Direct Marketing Data

Best Practice Guidelines

Updated June 2021

The Marketing Association's Data Special Interest Group (SIG) have designed Guidelines for Direct Marketing Data to enable data managers and marketers to ensure personal information used for marketing purposes is collected, managed and maintained in accordance with best practice standards, and follows relevant data protection and privacy legislation. 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 2020 governs the collection and storage of personal information about identifiable individuals in New Zealand. The core of this legislation is covered in the 13 Principles:

Principle 1 - Purpose for collection
Principle 2 - Source of information
Principle 3 - What to tell an individual
Principle 4 - Manner of collection
Principle 5 - Storage and security
Principle 6 - Access
Principle 7 - Correction
Principle 8 - Accuracy
Principle 9 - Retention
Principle 10 - Use
Principle 11 - Disclosure
Principle 12 - Disclosure outside New Zealand
Principle 13 - Unique identifiers

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.

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. Disclosure outside New Zealand
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. The person must be expressly informed that their information may not be given the same protection as provided by the New Zealand Privacy Act

13.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.

Further resources about the Privacy Act are available here.

2. 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 [S216 Privacy Act 2020]. Details of the responsibilities of a Privacy Officer are available here.

Recommendations for protocols governing storage of data

- Ensure personal information is stored securely and can only be accessed by authorised personnel.
- Only collect and store what you need to deliver required services or communications to customers
- Disposal of personal information should be by way of by a shredder or security bin. When removing people from databases or other systems consider records that may also be held in backups.
- Computer screens on which personal data is displayed must not be visible to unauthorised persons
- Password protection for electronic files with adequate standards for strong passwords
- Where applicable set up data retention principles to limit the amount of data you store and reduce risk of data loss

Security of access to data

- Ensure data is stored on a secure computer or cloud services, with protected access
- Databases holding personal information should be password protected
- Back-up data on a regular basis (once per day usually)
- Outline key people who need access to data and their roles when they access it

- When transferring data to other parties avoid emailing data. Use other secure data transfer methods and platforms where possible and ensure deletion when complete.
- Do not share personally identifiable information (PII) data with other parties unless it's required to perform outsourced services. Where possible de-identity data and create temporary or alternate IDs to avoid risk of potential loss of any information such as account numbers or user IDs.
- When sharing data with other parties, platforms or service providers do due diligence on their data security policies and procedures.
- When sharing data, encrypt or hash data using stronger encryption or hashing algorithms (e.g. SHA-256 or SHA-3).

Privacy Officer

Under the Privacy Act 2020 each organisation holding personal data must appoint a Privacy Officer. This person must understand the 13 Privacy Principles (as above) and all privacy related issues should be referred to them.

Ref: https://privacy.org.nz/responsibilities/your-obligations/privacy-officers/?highlight=Privacy+Officers

3. 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 and preferences 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 personal information is held and to access the information about themselves.

Organisations 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 amendments should be actioned/updated as soon as possible.

4. Maintenance of Data

Off-line communications (Mail & Telemarketing)

It makes good business sense to maintain an accurate and up-to-date database. Ensuring phone numbers and emails are current and conforming to postal address standards can save money as well as help deliver better service to customers.

New Zealand Postcodes and postal address standards

Ensuring mailing data adheres to addressing standards and is accurately postcoded can ensure faster delivery, fewer returns and lower postage costs. Information is available on the NZ Post website including an online Address and Postcode Finder, and downloadable PDF files on the Address Standards.

Data service providers also offer a range of tools and services to assist in postal address data management and maintenance including batch address hygiene and appending of postcodes through to flagging and removing people that have moved so you can update your database.

Good practice is to implement tools that verify, format and correctly postcode addresses at point of capture on your website or other systems. This also provides a better customer experience by making it easier and faster for them to enter an address into a form.

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.

Electronic communications (email, SMS and other instant messages)

Emails, Mobile phone numbers

Emails, unlike postal addresses, tend to change more frequently. Customers more frequently change, abandon or, create a new email address than they do with their postal addresses. Maintenance of the data with the latest and accurate email addresses is the foundation of your email marketing campaign' effectiveness and data privacy.

At the point of capturing email addresses a confirmation of the email via a double opt-in method is an effective way to check typos or data entry errors. Make sure the data consists of valid email addresses, bounces and opt-outs are filtered out and kept separately from your main database. Emailing to bounced email addresses can impact the reputation of your email domain and undermine the deliverability rate of your campaign.

Make sure you give a simple and non-obstructed way for customers to update their contact details or opt-out of your email lists. Absence of this is a violation of anti-spam law, the Unsolicited Electronic Messaging Act 2007, and you can be prosecuted. Modern marketing email platforms have 'Unsubscribe' management solutions that are already compliant with the latest privacy and anti-spam regulations.

Similar principles should be followed for management of mobile phone numbers if you intend to use them for SMS messaging. Customers should be able to update and change their contact details. They should be able to simply change their communication preferences and be able to opt-out from SMS campaigns.

Maintenance of email and phone details will payback with improved effectiveness of marketing campaigns, improved customer experience and keep your marketing efforts within legal frameworks.

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 13: 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.

Email bounces

Good practice is to remove hard bounces (e.g. invalid emails) from your database or flag as inactive to ensure they don't get added again. Soft bounces (e.g. Out of Office) should also be monitored. Inbox providers and Spam filters monitor bounce rates. You may risk having your emails blocked if you continue to send emails that bounce. Services are available that enable you to test or ping your list to identify and remove/flag invalid emails on your database which are inexpensive to use.

If people continually do not open or read your emails, it's also good practice stop emailing them to avoid being tagged as spam. Consider a re engagement campaign for disengaged contacts.

Always provide a clear functional unsubscribe and ideally options for people to update their email settings or preferences.

Duplications

Duplicated communications are a source of annoyance an unnecessary cost, and potential privacy breach. Best practice is to eliminate or update duplicated records through regular database maintenance.

Multiple fields or data points should be used to compare records for duplicates to ensure you have identified the same individual before merging records. Numeric fields (e.g. phone numbers) are recommended, as well as data points such as date of birth or email address, where available, which can be less variable in format than addresses. The fields being used for duplicate checking should be reduced to the bare basics, i.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 Data Service providers with advanced matching capability could also be considered.

5.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 or previously opted out. This will ensure ongoing suppression even if an individual is added back into a database inadvertently. Updating people's preferences regularly is also recommended.

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 marketing offers. All Marketing Association members are required to apply both the DNM and/or the DNC before any unsolicited marketing campaign.

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.

6. Data selection tips

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

Questions To Ask a List Broker Prior To List Rental

- Who owns the list?
- How often is it mailed or called?
- Last time mailed or called?
- How was the list compiled?
- How long has it been on the market?
- What is the deliverability guarantee? (You shouldn't pay for GNA's or disconnected numbers)
- When was the last validation?
- Typical response rates?
- Selection criteria available? (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 or call centre?
- Is it privacy compliant?
- Is it washed against the Marketing Association Do Not Mail or Do Not Call Register?

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

Residential Data

Essential

- Name
- Address
- Phone numbers – work, home, mobile
- Email address
- Gender

'Nice to have'

- Marital status
- Income bracket
- Age
- Occupation
- Household composition
- Other consumer segments or personas

Business Data

Essential

- Company name
- Address
- Name of contact
- Position within company
- Phone number
- email address

'Nice to have'

- Industry code
- Size of company/number of employees
- Public/Private Company
- Turnover
- Exporter/Importer

7. Data Warranty Register

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 personally identifiable information or PII. A list of these organisations is published on the MA website.