



## Best Practice Guidelines Direct Marketing Data

Updated December 2007

*The Marketing Association's Data Advisory Network (DAN) have designed the 6 Guiding Principles for Direct Marketing Data to provide data managers with guidelines to ensure personal information used for marketing purposes is collected, managed and maintained in accordance with best practice standards. The guidelines are to be considered as a collective entity. In brief, they are:*

- 1** [Legal collection of personal information](#)
- 2** [Storage and security of data](#)
- 3** [Access to data and disclosure](#)
- 4** [Maintenance of databases](#)
- 5** [Removal/suppression of names from databases](#)
- 6** [Tips on Selecting Data](#)

## Principle 1 Legal collection of personal information

The Privacy Act 1993 outlines 12 Principles

- 1) **The purpose of collection of personal information:** Information must be collected for a lawful purpose and must be necessary for that purpose;
- 2) **The source of personal information**  
Information about an individual is required to be obtained from that individual with a number of limited exceptions including where the information is publicly available and where the individual has authorised its collection.
- 3) **Collecting information from an individual**  
Where information is collected from an individual the individual must be made aware of several specific matters including that the information is being collected and the purpose for which it is being collected.
- 4) **Manner of collection of personal information:** Information may not be collected unlawfully or in circumstances that are unfair or that intrude to an unreasonable extent upon the personal affairs of the individual.
- 5) **Storage and security of personal information:** Information is to be stored with sufficient safeguards to protect against loss or unauthorised access.
- 6) **Access to personal information:** Where information is held about an individual in a form that can be readily retrieved the individual concerned is entitled to obtain confirmation that information is held and have access to that information.
- 7) **Correction of personal information:** Where information is held about an individual the individual is entitled to request the correction of that information.
- 8) **Accuracy of information:** There is an obligation to ensure that information retained is accurate, up to date, complete and not misleading.
- 9) **Information not to be kept longer than necessary:** Personal information must not be retained longer than is necessary for the purpose for which the information is lawfully able to be used.
- 10) **Limits on use of personal information:** A person holding information that is obtained for one purpose is not able to use it for other purposes except in certain limited situations.
- 11) **Limits on disclosure of personal information:** A person holding information is not entitled to disclose that information to anyone except in certain restricted circumstances.
- 12) **Unique identifiers:** Persons holding information are only able to assign “unique identifiers” (for example code numbers) to individuals if it is necessary to carry out their functions efficiently. The same unique identifier used by other persons e.g. government agencies cannot be used.

<http://www.marketing.org.nz/cms/Resources/105>

## The Code of Practice for Direct Marketing in New Zealand

**PRINCIPLE 1:** Marketers will comply with the laws of New Zealand and all appropriate industry Codes of Practice

**PRINCIPLE 2:** Offers will be clear and truthful and not present a product, service, or offer in a way that could mislead the consumer.

**PRINCIPLE 3:** Orders for products or services will be handled in a responsible and prompt manner.

**PRINCIPLE 4:** Marketers will carry out their business in a way that is socially responsible.

**PRINCIPLE 5:** Marketers will uphold high standards of business practice to bring about the trust of consumers.

Ref: <http://www.marketing.org.nz/cms/Resources/23>

## Principle 2 Storage & security of data

Requirement for protocols governing storage of data

- Ensure personal information is stored securely and can only be accessed by authorised personnel
- Disposal of personal information should be by way of by a shredder or security bin
- Computer screens on which personal data is displayed must not be visible to unauthorised persons

### Security of access to data

- Ensure data is stored on a secure computer with protected access
- Databases holding personal information should be password protected
- Back-up data on a regular basis (once per day normally)

### Privacy Officer

Under the Privacy Act 1993, each organisation holding personal data must appoint a Privacy Officer. This person must understand the 12 Privacy Principles (as above) and all Privacy related issues should be referred to them.

Ref: <http://www.privacy.org.nz/comply/comptop.html>

## Principle 3 Access and disclosure

Protocols relating to disclosure of such information

**[Privacy Act] 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 promptly. Incorporate checks to ensure that information requests are bona fide.*

*Organisations can charge a “reasonable” amount to supply data and if information is corrected by the individual, such amendment should be actioned/updated as soon as possible.*

## Principle 4 Maintenance of databases

### New Zealand Postcodes and postal address standards

New postcode and address standards were introduced in April 2006 to improve the quality of postal addressing. Benefits include reduced ambiguity in New Zealand postal addresses (the new postcodes are designed to ensure there are no duplicate street names or suburbs within a postcode boundary), reduced ‘Return to Sender’ or undeliverable mail, more effective direct marketing and prospect selection, and lower operating costs for data acquisition and management.

Mail addressed using the correct standards will pass through New Zealand Post’s automated systems quickly and are required for bulk mail discounts. From July 2008, this will include the use of the new postcodes.

It is Best Practice to ensure that data being used for direct mailing purposes has a Statement of Accuracy (SOA) issued by a New Zealand Post approved SendRight™ Certifier. For more information: <http://addressing.nzpost.co.nz/Cultures/en-NZ/SendRight/>.

Information about the address standards and postcodes, including an online Address and Postcode Finder and downloadable PDF files of the Postcode Directory and Address Standards can be found at [www.nzpost.co.nz/addressing](http://www.nzpost.co.nz/addressing).

Data service providers also offer a range of tools and services to assist in postal address data management and maintenance.

### Unique identifiers

Unique identifiers, generally computer-generated, are a useful tool for database management, providing a constant reference to enable individual records to be accurately identified.

The Privacy Act covers the use of unique identifiers in certain circumstances:

***[Privacy Act] Principle 12: Unique identifiers.***

*Persons holding information are only able to assign “unique identifiers” (for example code numbers) to individuals if it is necessary to carry out their functions efficiently. The same unique identifier used by other persons e.g. government agencies cannot be used.*

**GNA's (Gone No Address)**

To maintain database integrity, details of individuals who are the subject of returned mail marked “Gone No Address” should be amended promptly.

**Duplications**

Duplicated communications are a source of annoyance and an unnecessary cost. Best practice is to eliminate as many duplicated records by regular database maintenance.

More than one field should be used to compare records for duplicates. Numeric fields are recommended, e.g. phone numbers, fax numbers etc. The fields being used for duplicate checking should be reduced to the bare basics – .e. no spaces, hyphens. Fields can be combined to create “Keys” which can be used for comparing data.

Specialist software is available for purchase or a Data Service Bureau [A L2] could be considered.

## **Principle 5 Removal/suppression of names from databases**

**In-house suppression file/s**

It is critically important in maintaining database integrity, to honour requests for removal or opt-out.

Best Practice guidelines recommend that such records are not removed entirely from the database, but tagged in such a manner that they are not considered live. Data should be cross-matched with a “suppression list” before it is used, i.e. compare data with a list of people who have requested to be removed.

**Name Removal Register/Deaths Index**

The Marketing Association manages a Name Removal Register (NRR) file containing the names of individuals who do not wish to receive unsolicited advertising communications. The Name Removal Register incorporates the Deaths Index. All Marketing Association members are required to access the NRR before each unsolicited marketing campaign to suppress names contained on the Register from their data selection.

<http://www.marketing.org.nz/cms/Resources/104>

## Principle 6 Data selection tips

### Questions To Ask List Broker Prior To List Rental

- Who owns the list?
- How often is it mailed?
- Last time mailed?
- How was the list compiled?
- How long has it been on market?
- What is the deliverability guarantee? (you shouldn't pay for GNA's)
- When was the last validation?
- Percentage response rates?
- Selection criteria? (Age; gender; occupation; title; geographic; employee numbers; telephone numbers only etc.)
- Can list only be delivered to a third party e.g. a mailing house?
- Is it privacy compliant?
- Is it run against the Marketing Association Name Removal Register?

The chart below details levels of information that are essential to have and 'nice to have' in both residential and business databases.

	<b>Residential data</b>	<b>Business data</b>
Essential	Name Address Phone numbers – work, home, mobile Email address Gender	Company name Address Name of contact Position within company Phone number email address
"Nice to have"	Marital status Income bracket Age/date of birth Occupation Household composition	Industry code Size of company/number of employees Public/Private Company Turnover Exporter/Importer