

THE DATA WARRANTY REGISTER: QUESTIONS & ANSWERS

What is the Data Warranty Register

The Data Warranty Register (DWR) is a self-regulatory system that provides best-practice transparency relating to the collection, storage and use of marketing data by New Zealand businesses for marketing purposes.

It is designed to be an effective identifier of data owners, providers and enhancers who follow best practice guidelines and/or are trusted sources of data.

The DWR is intended to “future-proof” the collection, storage and use of both consumer and business data to demonstrate the effectiveness of a self-regulatory regime, thereby reducing the likelihood of restrictive laws being implemented which may affect the ability (and the right) to take goods and services to market.

Regarded as a key asset, customer and prospect data is now at the very heart of most businesses. The proliferation of media channels means it is more important than ever to collect, store and manage data professionally, legally and ethically – and to be seen to be doing just that!

Why do we need a Data Warranty Register?

With the proposed implementation of stringent data regulations in the EU and USA, it is critical for the growth and success of business in New Zealand that similar legislation is not regarded as being necessary here.

The robustness of the DWR process, which includes compliance checks, is intended to demonstrate to the lawmakers that in the increasingly important business arena of data management, the industry is capable of upholding self-regulated best-practice standards, and thus protect the privacy of individual New Zealanders.

What is being warranted under the DWR?

The Data Warranty Register is intended to ‘future proof’ the collection, storage and use of data for marketing purposes in New Zealand. This means that from time to time it may be enhanced to reflect a change in the law and/or best practice codes.

It is **data providers, enhancers and/or owners** that are being warranted and certifies that all of their marketing data processes comply with current legislation and best practice.

Is Business-to-Business data covered by the DWR?

The Privacy Act refers to “identifiable individuals” so while businesses/organisations are not covered by Act, the individuals who work for them are, so yes, B2B data is included.

Who does it apply to?

Data providers/brokers and data enhancers, including organisations who trade their own

lists/data files.

Data owners who maintain data files for their own purposes, and who wish to be recognised for their robust data processes. Even those who never trade their data files will be encouraged to have their processes warranted to demonstrate their commitment to best practice and to provide an additional level of assurance to their customers and prospective customers. Note: this includes owners of business-to-business lists that contain details of identifiable individuals.

If you are a **provider/cleanser/enhancer of data** for marketing purposes, you register on the MA's DWR by completing a Data Declaration. You will also be required to carry out an annual "self-audit", and be subject to compliance checks (likely to be at least once every three years); AND you will be required to subscribe to the relevant Name Suppression Service(s) for your data's intended use.

If you are a **data owner**, you will be encouraged to register on the MA's DWR by completing a Data Declaration. You will also be required to carry out an annual self-audit, and be subject to compliance checks (likely to be at least once every three years); AND subscribe to the relevant Name Suppression Service if you communicate with consumers who are not on your customer list. Alternatively, you should use a DWR-registered data bureau to cleanse/wash your data.

What does the DWR cover?

Initially it covers:

- compliance with MA Best Practice Guidelines
- compliance with The Privacy Act 1993
- compliance with The Unsolicited Electronic Messages Act 2007
- sourcing of personal data
- method of data collection
- security procedures
- storage of data
- the use of suppression lists (as and when applicable)
- documentation procedures
- record tracking
- data transfer protocols
- data sharing protocols
- staff training
- data disclosure
- compliance with current postal addressing standards

Will the DWR cover more data elements over time?

Yes. We appreciate that modern technologies enable the combining of various data elements and the implications of that. But we need to discuss and agree what the standards are going to be to cater for the era of 'big data' into the future. This means the DWR is likely to be expanded in phases, as and when appropriate.

Do I need to be an (NZ) MA member to become warranted?

All MA members are expected to follow and abide by published best practice guidelines and codes of practice and therefore to have their data processes warranted. However, this service is not exclusive to MA members. Effective data management procedures and a commitment to self-regulated best practice is the best way of protecting the consumer and thereby avoid restrictive legislation.

How will my data processes be warranted?

The Data Declaration and compliance process has been designed to help all NZ businesses to operate in a compliant manner. Once the compliance check has been completed and any issues addressed, the DWR Trustmark will be granted. This will be renewed annually on payment of the relevant fee and submission of a completed “self-audit” document.

The independent Compliance Consultant will help data owners/enhancers through the initial checking process. On receipt of the relevant annual fee, the DWR Trustmark will be granted.

Data owners who wish to have their data collection, storage and management processes warranted will submit a completed Data Declaration to the MA. Our independent Compliance Consultant will contact the applicant to clarify points if necessary. On receipt of the relevant annual fee, the DWR Trustmark will be granted.

Is there a cost to be warranted?

Yes, because we need to cover the cost of administering the service and the compliance checking process. It has been kept to a minimum and varies depending upon the number of personal records you hold. There are preferential rates for Marketing Association members.

The application/registration fees will be tiered on a number-of-records basis, as follows:

DWR Application/Registration Fees	Member	Non Member
Tier 1: Up to 5,000 individual records	\$195 + GST p.a.	\$295 + GST p.a.
Tier 2: 5,001 - 50,000 individual records	\$395 + GST p.a.	\$795 + GST p.a.
Tier 3: 50,001 - 200,000 individual records	\$595 + GST p.a.	\$995 + GST p.a.
Tier 4: 200,001+ individual records	\$995 + GST p.a.	\$1950+ GST p.a.

Note:

The Name Suppression Service fees will remain at the current level. [To see what these are, go to www.marketing.org.nz – type Name Suppression Service in the search box on the home page.]

How will I know who's warranted and who's not?

There will be a list of organisations authorised to use the DWR Trustmark on the MA website.

Where do the Suppression files (Do Not Mail, Do Not Call, Deaths Information) fit in with DWR?

Best practice requires that you make every effort to respect the express wish of those who've registered on the Do Not Mail and Do Not Call lists to not be contacted. This applies to all prospecting activity but not necessarily to an organisation's own customers. The Deaths Information file can **only** be used for suppression purposes and is able to be matched against data files containing details of people at their residential addresses, i.e. it does not contain businesses addresses.

All warranted data providers are required to wash their residential data against the MA suppression files.

What does a compliance check entail?

All DWR applicants will be required to have a compliance check carried out *before* the DWR Trustmark is granted. Random compliance checks may be carried out on data providers, enhancers and owners (approximately every two to three years), and will be mandatory in the event of a complaint about their data practices being received. Approximately 4 weeks' notice of an impending random compliance check will be given.

The compliance check will cover:

- Data sources
- Data maintenance
- Data transfer
- Privacy

The information you provide in your initial Data Declaration will be reviewed at the time of compliance checking.

You will receive a Compliance report for your records.

Where can we display the DWR Trustmark logo?

Once you've been granted the right to display the DATA WARRANTED logo (the DWR Trustmark), you'll be provided with two versions – one for print and one for electronic media. We recommend that you display the logo wherever you capture personal information, whether that's on a web page or printed material, and wherever you publish your Privacy statement.

You can also make it available to your staff to include in their email signatures if you wish...just make sure they know what it stands for and can answer questions about it. If you publish a staff newsletter, this would be a good way to let them know of your warranted status and explain what that means.