DATA PROTECTION LAWS OF THE WORLD

New Zealand

NEW ZEALAND

Last modified 18 January 2024

LAW

The Privacy Act 2020 (Act) and its Information Privacy Principles (IPPs) govern 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; and
- Civil Defence National Emergencies (Information Sharing) Code.

The Privacy Commissioner is also currently considering introducing a new code to regulate the collection of biometric information and anticipates that a biometrics code exposure draft will be issued in early 2024. The exposure draft will propose new rules for agencies who want to collect or use biometric personal information. There will be public consultation before the code is finalised.

Enforcement is through the Privacy Commissioner who has the power to investigate any action which appears to interfere with the privacy of an individual and can do so either on a complaint made to the Privacy Commissioner or on the Privacy Commissioner’s own initiative. The Privacy Commissioner can also issue compliance notices requiring agencies to do or refrain from doing something in order to comply with the Act.

Under the Act, an agency can be any person or body of persons, whether corporate or unincorporated, and whether in the public sector or in the private sector.

The Act has an extraterritorial scope — it applies to any actions taken by an overseas organisation in the course of carrying on business in New Zealand, regardless of where the information is or was collected or held and where the person to whom the information relates is located. An organisation may still be treated as carrying on business in New Zealand regardless of whether or not it has a physical place of business in New Zealand, charges any monetary payment for goods or services within New Zealand, or makes a profit from its business in New Zealand. For organisations subject to the Act (whether New Zealand agencies or overseas agencies), it is irrelevant where the personal information was collected, where it is held, or where the individual is or was located (i.e. the Act can extend to personal information collected overseas about foreign data subjects).

In September 2023, the New Zealand government released the Privacy Amendment Bill (Bill), which, if passed, will amend the Privacy Act. The Bill is currently in its first reading however, it is likely to commence into the Select Committee process in 2024. The main amendments to the Act will be the introduction of a new IPP 3A, requiring organisations that

collect personal information 'indirectly' (i.e. not directly from the relevant individual) to provide the individual with information about the processing of their data. Currently, under IPP 3, the Act requires organisations who collect personal information directly from the individual to ensure the individual is aware of certain details, such as the fact of collection, the purposes for which the information will be used, the intended recipients and the individual's right to request access to and correction of their personal information.

IPP 3A will require agencies collecting personal information from a source other than from the individual concerned to take reasonable steps to ensure that the individual is aware of the same information.

The Bill includes certain exceptions to complying with IPP 3A including where the individual has previously been made aware of the organisation's collection of their personal information, or compliance with IPP 3A is not reasonably practicable in the circumstances.

The Bill is set to come into force on 1 June 2025 and the Bill clarifies that IPP 3A will not have retrospective effect.

In September 2023, the Privacy Commissioner issued (non–binding) guidance on the application of the Act's IPPs to the use of AI tools in New Zealand (the Guidance). The Guidance is consistent with key themes from developing international regulations (e.g. the importance of transparency and explainability; accuracy; robustness and security; accountability; and human values and fairness). The Privacy Commissioner has recommended, among other things, that while not mandatory under the Act, it is generally best practice to undertake a Privacy Impact Assessment at the outset of an AI project. The Guidance also recognises an important element which is unique to New Zealand – the need to consider te ao Māori perspectives on privacy (broadly, *te ao Māori* is the Māori worldview including *tikanga Māori - Māori* customs and protocols). Specific concerns identified in the Guidance include:

- bias from systems developed overseas that do not work accurately for Māori;
- collection of Māori information without work to build relationships of trust, leading to inaccurate representation of *Māori taonga* that fail to uphold *tapu and tikanga*; and
- exclusion from processes and decisions of building and adopting AI tools that affect *Māori whānau, hapū, and iwi*, including use of these tools by the public sector.

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

The Act does not include a concept of 'sensitive personal data', and there is no differentiation between how different types of personal information are to be treated under the Act. However, the Privacy Commissioner has issued (non–binding) guidance defining sensitive personal information as information about the individual that has some real significance to them, is revealing of them, or generally relates to matters that an individual might wish to keep private. This can be contrasted with routine or mundane information that is about a person but is either not particularly revealing or does not reveal information that is very intimate or “private”. The Privacy Commissioner has indicated that information about a person’s race, ethnicity, gender or sexual orientation, sex life, health, disability, age, religious, cultural or political beliefs, activities or memberships will generally be considered sensitive in nature.

Because the Act does not include a concept of sensitive personal data, there are no specific statutory obligations attracting to more sensitive information. However, the Privacy Commissioner's guidance states that agencies have a higher standard of care when they collect or hold sensitive information. While the Act does not specify special procedures for information that is sensitive, the obligations on agencies are stronger with respect to sensitive information and they will be held to a higher standard

of accountability. For example, IPP 5 requires agencies to protect personal information with security safeguards that are reasonable in the circumstances — there will be a higher bar for what is considered reasonable if the information to be protected is sensitive in nature.

Additionally, 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. The Privacy Commissioner is currently considering introducing a new code to regulate biometric information, which the Privacy Commissioner considers to be particularly sensitive information and requires careful assessment before use.

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 13
15 Shortland Street
Auckland 1010
New Zealand

Telephone

+64 9 302 8680
0800 803 909

Email

enquiries@privacy.org.nz

Website

privacy.org.nz

REGISTRATION

There is no obligation on agencies to register or notify the Privacy Commissioner that they are processing personal information.

DATA PROTECTION OFFICERS

The Act requires each agency to appoint one or more individuals to be a privacy officer. The privacy officer may be within or external to the agency (i.e. the privacy officer role may be outsourced to a third party) and does not need to be a New Zealand citizen or reside in New Zealand.

The privacy officer's responsibilities include the following:

- The encouragement of compliance with the personal IPP 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; and
- Ensuring compliance with the provisions of the Act.

COLLECTION & PROCESSING

Subject to specific exceptions, agencies may collect, store and process personal information in accordance with the 13 IPPs summarised below.

IPP 1 – Purpose of collection of personal information

An agency must not collect personal information other than for a lawful purpose connected to the agency's functions, and only if the collection of the information is necessary for that purpose.

IPP 2 – Source of personal information

An agency must collect information directly from the relevant individual, unless one of the specified exceptions applies, which include if collection from the individual is not practical in the circumstances, if collection from a third party would not prejudice the interests of the individual, or if the information is publicly available.

IPP 3 – Collection of personal information from subject

Before collecting personal information, an agency has to make the relevant individual aware of certain things, such as the fact that information is being collected, the purposes for which it will be used, and the right to access and request correction of personal information. This is typically done by way of a privacy policy. There are several exceptions where the person collecting information would not need to comply with IPP 3, including where compliance is not reasonably practicable in the circumstances.

IPP 4 – Manner of collection of personal information

Agencies cannot collect personal information by unlawful or unfair means, or in a manner that intrudes to an unreasonable extent upon the personal affairs of the individual concerned. Particular care must be taken when collecting personal information from children or young persons.

IPP 5 – Storage and security of personal information

Agencies must ensure personal information is protected by reasonable security safeguards against loss and unauthorised access, use, modification or disclosure or other misuse. If it is necessary to give personal information to another person (e.g. a service provider), an agency must do everything reasonably within its power to prevent unauthorised use or disclosure of that information.

IPP 6 – Access to personal information

Where an agency holds personal information about an individual, subject to certain exceptions, if requested by the individual, the agency must confirm whether it holds the information and grant the individual access to it. The exceptions include where the information is not readily retrievable or:

- the refusal is for the protection of the health, safety or similar of an individual;
- in an employment context, the information is evaluative (e.g. compiled for the purpose of determining the suitability of an individual for employment) and disclosure would breach an implied promise that was made to the person who supplied the information;
- the information needs protecting because it would involve disclosure of a trade secret or be likely to unreasonably prejudice the commercial position of the person who supplied the information, unless the public interest in disclosure outweighs the withholding of the information;
- the information does not exist or cannot be found;
- the disclosure would involve the unwarranted disclosure of the affairs of another individual;
- the disclosure would breach legal professional privilege; or
- the request is frivolous or vexatious, or the information requested is trivial.

IPP 7 – Correction of personal information

An individual can request an agency to correct information the agency holds about the individual, or attach a statement of a correction sought but not made. If an agency has corrected personal information or attached a statement of a correction sought but not made, if reasonably practicable, it will inform each person or entity to whom it has disclosed that information of that correction or statement. The agency must inform the individual of any action taken as a result of the individuals request.

IPP 8 – Accuracy of personal information to be checked before use or disclosure

Agencies must take reasonable steps to ensure personal information they hold is accurate, up to date, complete, relevant, and not misleading.

IPP 9 – Agency not to keep personal information for longer than necessary

Agencies must not keep personal information for longer than is required for the purposes for which the information may lawfully be used.

IPP 10 – Limits on use of personal information

Agencies must not use personal information obtained in connection with one purpose for any other purpose unless the agency reasonably believes:

- the source of the information is publicly available and it would not be unfair or unreasonable to use that information;
- the use of the information for the other purpose is authorised by the relevant individual;
- non–compliance is necessary to avoid prejudice to the maintenance of the law by any public sector agency:
    - for the enforcement of a law imposing a pecuniary penalty;
    - for the protection of public revenue; or
    - for the conduct of proceedings before a court or tribunal;
- the use of the information for the other purpose is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual;
- the other purpose is directly related to the purpose for which the information was obtained, or the information is used in a form where the individual is not identified, or is used for statistical or research purposes and will not be published in a form where the individual could reasonably be expected to be identified.

IPP 11 – Limits on disclosure of personal information

Agencies must not disclose personal information for any purpose other than the purpose for which it was collected or a purpose directly related to the purpose for which it was collected unless the agency reasonably believes:

- the source of the information is publicly available and it would not be unfair or unreasonable to disclose that information;
- the disclosure is to the relevant individual;
- the disclosure is authorised by the relevant individual;
- non-compliance is necessary:
    - to avoid prejudice to the maintenance of the law by any public sector agency;
    - for the enforcement of a law imposing a pecuniary penalty;
    - for the protection of public revenue; or
    - for the conduct of proceedings before a court or tribunal;
- the disclosure of the information is necessary to prevent or lessen a serious threat to public health or safety, or the life or health of an individual;
- the disclosure is necessary to enable an intelligence and security agency to perform any of its functions;
- the disclosure is necessary to facilitate the sale or other disposition of a business as a going concern; or
- the information is to be used in a form where the individual is not identified, or is used for statistical or research purposes and will not be published in a form where the individual could reasonably be expected to be identified.

IPP 12 – Disclosure to an overseas person

Agencies must not disclose personal information to a foreign person or entity unless the agency reasonably believes:

- the relevant individual authorises the disclosure after being informed by the agency that the foreign person or entity may not be required to protect the information in a way that provides comparable safeguards to those in the Act;
- the foreign person or entity is carrying on business in New Zealand and the agency reasonably believes that, in relation to the information being disclosed, the foreign person or entity is subject to the Act;
- the foreign person or entity is subject to privacy laws that provide comparable safeguards to those in the Act;
- the foreign person or entity is a participant in a prescribed binding scheme;
- the foreign person or entity is subject to privacy laws of a prescribed country; or
- the foreign person or entity is required to protect the information in a way that provides comparable safeguards to those in the Act (for example, pursuant to contractual clauses). New Zealand's Privacy Commissioner has released model contractual clauses that can be used to satisfy these exceptions, but it is not mandatory to use these exact provisions.

IPP 13 – Unique identifiers

Agencies can only assign 'unique identifiers' to an individual if it is necessary to enable the agency to carry out one or more of its functions efficiently. The agency must not assign an individual a unique identifier that it knows has been assigned to that individual by another agency unless the unique identifier is being used for statistical or research purposes only. Additionally, the agency must take reasonable steps to ensure that unique identifiers are only assigned to individuals whose identities are clearly established and that the risk of the unique identifiers being misused is minimised. An agency must not require an individual to disclose any unique identifier assigned to them unless the disclosure is one of the purposes, or directly related to one of the purposes, for which that unique identifier was assigned.

TRANSFER

Generally, 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.

Transfer of personal information to another agency to hold as the transferring agency's agent (e.g. for safe custody or processing) is not considered a disclosure of the information for the purposes of the Act.

Agencies must not disclose personal information to a foreign person or entity unless the agency reasonably believes:

- the relevant individual authorises the disclosure after being informed by the agency that the foreign person or entity may not be required to protect the information in a way that provides comparable safeguards to those in the Act;
- the foreign person or entity is carrying on business in New Zealand and the agency reasonably believes that, in relation to the information being disclosed, the foreign person or entity is subject to the Act;
- the foreign person or entity is subject to privacy laws that provide comparable safeguards to those in the Act;
- the foreign person or entity is a participant in a prescribed binding scheme;
- the foreign person or entity is subject to privacy laws of a prescribed country; or
- the foreign person or entity is required to protect the information in a way that provides comparable safeguards to those in the Act (e.g. pursuant to contractual clauses). New Zealand's Privacy Commissioner has released model contractual clauses that can be used to satisfy these exceptions, but it is not mandatory to use these exact provisions.

Additionally, 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.

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 and Schrems II cases, there have been calls to review New Zealand's adequacy status, primarily due to New Zealand's membership with the Five Eyes network. In January 2024, the European Commission reviewed New Zealand's adequacy status. The review confirmed that New Zealand's adequacy status remains due to New Zealand's strengthened privacy legislation and clarification of certain privacy rules since the adoption of the initial adequacy decision, aligning it further with the EU framework.

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 that is not authorised by the agency, and other misuse.

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 unauthorised use or unauthorised disclosure of the information.

BREACH NOTIFICATION

Under the Act, any 'privacy breach' which it is reasonable to believe has caused or is likely to cause serious harm to an individual must be notified to the Privacy Commissioner and to the affected individuals.

A 'privacy breach' is any unauthorised or accidental access to, or disclosure, alteration, loss, or destruction of, personal information, or any action that prevents the agency from accessing the information on either a temporary or permanent basis.

When assessing whether a privacy breach is likely to cause serious harm, agencies must consider:

- any action taken by the agency to reduce the risk of harm following the breach;
- whether the personal information is sensitive in nature;
- the nature of the harm that may be caused to affected individuals;
- the person or body that has obtained or may obtain personal information as a result of the breach (if known);
- whether the personal information is protected by a security measure; and
- any other relevant matters.

Agencies must notify the Privacy Commissioner and affected individuals as soon as practicable after becoming aware of a notifiable privacy breach. The Privacy Commissioner has issued non-binding guidance that it expects to be notified within 72 hours of an agency discovering a notifiable privacy breach. If it is not reasonably practicable to notify an affected individual or each member of a group of affected individuals, an agency can give a public notice of the breach.

Notification to affected individuals is not required or can be delayed in certain circumstances. For example, notification to affected individuals can be delayed if the agency believes that a delay is necessary because notification or public notice may pose risks for the security of personal information held by the agency and those risks outweigh the benefits of informing affected individuals (for example, if notification of the breach would expose an unremedied security vulnerability).

Anyone who outsources services that involve data processing should be aware that the Act includes an express provision that anything relating to a notifiable privacy breach that is known by an agent is to be treated as being known by the principal agency. This is because the legislators consider that the principal agency should be responsible for informing individuals about a notifiable breach.

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.

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.

The Privacy Commissioner can also issue compliance notices requiring agencies to take certain actions, or stop certain activities, in order to comply with the Act. Compliance notices will describe the steps that the Privacy Commissioner considers are required to remedy non–compliance with the Act and will specify a date by which the agency must make the necessary changes. The Privacy Commissioner can also issue access directions requiring agencies to provide individuals access to their personal information.

It is an offence to:

- mislead an agency to access another individual's personal information;
- destroy personal information, knowing that a request has been made to access it;
- without reasonable excuse, obstruct, hinder, or resist the Privacy Commissioner or any other person in the exercise of their powers under the Act;
- without reasonable excuse, refuse or fail to comply with any lawful requirement of the Privacy Commissioner or any other person under the Act;
- give false or misleading statements to the Privacy Commissioner;
- represent directly or indirectly that a person holds any authority under the Act when they do not hold that authority; or
- fail to notify the Privacy Commissioner of a notifiable privacy breach.

The penalty for these offences is a fine of up to NZD 10,000.

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 include email, fax, instant messaging and text messages of a commercial nature – but do not cover Internet pop-ups or voice telemarketing) with a New Zealand link (messages sent to, from or within New Zealand);
- requires consent (which can be express, reasonably inferred, or deemed) from the recipient prior to sending commercial electronic messages;
- requires commercial electronic messages to include accurate information about who authorised 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; and
- 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/

Nick Valentine
Partner
T +64 9 916 3703
nick.valentine@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.