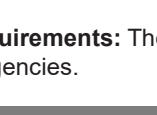
Data. Protection. Adding Value.

Data Protection Laws - New Zealand

Legislation

The principal privacy legislation is the Privacy Act 2020 (Privacy Act).
Scope: The Privacy Act applies to any person, business, and organisation (referred to as an 'agency') in relation to any action taken in respect of 'personal information' (information about an identifiable individual). The Privacy Act applies to New Zealand agencies, as well as overseas agencies that carry on business in New Zealand (regardless of where the overseas agency is based, and regardless of whether the overseas agency receives monetary payment for the supply of goods or services).
Sectoral Law Carve-Outs/Exemptions: Exemptions include Courts and Tribunals (where the information is related to its judicial functions), News Media (in relation to news activities) and Members of Parliament. In addition, individuals processing personal information solely in relation to their personal or domestic affairs are exempt.

Risk Level: Medium



Supervisory Authority

Supervisory Authority: The Office of the Privacy Commissioner (OPC) is the supervisory authority and has a range of functions under the Privacy Act, including investigating privacy related complaints and breaches, monitoring or enforcing compliance with the Privacy Act, making public statements regarding privacy related matters, helping to build privacy awareness, and issuing codes of practice for specific industries or sectors.

Registration/Approval Requirements: There are no registration / approval requirements for agencies.

General Data Privacy Principles

The Privacy Act contains 13 Privacy Principles which cover the collection, use and disclosure of personal information. Agencies must:

1. Only collect personal information where necessary for a lawful purpose.
2. Collect personal information directly from the individual concerned.
3. Take reasonable steps to make sure that the individual is made aware of a number of key facts.
4. Only collect personal information in ways that are lawful, fair and not unreasonably intrusive.
5. Ensure there are reasonable security safeguards in place to prevent loss, misuse or disclosure of personal information.
6. Provide individuals with the right to request access to their personal information.
7. Provide individuals with the right to request correction of their personal information.
8. Take reasonable steps to check personal information is accurate, complete, relevant, up to date and not misleading.
9. Not keep personal information for longer than necessary.
10. Only use personal information for the purpose they collected it.
11. Only disclose personal information in limited circumstances.
12. Only send personal information overseas if the information will be adequately protected.
13. Only assign a unique identifier to individuals where it is necessary for operational functions.

Enforcement

Enforcement (Fines, Criminal Penalties): The OPC does not have any ability to issue fines or bring prosecutions. There are criminal offences in the Privacy Act (punishable on summary conviction with a fine not exceeding NZ$10,000). For example, it is an offence to obstruct or hinder the OPC in the exercise of its powers under the Privacy Act, or to destroy any document containing personal information, knowing that a request has been made for it under the Privacy Act. In addition, it is an offence to fail to notify OPC of a notifiable privacy breach (fine not exceeding NZ$10,000).

Remedies for Individuals: The OPC will often try to settle a Privacy Act complaint by mediation. Where it is not resolved, the complaint may be referred to the Director of Human Rights Proceedings, or the complainant can file proceedings with the Human Rights Review Tribunal on his/her own account. The Tribunal can award various remedies, including damages up to a maximum of NZD$350,000 (approx €193,000).

Data Processing

Legal Basis for Processing: Before collecting information, an agency must have identified a legal purpose for the collection, connected to the agency's functions or activities.

Sensitive Personal Data: The Privacy Act does not contain a definition of sensitive personal data. However, the OPC has guidance that outlines how sensitive personal information should be handled. It lists health, genetic, biometric and financial information, as well as the personal information of children and young people as sensitive personal information.

The Privacy Act is supplemented by Codes of Practice in relation to specific sectors (for instance, the Health Information Privacy Code).

Transparency Requirements

The agency must provide the following transparency information to the individual:

- The fact that their personal information is being collected;
- The purpose for which the information is being collected;
- The intended recipients of the information;
- The name and address of the agency collecting the information and the agency holding the information;
- Whether the collection is authorised or required by law;
- Whether the supply of the information is voluntary or mandatory and the consequences if not provided;
- The right of the individual to access and correct personal information.

pwc

Individual Rights

Under the Privacy Act, individuals have the following rights:

- Right to access their personal information, subject to withholding grounds;
- Right to correction of their personal information. If the agency is not willing to correct the information as requested, it must attach the individual's statement of correction to the contested information, so that it can be read alongside it.

Security & Data Breaches

Security Requirements: Under the Privacy Act, agencies must implement such security safeguards as are reasonable in the circumstances to protect the personal information from misuse, interference, and loss; as well as unauthorised access, modification, or disclosure.

Data Breaches: The Privacy Act defines a privacy breach as the unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, the personal information; or an action that prevents the agency from accessing the information on either a temporary or permanent basis (for example,. where it is encrypted by ransomware).

A "notifiable data breach" is where the privacy breach either has caused or is likely to cause serious harm (e.g. physical harm, financial fraud, family violence, and/or psychological harm). Where a "notifiable privacy breach" occurs, the organisation must notify the OPC within 72 hours, and notify the individuals concerned as soon as reasonably practicable.

Other Business Obligations

Data Protection Officer: Under the Privacy Act, every agency is required to appoint a privacy officer.
Risk Assessments: The Privacy Act does not require the completion of the Privacy Impact Assessments (PIAs). However, OPC strongly encourages agencies to do so.
Audits: The Privacy Act does not require privacy audits. However, when requested to do so by an agency, OPC has the ability to conduct a Privacy Act audit of that agency.
Record Keeping: There are no specific record keeping requirements required by the Privacy Act.
Trainings: There are no specific training requirements under the Privacy Act. However, the OPC recommends that a privacy officer should provide privacy training to other staff at the agency.

Service Providers & Cross-Border Transfers

Service Provider Arrangements: The Privacy Act does not contain specific rules regarding service provider arrangements. However, the Act does specify that where an agency appoints a service provider to process personal information on its behalf, the agency will remain the responsible party under the Privacy Act.

Cross-Border Data Transfers: Before transferring personal information cross-border, the agency must either believe on reasonable grounds that the overseas recipient is subject to privacy laws that provide comparable safeguards to the New Zealand Privacy Act; or the recipient is required to protect the information in a way that overall provides comparable safeguards to the Privacy Act (for example, pursuant to contract). If the overseas jurisdiction does not offer comparable safeguards (and appropriate contract terms cannot be put in place), the individual concerned must be fully informed that their information may not be adequately protected and must expressly authorise the relevant transfer.

Localisation Requirements: There is no general requirement to store personal information exclusively in New Zealand.

Other/To Watch

Privacy Act Amendment Bill: This Bill will establish a new Privacy Principle 3A. This will require agencies that collect personal information about an individual from a source other than the individual concerned, to make the individual aware of the fact of collection and the lawful purpose for the collection, as part of transparency information.

Consumer & Product Data Bill: This draft Bill proposes the introduction of new "consumer data rights" to consumers and small businesses, in order to access and share their data with trusted third parties.

Let's connect to discuss how we can help:

Polly Ralph
Privacy & Data Protection Law Lead
Director, PwC Legal New Zealand

+64 27 3742031
polly.k.ralph@pwc.com