



# A Marketers guide to the New Zealand Privacy Act

Updated March 2022

## Human Rights in New Zealand

Consumers around the world are demanding that Government, commerce and service providers recognise their rights of individual privacy. New Zealand has become a world leader in privacy legislation and many other countries have used our law as a model for their own regulation.

### **The Privacy Act 2020 Protects people, not organisations.**

The Privacy Act 2020 deals with the collection, storage and use of personal information about identifiable individuals and therefore principally affects consumer marketing.

As with all legislation, it is important to understand the motives of the select committee who introduced the bill, and the Ministry responsible. On the day the 1993 Act became law the Minister of Justice said, "The Act is not meant to inhibit normal commercial communication". That philosophy has been the underlying principle of the Privacy Commissioner and the Commission staff from day one.

Common sense and good business practice will be your most effective guide as you seek to comply with the 13 Privacy Principles which are at the heart of the legislation.

## **The Role of the Privacy Commission**

The Privacy Commission is the initial complaints authority and endeavours to settle any complaint before referring serious non-compliance to the (Human Rights) Complaints Review Tribunal. The Complaints Review Tribunal has the power to award damages for the interference of privacy of an individual up to a maximum of \$50,000.

## **The 13 Privacy Principles**

### **Principle 1: Purpose of collection of personal information**

This principle ensures that personal information can only be collected for a lawful purpose relevant to the organisation and must be necessary for the required purpose.

To comply you must ensure that any information collected is relevant for your business purpose (assuming your business is lawful!).

### **Principle 2: Source of personal information**

Information must be collected directly from the individual concerned except where:

- (a) the information is publicly available (such as business directory or website)
- (b) you are authorised by the individual (to collect it)

To comply with this Principle, you should endeavour to collect information directly from the individuals concerned. Otherwise, be sure that the information is publicly available or that the individual has authorised collection.

Marketers can buy, rent or exchange personal information, but it must be with the authority of the individual - refer Principle 11: Disclosure. Activities such as lead generation, member-get-member campaigns and personal referral campaigns are still possible as long as you practice full disclosure.

### **Principle 3: Collection of information directly from the individual concerned.**

Reasonable steps must be taken to make the individual aware of the following :

- (a) that the information is being collected
- (b) the purpose for which the information is being collected
- (c) who is going to receive the information
- (d) name and address of organisation collecting and holding the information, and
- (e) the individual's right to access and correct any information

To comply, make sure that when collecting information, you make clear who is collecting it, how it will be used, who is going to use it, who will hold or store it, and how it can be accessed or corrected by the individual concerned.

A simple privacy box on every information-gathering vehicle (website, order forms, competitions, coupons etc) is the most professional method. Here's an example of one used by the Marketing Association:

*Your Privacy: The Marketing Association collects your details to keep you informed about marketing matters including training, education and current issues. Your details are stored securely at our National Office and can only be accessed and used by members of the Marketing Association. You are welcome to contact us at any time to access and update your personal information or to opt out\* of receiving further communications from us P O Box 137266, Parnell, Auckland 1151, freephone 0800 347 328 or email [marketing@marketing.org.nz](mailto:marketing@marketing.org.nz).*

\* NB: The Privacy Act does not require an option to 'opt out'. However, the Marketing Association's Code of Practice for Direct Marketing does require you to provide an opt-out facility.

If you would like the wording of your Privacy Clause checked to make sure it complies with the requirements of Principle 3, email the Marketing Association – [contactus@marketing.org.nz](mailto:contactus@marketing.org.nz)

### **Principle 4: Manner of collection of personal information**

Information shall not be collected by unlawful or unfair means and shall not intrude to an unreasonable extent upon the personal affairs of the individual. To comply, ensure that only lawful and fair means are used to collect information. Avoid practices that may be interpreted as misleading, deceptive or unreasonable. Be transparent!

### **Principle 5: Storage and security of personal information**

Information must be protected against loss, unauthorised access, misuse and modification. You must take reasonable precautions to safeguard information. Access should be available only to people who are authorised to use the information.

NB: The Act requires every organisation holding personal information to appoint a Privacy Officer who will be responsible for compliance with the Privacy Principles within the organisation. If you have a customer database, **you are required to have a Privacy Officer.**

#### **Principle 6: Access to personal information**

Individuals are entitled to obtain from organisations confirmation of whether or not personal information is held and to access the information about themselves.

You should establish, document and implement procedures to handle enquiries from individuals and to provide information requested. Incorporate checks to ensure that information requests are bona fide.

#### **Principle 7: Correction of personal information**

Individuals have the right to request correction of their personal information. Take care to ensure that accurate information is held and that corrections are made promptly. (Sounds remarkably like a golden rule for data-driven marketing!).

#### **Principle 8: Accuracy of personal information**

The agency holding personal information must not use that information without taking steps to ensure it is accurate, up-to-date, complete, relevant and not misleading. Your database management procedures should include constant checks on information collection systems and updating methods. (Another golden rule!).

#### **Principle 9: Retention of information**

Personal information shall not be kept for longer than required for its lawful use.

You will need to develop a system to identify and carefully dispose of out-of-date information. How you ascertain what information should be kept and for how long is subjective. It will vary according to the relationship you have with the individual.

#### **Principle 10: Limits on use of personal information**

Personal information shall not be used for any purpose unrelated to that for which it was obtained unless the source of the information is a publicly available publication or the use of the information for another purpose was authorised by the individual concerned.

Be clear and up-front about the purpose(s) for which information is being collected. Obtain appropriate authorisation from individuals where it is intended to make extended use of personal information. Think and plan ahead for possible future extended uses of information and build these into your initial authorisation process. Try to ensure that your information systems enable you to separate individuals with different levels of authorisation.

### Principle 11: Disclosure

Personal information shall not be disclosed unless the disclosure is directly related to the reason for which the information was originally collected, or the source of the information is a publicly available document, or the disclosure is authorised by the individual concerned.

Ensure that any disclosure of personal information is directly related to the reason for which the information was originally collected, or that the disclosure was/is authorised by the individual(s) concerned. If you intend to rent, sell or lend your list, you must advise people up-front.

### Principle 12: Cross-border disclosure

Principle 12 sets rules around sending personal information to organisations or people outside New Zealand (cross-border disclosure).

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

- is subject to the Privacy Act because they do business in New Zealand.
- is subject to privacy laws that provide comparable safeguards to the Privacy Act.
- agrees to adequately protect the information, e.g. by using [model contract clauses](#).
- is covered by a binding scheme or is subject to the privacy laws of a country prescribed by the New Zealand Government.

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.

### Principle 13 Unique identifiers

You should not assign a unique identifier to an individual unless it is necessary to carry out the lawful functions of your business.

A unique identifier, such as a customer number, is acceptable where there is a large customer base. However, the same unique identifier cannot be applied to an individual by more than one organisation.

## What Happens if you Transgress?

Years of experience with the Act has shown us that it is not difficult to live with. Complaints about Marketers have been few and far between. Those which have been upheld have usually been settled by an apology or small monetary compensation.

Remember that for a complaint against you to be upheld there should be evidence that the breach has caused the individual "loss, detriment, damage or injury", or has caused "humiliation, loss of dignity or injured feelings".

If you or your company are members of the Marketing Association, you can obtain advice on legislation affecting marketing communications simply by emailing [keith@marketing.org.nz](mailto:keith@marketing.org.nz) or [contactus@marketing.org.nz](mailto:contactus@marketing.org.nz). If you're not a member, get in touch anyway and discuss membership!

## Privacy Officer

A privacy officer is a person within an agency whose job it is to encourage compliance with the Information Privacy Principles and with other provisions of the Privacy Act. Deal with requests for personal information and issues concerning personal information, and generally work with the Privacy Commission when they are investigating complaints.

The Privacy Act says that each agency is responsible for ensuring that there are, within the agency, one or more privacy officers. The agency should ensure that the person has enough resources to carry out his or her responsibilities properly.

The name of the Privacy Officer should be publicised within the agency and staff should be encouraged to discuss issues with that person. If the Privacy Officer is unable to assist, the Office of the Privacy Commissioner can provide guidance, including written information. However, it is not the role of the Commissioner to provide legal advice or guidance on a hypothetical situation.

A large organisation with a number of branch offices might find it desirable to designate a Privacy Officer in each location. However, a company (either big or small) that holds very little personal information might find that one Privacy Officer in the head office (or the only office) is enough.

An "agency" is any person or company or Government department.

Who else should know about the Information Privacy Principles and Privacy Act?

Everyone in the organisation who handles personal information should be aware of the Information Privacy Principles and the objectives of the Privacy Act generally. Where a more detailed knowledge of the agency's rights and responsibilities is required, the privacy officer should be able to assist. If not, he or she can contact the Office of the Privacy Commissioner for help.

---

Fact Sheets are available from The Office of the Privacy Commissioner, PO Box 10094, Wellington 6143, Tel 04 474 7590 or P O Box 466, Auckland 1140, Tel 09 302 8680 or at [www.privacy.org.nz](http://www.privacy.org.nz)

---