privacy Principles

Key Changes from the 1993 Act

What Changed in 2020

- **Mandatory breach notification** — Must notify within 72 hours of becoming aware
- **Compliance notices** — Privacy Commissioner can issue binding notices
- **New access denial grounds** — Updated provisions for refusing access requests
- **Strengthened cross-border rules** — Tighter controls on overseas data transfers
- **Expanded Commissioner powers** — Greater enforcement capability
- **Increased maximum penalties** — Higher fines for non-compliance

The 13 Information Privacy Principles

IPP	PRINCIPLE	NGO APPLICATION
1	Purpose of Collection	Only collect data for lawful purposes connected to your charitable mission
2	Source of Information	Collect directly from individuals unless an exception applies (e.g., referrals with consent)
3	Collection from Subject	Inform individuals about what you collect, why, who receives it, and their rights
4	Manner of Collection	Collect lawfully and fairly, with respect for vulnerable populations
5	Storage and Security	Protect from loss and unauthorised access with appropriate controls
6	Access to Information	Respond to access requests within 20 working days
7	Correction	Correct inaccurate information promptly when requested
8	Accuracy Before Use	Verify information is accurate before using for decisions
9	Retention	Don't keep data longer than necessary; follow retention schedule
10	Use Limitation	Only use for the purpose collected; get consent for new uses
11	Disclosure Limitation	Only disclose as permitted; document all disclosures
12	Cross-Border Disclosure	Ensure comparable protections for overseas transfers
13	Unique Identifiers	Use your own IDs; minimise collection of government identifiers

Security Controls (IPP 5)

Access Controls

- Unique user accounts (no shared logins)
- Strong passwords (12+ characters)
- Multi-factor authentication for sensitive systems
- Regular access reviews

Physical Security

- Locked offices after hours
- Secure storage for paper files
- Clean desk policy
- Visitor management

Technical Security

- Encrypted devices
- Regular software updates
- Antivirus protection
- Secure backup systems

Human Security

- Staff training
- Background checks where appropriate
- Volunteer agreements
- Exit procedures

tralian Privacy Principles Compliance

tanding the 13 APPs and how they apply to not-for-profit organisations

Who Is Covered?

The Privacy Act 1988 and its 13 Australian Privacy Principles (APPs) apply to organisations with annual turnover over $3 million, plus health service providers, organisations trading in personal information, and government contractors.

Many NGOs Are Covered Through

- Funding contracts requiring APP compliance
- Health service delivery
- Government contracting obligations
- Voluntary opt-in to demonstrate best practice

Key Differences from NZ Privacy Act

ASPECT	NEW ZEALAND (IPPS)	AUSTRALIA (APPS)
Breach Notification	Notify "as soon as practicable"	Notify within 30 days of awareness
Sensitive Info	Covered under general principles	Specific enhanced protections for sensitive info
Direct Marketing	Covered by purpose and use limits	Specific APP 7 governs direct marketing
Government IDs	IPP 13 (unique identifiers)	APP 9 with additional restrictions
Anonymity	Not specifically addressed	APP 2 requires anonymity option

Mana Raraunga – Māori Data Sovereignty

ring Māori rights and interests in data about Māori communities

Understanding Māori Data Sovereignty

Te Mana Raraunga (the Māori Data Sovereignty Network) advocates for Māori rights and interests in data. For NGOs working with Māori communities, understanding and implementing Māori data sovereignty principles is both an ethical obligation and a Treaty responsibility.

Core Principles

- **Rangatiratanga (Authority)** — Māori have an inherent right to exercise control over Māori data
- **Whakapapa (Relationships)** — Data has genealogical connections that must be respected
- **Whanaungatanga (Obligations)** — Reciprocal relationships and obligations to Māori communities
- **Kotahitanga (Collective benefit)** — Data should be used for collective Māori benefit
- **Manaakitanga (Guardianship)** — Caring for data as a taonga (treasure)
- **Kaitiakitanga (Stewardship)** — Sustainable and responsible data management

Practical Application for NGOs

- [ ] Engage with Māori communities about data practices before collecting data
- [ ] Develop data sharing agreements with iwi and Māori organisations
- [ ] Ensure Māori communities have access to data about their communities
- [ ] Consider Māori governance of Māori data within your organisation
- [ ] Report aggregate Māori data back to Māori communities
- [ ] Avoid deficit framing when reporting Māori data
- [ ] Protect cultural knowledge and ensure it is not misappropriated

a Governance Roles & RACI Matrix

g clear accountability and responsibilities for data governance

RACI Matrix for Data Governance

ACTIVITY	BOARD	CEO	DATA PROTECTION LEAD	IT/SYSTEMS	PROGRAMME MANAGERS	ALL STAFF
Privacy Policy approval	A	R	C	I	I	I
Privacy risk oversight	A	R	R	C	C	I
Data collection practices	I	A	C	I	R	R
System security	I	A	C	R	I	C
Breach response	I	A	R	R	C	C
Staff training	I	A	R	C	C	R
Data quality	I	A	C	C	R	R
Third-party agreements	I	A	R	C	C	I

RACI Key

R = Responsible (does the work) • **A** = Accountable (owns the outcome) • **C** = Consulted (provides input) • **I** = Informed (kept up to date)

a Classification & Handling

rising data by sensitivity and applying appropriate protection controls

Data Classification Levels

Highly Sensitive	**Examples:** Health records, abuse disclosures, financial data, cultural knowledge. **Controls:** Encrypted, access restricted, audit logged, no email sharing.
Sensitive	**Examples:** Beneficiary contact details, donor records, HR data. **Controls:** Password protected, limited access, secure storage.
Internal	**Examples:** Meeting minutes, internal reports, policies. **Controls:** Staff access, organisational systems, standard security.
Public	**Examples:** Annual report, website content, marketing materials. **Controls:** No restrictions, quality control on publication.

nsent Management Framework

ng, recording, and managing consent for data collection and use

Types of Consent

Explicit Consent

Active, clear agreement for specific purposes. Required for sensitive data, marketing, and third-party sharing.

- Written or digital signature
- Tick-box (not pre-ticked)
- Verbal with documented record

Implied Consent

Reasonably inferred from actions and context. Appropriate for routine service delivery and administrative purposes.

- Completing an application form
- Continuing to use a service
- Not objecting after notification

Consent Management Checklist

- [ ] Consent is freely given (no coercion or service denial for refusal)
- [ ] Purpose of data use is clearly explained in plain language
- [ ] Individuals understand what they are consenting to
- [ ] Consent is specific to identified purposes (not bundled)
- [ ] Individuals can withdraw consent at any time
- [ ] Consent records are stored securely with date and scope
- [ ] Regular review and renewal of consent where appropriate

ıor Data Protection

ing donor information and maintaining trust in your fundraising relationships

Donor Data Categories

DATA TYPE	CLASSIFICATION	RETENTION PERIOD	KEY CONTROLS
Contact details	Sensitive	7 years after last donation	CRM access controls, regular updates
Payment/banking information	Highly Sensitive	Only during processing	PCI compliance, encryption, no local storage
Donation history	Sensitive	7 years (tax purposes)	CRM access controls, audit trail
Communication preferences	Internal	Duration of relationship	Opt-in/opt-out management
Bequest/legacy information	Highly Sensitive	Until estate settled + 7 years	Restricted access, encrypted storage

Common Donor Data Pitfalls

- Using donor data for purposes beyond what was consented to
- Sharing donor lists with partner organisations without consent
- Storing credit card details locally instead of using secure payment processors
- Not providing opt-out options for different communication types
- Retaining data indefinitely without a retention policy

ıeficiary & Client Data Protection

ing the people you serve through responsible data practices

Special Considerations for Beneficiary Data

Power Imbalance Awareness

Beneficiaries may feel unable to refuse data collection when they depend on your services. Extra care is needed to ensure consent is truly voluntary and that data collection is proportionate to service delivery needs.

Vulnerable Populations

- Trauma-informed data collection approaches
- Right to decline without service impact
- Cultural safety in assessment processes
- Age-appropriate consent for children/young people

Case Notes & Assessments

- Factual, objective recording
- Client right to access their records
- Secure storage and restricted access
- Clear retention and destruction schedules

vacy Impact Assessment

ving and mitigating privacy risks in new projects and systems

When to Conduct a PIA

Trigger Events

- Implementing a new CRM, database, or technology system
- Starting a new programme that collects personal information
- Changing how existing personal information is used or shared
- Entering data sharing agreements with partner organisations
- Moving to cloud-based systems or changing service providers
- Any project involving sensitive or vulnerable populations

PIA Process

1. **Describe the Project**

   Document what personal information will be collected, how it will be used, who will access it, and how long it will be retained.

2. **Identify Privacy Risks**

   Assess risks against all applicable privacy principles (IPPs/APPs). Consider risks of collection, storage, use, disclosure, and destruction.

3. **Assess Risk Level**

   Rate each risk by likelihood and impact. Consider the sensitivity of data and vulnerability of individuals involved.

4. **Develop Mitigations**

   Design controls to reduce risks to acceptable levels. Document decisions and rationale.

5. **Review and Monitor**

   Get sign-off from Data Protection Lead and management. Schedule regular reviews of the PIA as the project evolves.

a Breach Response Plan

ng for, responding to, and recovering from data breaches

Breach Response Timeline

! **Immediate (0-4 hours): Contain**

Contain the breach, secure systems, preserve evidence. Alert Data Protection Lead and CEO.

2 **Within 24 hours: Assess**

Assess scope, identify affected individuals, determine if breach is notifiable. Engage IT support.

3 **Within 72 hours: Notify**

Notify Privacy Commissioner (NZ) or OAIC (AU) if breach is notifiable. Notify affected individuals.

4 **Post-Breach: Review**

Conduct root cause analysis. Implement improvements to prevent recurrence. Update policies and training. Report to board.

Notifiable Breach Checklist

A breach is notifiable if it:

- Involves personal information, AND
- Has caused, or is likely to cause, serious harm

Serious harm factors: Sensitivity of information, whether data was encrypted, who obtained it, nature of potential harm, and whether steps can reduce harm.

a Retention & Disposal

ing the lifecycle of data from collection through secure destruction

Recommended Retention Periods

DATA TYPE	RETENTION PERIOD	DISPOSAL METHOD
Donor records	7 years after last donation	Secure deletion/shredding
Beneficiary records	7 years after service ends	Secure deletion/shredding
Staff records	7 years after employment ends	Secure deletion/shredding
Financial records	7 years (legal requirement)	Secure deletion/shredding
Board minutes	Permanently	Archive to secure storage
Contracts	7 years after expiry	Secure deletion/shredding
Volunteer records	3 years after engagement ends	Secure deletion/shredding
Event registrations	2 years after event	Secure deletion

rd-Party Data Sharing

ing data sharing with partners, funders, and service providers

Data Sharing Agreement Essentials

- [ ] **Purpose** — Clearly defined reasons for sharing data
- [ ] **Legal basis** — Consent, legitimate purpose, or legal requirement
- [ ] **Data description** — Specific fields/types of data being shared
- [ ] **Security requirements** — Minimum protection standards
- [ ] **Use restrictions** — Data cannot be used beyond agreed purposes
- [ ] **Retention and disposal** — How long data is kept and how it is destroyed
- [ ] **Breach notification** — Obligation to notify of any breaches
- [ ] **Review and termination** — Regular review dates and exit provisions

icy Templates

to-adapt templates for your organisation's data governance policies

Essential Data Governance Policies

Privacy Policy

Your public-facing commitment to data protection. Covers what you collect, why, how you protect it, and individuals' rights.

Data Classification Policy

Defines classification levels and handling requirements for each category of data.

Acceptable Use Policy

Staff and volunteer obligations for appropriate use of data and technology systems.

Data Breach Response Policy

Step-by-step procedures for responding to data breaches including notification requirements.

Data Retention Policy

Retention schedules for all data types with destruction procedures and documentation.

Data Sharing Policy

Framework for sharing data with third parties including agreement templates.

mpliance Checklists

al checklists for ongoing privacy and data governance compliance

Annual Data Governance Review

- [ ] Review and update privacy policy
- [ ] Audit data holdings against retention schedule
- [ ] Review and update data sharing agreements
- [ ] Complete staff privacy training
- [ ] Test data breach response procedures
- [ ] Review access controls and user permissions
- [ ] Audit third-party system providers for compliance
- [ ] Update RACI matrix for any organisational changes
- [ ] Report data governance status to board
- [ ] Review and update Privacy Impact Assessments

lementation Roadmap

ed approach to implementing your data governance framework

12-Month Implementation Plan

Months 1-3	**Foundation:** Appoint data governance lead, conduct data audit, draft privacy policy, classify data types, establish breach response process
Months 4-6	**Build:** Implement consent framework, develop retention schedule, create data sharing agreements, begin staff training programme
Months 7-9	**Embed:** Roll out policies to all staff, conduct PIAs for key systems, review third-party providers, implement access controls
Months 10-12	**Mature:** Conduct compliance audit, test breach response, report to board, plan for Year 2 improvements, celebrate progress

ources & Further Reading

ganisations and resources for ongoing data governance support

Key Organisations

New Zealand

- Office of the Privacy Commissioner (privacy.org.nz)
- Te Mana Raraunga — Māori Data Sovereignty Network
- CERT NZ — Cyber security advice
- Charities Services — Governance guidance
- Netsafe — Online safety resources

Australia

- Office of the Australian Information Commissioner (OAIC)
- Australian Cyber Security Centre (ACSC)
- ACNC — Governance and compliance
- IDCARE — Identity and cyber support
- Not-for-Profit Law (Justice Connect)

AmplifyData.org.nz • Contact@AmplifyData.org.nz