NEW ZEALAND

LAW

The Privacy Act 1993 (Act) governs how agencies collect, use, disclose, store, retain and give access to personal information. The Act gives the Privacy Commissioner the power to issue codes of practice that modify the operation of the Act in relation to specific industries, agencies, activities or types of personal information. The following codes are currently in place:

- Credit Reporting Privacy Code
- Health Information Privacy Code
- Justice Sector Unique Identifier Code
- Superannuation Schemes Unique Identifier Code
- Telecommunications Information Privacy Code
- Civil Defence National Emergencies (Information Sharing) Code

Enforcement is through the Privacy Commissioner.

A Privacy Amendment Bill was introduced to New Zealand’s parliament in 2018. If enacted it will include stronger powers for the Privacy Commissioner, mandatory reporting of privacy breaches, new offenses and increased fines. Timing and final content are not yet known, but the bill is expected to become law during 2019. The Privacy Commissioner has requested further amendments to the bill.

DEFINITIONS

Definition of personal data

Personal information under the Act is defined as information about an identifiable individual and includes information relating to a death that is maintained by the Registrar General pursuant to the Births, Deaths, Marriages, and Relationships Registration Act 1995, or any former Act.

Definition of sensitive personal data

Although no differentiation is made between how different types of personal information are to be treated under the Act, the codes of practice issued by the Privacy Commissioner may modify the operation of the Act for specific industries, agencies, activities and types of personnel information.

Definition of agency
Agency is defined under the Act as any person or body of persons, whether corporate or unincorporated, and whether in the public sector (including government departments) or the private sector. Certain bodies are specifically excluded from the definition.

**NATIONAL DATA PROTECTION AUTHORITY**

The Privacy Commissioner’s Office

Level 4
109-111 Featherston Street
Wellington 6143
New Zealand

T +64 474 7590
F +64 474 7595

enquiries@privacy.org.nz
www.privacy.org.nz

**REGISTRATION**

There is no obligation on agencies to notify the Privacy Commissioner that they are processing personal information. However, the Privacy Commissioner may require an agency to supply information for the purpose of publishing or supplementing a directory or to enable the Privacy Commissioner to respond to public enquiries in this regard.

The Privacy Commissioner may from time to time publish a directory of personal information processing activities including the following:

- The nature of any personal information held by an agency
- The purpose for which personal information is held by an agency
- The classes of individuals about whom personal information is held by an agency
- The period for which personal information is held by an agency
- The individuals entitled to access personal information held by an agency and the conditions relating to such access
- Steps to be taken by an individual wishing to obtain access to personal information held by an agency

**DATA PROTECTION OFFICERS**

The Act requires each agency to appoint within that agency, one or more individuals to be a privacy officer. The privacy officer’s responsibilities include the following:

- The encouragement of compliance with the personal information privacy principles contained in the Act
- Dealing with requests made to the agency pursuant to the Act
- Working with the Privacy Commissioner in relation to investigations relating to the agency
- Ensuring compliance with the provisions of the Act

Provided the person appointed a privacy officer is within the agency, that person does not have to be a New Zealand citizen or reside in New Zealand.
Failure to appoint a privacy officer or obstructing or hindering the Privacy Commissioner is an offense under the Act.

**COLLECTION & PROCESSING**

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the following 12 information privacy principles:

- The personal information is needed for a lawful purpose connected with the agency’s work
- The personal information is collected directly from the relevant person (unless a relevant exception applies as set forth below)
- Before the personal information is collected, the agency has taken reasonable steps to ensure that the person knows that the information is being collected; the purpose for which it is being collected; the intended recipients; the name and address of the agency collecting and holding the information; if the information is authorized or required by law, the applicable law and the consequences if the requested information is not provided; and that the person concerned may access and correct the information
- The personal information is not collected in an unlawful or unfair way or in a way that unreasonably invades a person’s privacy
- The personal information must be kept reasonably safe from being lost, accessed, used, modified or disclosed to unauthorized persons
- If the personal information is readily retrievable, the relevant person is entitled to know whether information is held and to have access to it
- The relevant person is entitled to request correction of the personal information. If the agency will not correct the information, the person may provide a statement of the correction sought to be attached to the personal information
- Before it is used, the agency must ensure that the personal information is accurate, up-to-date, complete, relevant and not misleading
- The personal information may not be kept for any longer than it is needed
- Subject to certain exceptions, personal information collected for one purpose may not be used for another purpose
- An agency must not disclose personal information to another person, body or agency except in specific circumstances
- An agency may only assign a unique identifier to an individual if it is needed for the agency to carry on its work efficiently and may not assign a unique identifier to an individual if the same identifier is used by another agency

Personal information does not need to be collected directly from the relevant person if:

- The personal information is publicly available
- The relevant person authorizes collection of the personal information from someone else
- Non-compliance would not prejudice the interests of the relevant individual
- The personal information is being collected for a criminal investigation, enforcement of a financial penalty, protection of public revenue or the conduct of court proceedings
- Compliance would prejudice the purpose of the collection of the personal information or is not practical in the circumstances
- The personal information will be used in a way which will not identify the person concerned

**TRANSFER**

An agency should not disclose personal information to another entity unless the disclosure of the information is one of the purposes in connection with which the information was obtained or is directly related to the purposes in connection with which
the information was obtained. Care must be taken that all safety and security precautions are met to ensure the safeguarding of that personal information to make certain that it is not misused or disclosed to any other party.

The Privacy Commissioner is given the power to prohibit a transfer of personal information from New Zealand to another state, territory, province or other part of a country (State) by issuing a transfer prohibition notice (Notice) if it is satisfied that information has been received in New Zealand from one State and will be transferred by an agency to a third State which does not provide comparable safeguards to the Act and the transfer would be likely to lead to a contravention of the basic principles of national application set out in Part Two of the Organisation for Economic Co-operation and Development (OECD) Guidelines, which include:

- The collection limitation principle (there should be limits to the collection of personal data)
- The data quality principle (personal data should be accurate, complete and kept up to date)
- The purpose specification principle (the purposes for which personal data are collected should be specified)
- The use limitation principle (personal data should not be used otherwise than in accordance with the purpose specification principle, except with the consent of the data subject or by authority of law)
- The security safeguards principle (personal data should be protected by reasonable security safeguards)
- The openness principle (there should be a general policy of openness about developments, practices and policies relating to personal data)
- The individual participation principle (individuals should have the right to obtain confirmation of whether a data controller holds their personal data, to have that data communicated to him/her, to be given reasons if a request for that data is denied and to be able to challenge that denial, and to challenge data relating to him/her and have that data erased, rectified, completed or amended if successful)
- The accountability principle (a data controller should be accountable for complying with the above principles)

In considering whether to issue a Notice, the Privacy Commissioner must have regard to whether the proposed transfer of personal information affects, or would be likely to affect any individual, the desirability of facilitating the free flow of information between New Zealand and other States, and any existing or developing international guidelines relevant to trans-border data flows.

On December 19, 2012 the European Commission issued a decision formally declaring that New Zealand law provides a standard of data protection that is adequate for the purposes of EU law. This decision means that personal data can flow from the 27 EU member states to New Zealand for processing without any further safeguards being necessary.

Following the decision in the Schrems case, where the European Commission’s decision to recognize the safe harbor agreement with the USA was invalidated, there have been calls to review New Zealand’s adequacy status, primarily due to New Zealand’s membership with the Five Eyes network. However, to date this has not been acted upon by the European Commission.

SECURITY

An agency that holds personal information shall ensure that the information is kept securely and protected by such security safeguards as are reasonable in the circumstances to protect against:

- Loss
- Access, use, modification or disclosure, except with the authority of the agency
- Other misuse or unauthorized disclosure
If it is necessary for the information to be given to a person in connection with the provision of a service to the agency, everything reasonably within the power of the agency must be done to prevent unauthorized use or unauthorized disclosure of the information.

**BREACH NOTIFICATION**

There is no mandatory requirement in the Act to report an interference with privacy. There will be a mandatory requirement to report data breaches once the Privacy Amendment Bill is enacted, which is expected to occur during 2019.

Any person may make a complaint to the Privacy Commissioner alleging an action is, or appears to be, an interference with the privacy of an individual. For there to be an interference with privacy, there must be a breach of the law and the breach must lead to financial loss or other injury, an adverse effect on a person’s right, benefit, privilege, obligation or interest or significant humiliation, loss of dignity or injury to a person’s feelings. There is no requirement to show harm in a complaint about access to, or correction of, personal information. An unauthorized disclosure of personal information is sufficient to breach the Act.

**ENFORCEMENT**

In New Zealand, the Privacy Commissioner is responsible for investigating a breach of privacy laws. The Privacy Commissioner has powers to enquire into any matter if the Privacy Commissioner believes that the privacy of an individual is being, or is likely to be, infringed. The Privacy Commissioner will primarily seek to settle a complaint by conciliation and mediation. If a complaint cannot be settled in this way, a formal investigation may be conducted so that the Privacy Commissioner may form an opinion on how the law applies to the complaint. The Privacy Commissioner’s opinion is not legally binding but is highly persuasive. The Privacy Commissioner is not able to issue a formal ruling or determination and cannot begin prosecution proceedings or impose a fine.

If the Privacy Commissioner is of the opinion that there has been an interference with privacy, the Privacy Commissioner may refer the matter to the Director of Human Rights who may then in turn decide to take the complaint to the Human Rights Review Tribunal. The Tribunal will hear the complaint afresh and its decision is legally binding. It can award damages for breaches of privacy.

**ELECTRONIC MARKETING**

The Act does not differentiate between the collection of and use of any personal information for electronic marketing or other forms of direct marketing.

The Unsolicited Electronic Messages Act 2007:

- Prohibits unsolicited commercial electronic messages (this includes email, fax, instant messaging, mobile / smart phone text (TXT) and image-based messages of a commercial nature – but does not cover Internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand)
- Requires commercial electronic messages to include accurate information about who authorized the message to be sent
- Requires a functional unsubscribe facility to be included so that the recipient can instruct the sender not to send the recipient further messages
- Prohibits using address-harvesting software to create address lists for sending unsolicited commercial electronic messages

The Marketing Association of New Zealand has a code of practice for direct marketing which governs compliance by members of the principles of the code. The code establishes a ‘Do Not Call’ register to which anyone not wanting to receive any direct marketing can register.

**ONLINE PRIVACY**

Other than compliance with the Act, no additional legislation deals with the collection of location and traffic data by public electronic communications services providers and use of cookies (and similar technologies). The New Zealand Privacy
Commissioner has general guidelines on protecting online privacy.

**KEY CONTACTS**

**DLA Piper New Zealand**

www.dlapiper.co.nz/

*John Hannan*
Partner
T +64 9 399 3843
john.hannan@dlapiper.com

**DATA PRIVACY TOOL**

You may also be interested in our Data Privacy Scorebox to assess your organization’s level of data protection maturity.