Good Security

GUIDE WATERMARKED PDF

PRACTICAL GUIDANCE

Privacy Act 2020 Compliance Guide

A plain-English guide to NZ Privacy Act 2020 obligations for SMEs — covering the 13 Information Privacy Principles, IPP 3A indirect collection notification (May 2026), IPP 12 cross-border disclosure, and breach notification obligations.

Branded customer-ready document | Shareable with leadership teams | Generated 12 Mar 2026

A plain-English guide for NZ businesses

Good Security · goodsecurity.co.nz · **hello@goodsecurity.co.nz**

About this guide The Privacy Act 2020 applies to every NZ business — regardless of size — that holds personal information about individuals. This guide explains the key obligations in plain English, covers what changed from the 1993 Act, and addresses IPP 3A indirect collection notification (taking effect May 2026) and IPP 12 cross-border disclosure obligations.

PART 1: THE BASICS

What is "personal information"?

Personal information is any information about an identifiable individual. This includes:

- Names, contact details, email addresses
- IP addresses and online identifiers
- Financial information — account numbers, transaction history
- Health information
- Employment records

- Photos and CCTV footage
- Anything else that could identify a specific person, or be combined with other data to do so

The threshold for "identifiable" is deliberately low. If information can be combined with other readily available data to identify someone, it counts.

Who does the Act apply to?

The Act applies to every agency — every business, organisation, and individual — that holds personal information about people in New Zealand. There is no minimum size threshold. A sole trader with a customer contact list is covered. A multinational with NZ customers is covered.

PART 2: THE INFORMATION PRIVACY PRINCIPLES (IPPs)

The Act contains 13 Information Privacy Principles. These are the core rules governing how you must handle personal information.

IPP 1 — Purpose of collection Only collect personal information if you have a lawful purpose and genuinely need it. Do not collect more than you need.

IPP 2 — Source of collection Collect personal information directly from the individual where practicable.

IPP 3 — Collection notice When collecting personal information, tell the individual: who you are, why you are collecting it, and who you will share it with. This transparency requirement applies at the point of collection — on your website form, at your front desk, on your intake paperwork.

IPP 3A — Indirect collection notification *(effective May 2026, see Part 3 below)* When collecting personal information from a source other than the individual (indirect collection), take reasonable steps to ensure the individual is aware of specified matters including the fact of collection, its source, and its purpose.

IPP 4 — Manner of collection Do not collect personal information by unlawful means or by means that are unfair or unreasonably intrusive.

IPP 5 — Storage and security Protect personal information from loss, unauthorised access, use, modification, disclosure, or other misuse. Take reasonable security safeguards proportionate to the sensitivity of the information.

IPP 6 — Access to personal information Individuals have the right to request access to personal information you hold about them. You must respond within 20 working days.

IPP 7 — Correction of personal information Individuals have the right to request correction of inaccurate personal information. You must correct it, or note that correction was requested.

IPP 8 — Accuracy Before using personal information, take reasonable steps to ensure it is accurate, up to date, complete, and not misleading.

IPP 9 — Retention Do not keep personal information longer than you need it. Have a retention schedule and dispose of data securely when it is no longer required.

IPP 10 — Use of personal information Only use personal information for the purpose for which it was collected, or a directly related purpose, unless an exception applies — such as individual consent.

IPP 11 — Disclosure of personal information Do not share personal information with other parties unless an exception applies — consent, legal requirement, or a purpose directly related to why it was collected.

IPP 12 — Cross-border disclosure *(see Part 3A below)* Before disclosing personal information to an overseas recipient, ensure the recipient is subject to comparable privacy protections, or take other prescribed steps. The Section 11 agent exception means cloud providers holding data on your behalf under contract are generally not considered overseas recipients.

IPP 13 — Unique identifiers Do not assign a unique identifier to an individual unless it is necessary for your functions. Do not use another agency's unique identifier unless required by law or with the individual's consent.

PART 3: IPP 3A — INDIRECT COLLECTION NOTIFICATION (MAY 2026)

What is IPP 3A?

IPP 3A is a new principle taking effect on **1 May 2026**. It requires organisations to take reasonable steps to notify individuals when their personal information has been collected indirectly — from a third party rather than directly from the person.

Why does this matter?

Many NZ businesses collect personal information from sources other than the individual without a formal notification process. Common examples include:

- Receiving candidate details from recruitment agencies
- Getting referral information from business partners
- Receiving customer lists from parent companies or distributors
- Collecting information from public registers or industry databases
- Obtaining financial information from brokers or intermediaries

What do you need to do before May 2026?

Step 1: Identify your indirect collection sources List every workflow where personal information comes to your business from someone other than the individual. Include HR, sales, operations, and partner channels.

Step 2: Assess whether IPP 3A applies For each indirect collection path, determine whether an exception applies (e.g., the information was collected by an agent on your behalf under Section 11, or notification would prejudice the purpose of collection).

Step 3: Establish notification processes For each indirect collection path where IPP 3A applies, decide how and when the individual will be notified. This could be an email, letter, phone call, or integration into an existing workflow.

Step 4: Document your decisions Record your assessment for each indirect collection source — whether IPP 3A applies, what notification process is in place, and if an exception is relied on, why.

PART 3A: IPP 12 — CROSS-BORDER DISCLOSURE (ALREADY IN FORCE)

What is IPP 12?

IPP 12 has been in force since the Privacy Act 2020 commenced on 1 December 2020. It governs the disclosure of personal information to overseas recipients, requiring organisations to take reasonable steps to ensure comparable privacy protection.

Why does this matter?

Most NZ businesses store personal information overseas through cloud services. If you use Microsoft 365, Google Workspace, Xero, Salesforce, AWS, or any overseas SaaS application, IPP 12 is relevant.

However, many standard cloud service arrangements fall under the **Section 11 agent exception**: when an overseas provider holds your data solely as your agent (processing it under your instructions, under contract), the transfer is generally not treated as a "disclosure" to an overseas recipient.

What do you need to do?

Step 1: Know where your personal data goes Build or review your Personal Data Inventory. For each category of personal data, identify which systems store it and where those systems are hosted.

Step 2: Assess each overseas provider Determine whether each provider operates as your agent (under a data processing agreement) or as an independent recipient. For agent relationships, confirm adequate contractual safeguards. For disclosures, assess whether the recipient is subject to comparable privacy protections.

Step 3: Update your Privacy Policy Your Privacy Policy must disclose that personal information may be stored or processed overseas, and identify the countries or regions involved.

Step 4: Document your compliance steps Maintain evidence that you have taken reasonable steps. This protects you if a complaint is made.

PART 4: PRIVACY BREACH OBLIGATIONS

When must you notify?

Under the Privacy Act 2020, you **must** notify the Privacy Commissioner of a privacy breach if it has caused, or is **likely to cause**, serious harm. This is not optional and the threshold is lower than you might expect.

You should also notify affected individuals if the breach poses a real risk of harm to them.

What is a "serious harm" breach?

Serious harm is assessed based on:

- The sensitivity of the information involved
- Whether it could be used for fraud, identity theft, or other harmful purposes
- The scale of the breach — how many individuals are affected
- The security measures in place at the time

Examples of breaches that typically meet the serious harm threshold:

- Customer financial or health data accessed by an attacker
- Significant quantities of personal data exposed through a system misconfiguration
- Personal data of staff or clients stolen on an unencrypted laptop

How do you report?

Privacy breach notifications are made to the Office of the Privacy Commissioner (OPC) at privacy.org.nz. There is an online notification form. You must notify as soon as practicable after becoming aware of the breach.

When in doubt, notify

If you are not sure whether a breach meets the serious harm threshold, err on the side of notification. The Privacy Commissioner takes a collaborative approach with organisations that self-report in good faith. The consequences of failing to notify a notifiable breach are significantly worse than notifying one that may not have met the threshold.

PART 5: PRACTICAL STEPS FOR SME COMPLIANCE

Priority actions for most NZ SMEs

1. Conduct a Personal Data Inventory Know what personal information you hold, where it is stored, who has access, and how long you keep it. This is the foundation of Privacy Act compliance and a

prerequisite for IPP 3A. Start with your highest-volume data flows: customer records, staff records, and payment processing.

2. Review and update your Privacy Policy Your Privacy Policy must accurately describe how you collect, use, store, and share personal information. Under IPP 12, it must disclose overseas storage and the regions involved. After May 2026, your processes must also address IPP 3A indirect collection notification.

3. Establish a privacy breach response procedure Have a written procedure for identifying, assessing, containing, and reporting privacy breaches. Know who is responsible and what the first three steps are. This does not need to be lengthy.

4. Train staff on privacy obligations Staff who handle personal information must understand their obligations — what to do when a customer asks for their data, what to do if they suspect a breach, what not to share and with whom. Annual training of one hour or less is a reasonable minimum for most SMEs.

5. Review contracts with third-party providers Ensure your agreements with cloud providers, IT suppliers, and any other party handling personal information on your behalf include appropriate data processing provisions and breach notification requirements.

6. Implement IPP 3A compliance before May 2026 Audit your indirect collection sources, establish notification processes for each applicable workflow, document your decisions, and train the staff who handle indirect collection.

7. Review IPP 12 cross-border disclosure arrangements Review your overseas data flows, assess each cloud provider's agent status and contractual safeguards, document your findings, and update your Privacy Policy to disclose overseas storage.

PART 6: PENALTIES AND ENFORCEMENT

The Privacy Commissioner can:

- Investigate complaints from individuals
- Issue compliance notices requiring specific action
- Refer cases to the Human Rights Review Tribunal

The Tribunal can award damages of up to **$350,000** for interference with privacy. Criminal penalties apply for misleading the Commissioner or obstructing investigations.

The Act also creates a tort of interference with privacy, meaning individuals can sue directly for serious privacy breaches in civil proceedings.

GETTING HELP

Privacy Act compliance for NZ SMEs does not need to be overwhelming. Good Security provides:

- **Personal Data Inventory** — Map your personal data flows and build your register
- **Privacy Impact Assessment** — Assess privacy risks before launching new products or processes
- **Privacy Breach Readiness** — Build your breach response capability before you need it
- **IPP 3A Compliance** — Map your indirect collection sources and establish notification processes
- **IPP 12 Compliance** — Assess your overseas data flows and document your cross-border disclosure arrangements
- **Policy Suite** — Privacy policy, data handling procedures, and staff guidance documents

Book a free 30-minute health check at https://goodsecurity.co.nz/health-check