ma.

Marketing Association

Direct Marketing Data Best Practice Guidelines

Updated

The Marketing Association's Data Advisory Network (DAN) have designed Guidelines for Direct Marketing Data to enable data managers 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 Data selection tips

7 Data Warranty Register

1 Legal collection of personal information

The Privacy Act governs the collection and storage of personal information about identifiable individuals in New Zealand. The core of this legislation is covered in the 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. There are 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, s/he must be made aware of the fact that the information is being collected, what it will be used for, where it will be stored and their rights of access and correction.

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 s/he 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.

    Limits on disclosure of personal information: A person holding information is not entitled to disclose that information to anyone except in certain restricted circumstances.

2

1. **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.

Download a Guide to the Privacy Act

3 Storage & security of data

There is growing concern around the world about the security of personal information. Any organisation holding data on identifiable individuals must appoint one or more Privacy Officers [S23 Privacy Act]. Details of the responsibilities of a Privacy Officer are available here.

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

4 Access and disclosure

Honesty and transparency are the key to good customer relationships. Making it simple for people to access, correct or update their information is best practice.

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.

5 Maintenance of databases

It makes good business sense to maintain an accurate and up-to-date database which conforms to New Zealand Postcodes and postal address standards.

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: www.nzpost.co.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.

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 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 could be considered.

6 Removal/suppression of names from databases

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

In-house suppression file/s

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.

Do Not Mail List/Deaths Information

The Marketing Association operates a national Name Suppression Service. This includes a Do Not Mail List (DNM) and Do Not Call List (DNC) containing the details of individuals who do not wish to receive unsolicited advertising communications. All Marketing Association members are required to access both the DNM and/or the DNC before each unsolicited marketing campaigns.

The Name Suppression Service includes the New Zealand Deaths Information, containing details of people who have died over recent years. It is clearly best practice to subscribe to the Deaths Index to avoid upsetting or offending bereaved families.

7 Data selection tips

The key to successful direct marketing lies in the quality of the data used.

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 Do Not Mail Register?

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

	Residential data	**Business data**
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

8 Data Warranty Register

7.1 Marketers collecting, storing or using personal data should become 'Data Warranted' and thereby entitled to use the 'Data Warranted' trustmark. The Data Warranty Register (DWR) is maintained by the MA and contains the details of all organisations who follow industry best practice in the management of personal data. A list of these organisations is published on the MA website.