

Important Changes to New Zealand's Privacy Laws

New Zealand privacy laws are set to change on **1 December 2020** under the new Privacy Act 2020.

To prepare for 1 December, all businesses should start reviewing and updating their privacy policy and data protection practices to ensure they meet the requirements under the new Privacy Act.

What does this mean for your business?

- **Mandatory reporting of serious data breaches.** You will be responsible for any privacy breach committed by anyone that you engage for the collection, storage, use or disclosure of personal information undertaken by your business. This is known as the "data lifecycle". A privacy breach that poses a risk of serious harm to an affected individual must be notified to the Privacy Commissioner and to the affected individual as soon as practical after you become aware of the breach.

You should implement processes for immediate privacy breach reporting

- Put in place a **privacy breach handling process** to enable timely management of a privacy breach, including steps to contain the breach, a framework to assist in determining whether the breach must be notified to the Privacy Commissioner and to affected individuals, and steps to capture learnings for future breach mitigation.
- Make sure all your contractors, agents and commercial partners that are engaged or involved in any part of the "data lifecycle" of your business are required to **immediately notify you of a privacy breach** so you can take action to contain the breach and assess if the breach must be notified.

- **Mandatory compliance with Privacy Commissioner's directions.** For serious or repeated breaches of the new Privacy Act 2020, the Privacy Commissioner can direct a business to comply with the Act, including directing a business to provide an individual with access to his or her personal information.

You should appoint a Privacy Officer

- **Appoint a privacy officer** who is responsible for upholding privacy within your business. This can be you or one of your employees.

You should put in place privacy management processes

- Implement **systems and procedures covering how your business will collect, store, use and disclose personal information.** Your privacy officer should be responsible for implementing the policy and regularly reviewing and updating it.
- Implement an **internal data access process** so privacy requests can be actioned within 20 working days.
- Ensure this is **matched** with the data access arrangements you have with your data service provider, especially if it is an overseas provider.

- **Greater controls on the sharing of personal information overseas.** If you need to share your customers' personal information with overseas companies, you can only do so if:
 - your customer consents; and
 - the overseas company receiving the personal information will protect the data in a way that is consistent with New Zealand privacy laws.

You should obtain your customers' consent.

- Review and update your **privacy policy** so that your customers are clearly informed that their personal information will be transferred overseas and the reasons for the transfer (e.g., data storage, provision of services, etc).

You should ask how your customers' personal information will be protected.

- Conduct **due diligence** on the overseas company that you wish to share your customers' personal information with.

- Does the overseas company operate in countries like the EU or Australia with similar privacy laws to New Zealand?
- Does it have a global reputation for taking privacy seriously?
- Has it been in the gun for privacy breaches in the past?
- Update your contracts so that any overseas contractor, agent or commercial partner that is engaged or involved in the “data lifecycle” of your business is required to **comply with New Zealand privacy standards** (or similar).

What are the risks if it all goes wrong?

- **Reputational loss.** The Privacy Commissioner may publicly identify a business that breaches the Privacy Act 2020. This could cause your customers to lose confidence in your business.
- **Criminal liability.** There are now a range of consequences for breaching the Privacy Act, including criminal liability for both the company and its directors, with fines of up to NZD\$10,000.
- **Class action.** Class actions for privacy breaches are now permitted. If successful, each member of the class action may be awarded up to NZD\$350,000.

Let us help you navigate this complex area

Data can be one your most valuable assets. But so is customer trust and confidence. The global movement behind greater data protection for individuals is ultimately driven by customer demand that their personal information is safeguarded throughout the entire lifecycle of collection, storage, use and disclosure.

Protecting your customer’s privacy is not only a legal requirement; it is a business-critical one.

Call us for a chat on how we can protect your business interests.

Data protection and privacy specialists



Tina Liu
 Senior Associate and Privacy Specialist
Tina.liu@tompkinswake.co.nz



Robert Bycroft
 Special Counsel and Privacy Specialist
Robert.bycroft@tompkinswake.co.nz