Privacy Act 2020- Part 2 – Introduction to Information Privacy Principles

Your privacy rights

All New Zealanders regardless of age or circumstance have privacy rights. The Privacy Act 2020 is the law that enforces those rights by setting out how organisations, government departments and businesses can collect, store, use and share your personal information.

Information Privacy Principles (IPP)

The Privacy Act has thirteen principles that businesses and organisations must follow when collecting, using, and storing your personal information. The principles are designed to ensure your personal information is protected and respected.

These principles are:

Principle 1 - Purpose for collection of personal information

Principle 1 states that organisations must only collect personal information if it is for a lawful purpose connected with their functions or activities, and the information is necessary for that purpose. This principle is about data minimisation.

If the personal information an agency is asking for isn't necessary to achieve something closely linked to the organisation's activities, they shouldn't be collecting it.

Principle 2 - Source of personal information - collect it from the individual

Principle 2 states that personal information should be collected directly from the person it is about. The best source of information about a person is usually the person themselves. Collecting information from the person concerned means they know what is going on and have some control over their information.

It won't always be possible to collect information directly from the person concerned so organisations can collect it from other people in certain situations. For instance:

- if the person concerned authorises collection from someone else
- if the information is collected from a publicly available source
- if collecting information from the person directly is not really practicable or would undermine the purpose of collection.

Sometimes, information can be collected from other sources for law enforcement and court proceedings.

Principle 3 - Collection of information from subject - what to tell the individual

Principle 3 means that organisations should be open about why they are collecting personal information and what they will do with it. This principle is about helping people understand the reasons you are collecting their information.

When an organisation collects personal information, it must take reasonable steps to make sure that the person knows:

- why it's being collected
- who will receive it
- whether giving it is compulsory or voluntary
- what will happen if the information isn't provided.

Sometimes there may be good reasons for not letting a person know about the collection – for example, if it would undermine the purpose of the collection to protect law enforcement investigations, or it's just not possible to tell the person.

Principle 4 - Manner of collection

Principle 4 states that personal information must be collected in a way that is lawful and seen as fair and reasonable in the circumstances.

What is fair depends a lot on the circumstances like the individual concerned (age and capacity) and the natural sensitivity of the information. Note that threatening, coercive, or misleading behaviour when collecting information from an individual could well be considered unfair.

If the law is broken when collecting information, then the information has been collected unlawfully.

What is fair also depends on the circumstances, such as the purpose for collection, the degree to which the collection intrudes on privacy, and the time and place it was collected.

Principle 5 - Storage and security of information

Principle 5 states that organisations must ensure there are safeguards in place that are reasonable in the circumstances to prevent loss, misuse or disclosure of personal information.

If an organisation has a serious privacy breach it must notify the Office of the Privacy Commissioner as soon as possible (within 72 hours).

Principle 6 - Access to personal information

Principle 6 states that people have a right to ask for access to their own personal information.

Generally, an organisation must provide access to the personal information it holds about someone if the person in question asks to see it.

People can only ask for information about themselves. The Privacy Act does not allow you to request information about another person, unless you are acting on that person's behalf and have written permission.

In some situations, an organisation may have good reasons to refuse a request for access to personal information. For example, the information may involve an unwarranted breach of someone else's privacy, or releasing it may pose a serious threat to someone's safety.

If a business or organisation fails to provide information to an individual, the Privacy Commissioner can issue an access direction requiring them to release the personal information.

Principle 7 - Correction of personal information

Principle 7 states that a person has a right to ask an organisation or business to correct information about them if they think it is wrong.

If an organisation does not agree that the information needs correcting, an individual can ask that an agency attach a statement of correction to its records, and the agency should take reasonable steps to do so.

Principle 8 - Accuracy of personal information

Principle 8 states that an organisation must check before using or disclosing personal information that it is accurate, up to date, complete, relevant and not misleading.

Principle 9 - Retention of personal information

Principle 9 states that an organisation should not keep personal information for longer than it is required for the purpose it may lawfully be used.

Principle 10 - Limits on use of personal information

Principle 10 means that organisations can generally only use personal information for the purpose it was collected, and there are limits on using personal information for different purposes.

Sometimes other uses are allowed, such as use that is directly related to the original purpose, or if the person in question gives their permission for their information to be used in a different way.

Principle 11 - Disclosure of personal information

Principle 11 means that an organisation may generally only disclose personal information for the purpose for which it was originally collected or obtained. Sometimes other reasons for disclosure are allowed, such as disclosure for a directly related purpose, or if the person in question gives their permission for the disclosure.

For instance, an organisation may disclose personal information when:

- disclosure is one of the purposes for which the organisation got the information
- the person concerned authorises the disclosure
- the information is to be used in a way that does not identify the person concerned
- disclosure is necessary to avoid endangering someone's health or safety
- disclosure is necessary to uphold or enforce the law.

Principle 12 - Disclosure outside New Zealand

Principle 12 sets rules around sending personal information to organisations or people outside New Zealand.

Principle 12 is a new principle in the Privacy Act 2020.

A business or organisation may only disclose personal information to another organisation outside New Zealand if they check that the receiving organisation:

- is subject to the Privacy Act because they do business in New Zealand
- will adequately protect the information, e.g. by using model contract clauses, or
- is subject to privacy laws that provide comparable safeguards to the Privacy Act

If none of the above criteria apply, a business or organisation may only make a cross-border disclosure with the permission of the person concerned. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act.

The goal is to make sure that the privacy protections that individuals can reasonably expect under New Zealand's Privacy Act continue to apply when their information is disclosed and used in a different country.

Principle 13 - Unique identifiers

Principle 13 sets restrictions on assigning identifying numbers and other unique identifiers to individuals. The principle states that an organisation can only assign unique identifiers to people when it is necessary for its functions.

Unique identifiers are individual numbers, references, or other forms of identification allocated to people by organisations as a way to uniquely identify the person to the organisation assigning the identifier. Examples include driver's licence numbers, passport numbers, IRD numbers, or National Health Index (NHI) numbers.

An organisation cannot assign a unique identifier to a person if that unique identifier has already been given to that person by another organisation. For example, this prevents the Government from giving you one personal number to use in all your dealings with government agencies.

However, an organisation can record (and use) a person's unique identifier so that they can communicate with another organisation about the individual.

Organisations must also take reasonable steps to protect unique identifiers from misuse and make sure they verify someone's identity before assigning a unique identifier.

For Further information please go to the following website:

https://www.privacy.org.nz

DISCLAIMER & ACKNOWLEDGEMENT: The Office of the Privacy Commissioner is the original creator of the material regarding privacy that is on this site and which they outline as being covered by a Creative Commons 'Attribution (BY)' Licence. This licence allows for copying, distributing and adapting this material on privacy for an organization's purposes; where ADL's purpose is to present this information on privacy for knowledge and assistance. This in no way suggests that the Office of the Privacy Commissioner endorses ADL or our website and the use of the material on privacy that is provided here.