



Rangahau  
Aotearoa

Research  
New Zealand

# Privacy Policies and Practices

Updated: September 2024

---

9 September, 2024

# Privacy Policies and Practices

## Introduction

As a member of the research community, Rangahau Aotearoa (Research New Zealand) has an obligation to conduct its work in an ethical and professional manner, in accordance with relevant law (i.e., the Privacy Act 2020) and the Codes of Practice of the European Society of Marketing & Opinion Research and the Research Association of New Zealand.

As such, we have specific obligations to both our clients and respondents in terms of their privacy and the protection thereof.

## Purpose and scope

This document outlines Rangahau Aotearoa's **privacy policies and practices**.

It sets essential standards of conduct designed to maintain client and public confidence in our research. It ensures that researchers, interviewers and staff in support roles meet their responsibilities in relation to the individuals whose data they use in research and to the clients and organisations they serve.

Throughout this document the word "must" is used to identify mandatory requirements; that is, a principle or practice that researchers, interviewers and staff are obliged to follow. The word "should" is used when describing implementation and denotes a recommended practice.

# Privacy statement

Rangahau Aotearoa's **privacy statement** is as follows:

"As a research company we collect, are provided and make use of personal information. We are very mindful of the responsibilities that are associated with this aspect of our business. To ensure we meet our responsibilities to our clients and data subjects (respondents), we follow the Privacy Act 2020, the Public Records Act 2005 and the Code of Practice of European Society of Marketing & Opinion Research (the professional research organisation we belong to):

- **Informed consent**

We will always tell respondents beforehand:

- About the purpose of the research they are being invited to participate in, why and how they have been invited and what is involved in participating.
- That their participation is voluntary.
- That their participation is on a confidential basis.
- That the answers and other information they provide will only be used for the purposes of the research they have been invited to complete.

- **Participation**

We will always tell respondents:

- That they can withdraw from an interview they are completing if they want to.
- That they can change the answers they have provided to the research questions.
- That they can request a copy of the interview they have completed, with their answers.
- That they can request their completed interview to be deleted/withdrawn.

- **Privacy**

We will always tell respondents:

- That their answers to the research questions will be depersonalised as soon as practically possible (i.e., they will not be directly or indirectly identifiable).
- That the information they provide will be analysed and reported in an aggregated (summary) form.
- That any contact database which lists them and which we have used for the research they have been invited to complete/participated in will be deleted from our system.

- **Storage and access**

We will always tell respondents:

- That the information they provide will be safely stored, indefinitely, in a depersonalised form, with a government-approved local cloud provider, onshore.
- That access to this information will be restricted and actively monitored."

## Definitions

For the purposes of this document, these terms have the following specific meanings:

**Client** means any individual or organisation that requests, commissions or subscribes to all or any part of a research project.

**Consent** means a freely given and informed indication of agreement by a person to the collection and processing of his/her personal data.

**Data analytics** means the process of examining data sets to uncover hidden patterns, unknown correlations, trends, preferences and other useful information for research purposes.

**Data subject** (also referred to as a respondent) means any individual whose personal data is used in research.

**Harm** means tangible and material harm (such as, physical injury or financial loss), intangible or moral harm (such as, damage to reputation or goodwill), or excessive intrusion into private life, including unsolicited personally-targeted marketing messages.

**Non-research activity** means taking direct action toward an individual whose personal data was collected or analysed with the intent to change the attitudes, opinions or actions of that individual.

**Passive data collection** means the collection of personal data by observing, measuring or recording an individual's actions or behaviour.

**Personal data** (sometimes referred to as personally identifiable information or PII) means any information relating to a natural living person that can be used to identify an individual, For example, by reference to direct identifiers (such as a name, specific geographic location, telephone number, picture, sound or video recording), or indirectly, by reference to an individual's physical, physiological, mental, economic, cultural or social characteristics.

**Primary data** means data collected by a researcher from or about an individual for the purpose of research.

**Privacy notice** (sometimes referred to as privacy policy) means a published summary of an organisation's privacy practices, describing the ways an organisation gathers, uses, discloses and manages a data subject's personal data.

**Research** that includes all forms of market, opinion and social research and data analytics, is the systematic gathering and interpretation of information about individuals and organisations. It uses the statistical and analytical methods and techniques of the applied social, behavioural and data sciences to generate insights and support decision-making by providers of goods and services, governments, non-profit organisations and the general public.

**Researcher** means any individual or organisation carrying out or acting as a consultant on research, including those working in client organisations and any subcontractors used.

**Secondary data** means data collected for another purpose and subsequently used in the research.

# 1.0 Data protection and privacy policy

This section is based on Articles 1-6 of the ESOMAR Code of Practice.

## 1.1 Fundamental principles

This document is based on **four** fundamental principles:

1. When collecting personal data from data subjects for the purpose of research, researchers must be **transparent** about the information they plan to collect, the purpose for which it will be collected, with whom it might be shared and in what form.
2. Researchers must ensure that data subjects are **not harmed** as a direct result of their personal data collected and being used for research.
3. Researchers must ensure that personal data used in research is thoroughly **protected** from unauthorised access and not disclosed without the consent of the data subject.
4. Researchers must ensure that personal data used in research is **only used** for the purposes it was provided/collected and, therefore, must remain diligent in maintaining the distinction between research and non-research activities.

## 1.2 Primary data collection

When collecting **personal data directly** from a data subject for the purpose of research:

1. Researchers must **identify themselves** promptly and data subjects must be able to verify the identity and bona fides of the researcher without any difficulty.
2. Researchers must **clearly state** the general purpose of the research as soon as methodologically possible.
3. Researchers must ensure that **participation is promoted as being voluntary** and based on information about the general purpose and nature of the research that is adequate and not misleading.
4. Researchers must **inform** data subjects if there is any activity that will involve re-contacting and that the data subjects must agree to be re-contacted. The only exception to this is to re-contact for quality control purposes.
5. Researchers must respect the right of data subjects to **refuse** requests to participate in research.
6. Researchers must allow data subjects to **withdraw** from the research at any time and access or rectify personal data held about them.
7. Researchers must **limit** the collection and/or processing of personal data to those items that are relevant to the research.
8. Passive data collection should be based on the **consent** of the data subject and meet all conditions outlined above. Where it is not possible to obtain consent, researchers must have legally permissible grounds to collect the data, and they must remove or obscure any identifying characteristics as soon as operationally possible.

## 1.3 Secondary data

When using **secondary data** that includes personal data, researchers must ensure that:

1. The intended use is **compatible** with the purpose for which the data was originally collected.
2. The data was **not** collected in violation of restrictions imposed by law, through deception, or in ways that were not apparent to or reasonably discernible and anticipated by the data subject.
3. The intended use was **not** specifically excluded in the privacy notice provided at the time of original collection.
4. Any **requests** from individual data subjects that their data not be used for other purposes are honoured.
5. Use of the data will **not** result in harm to data subjects and there are measures in place to guard against such harm.

## 1.4 Important obligations to data subjects

With respect to data protection and privacy, researchers must ensure the following:

1. They have a **privacy notice** that is readily accessible by data subjects and is easily understood.
2. They ensure that personal data **cannot be traced nor an individual's identity inferred** via deductive disclosure (for example, through cross-analysis, small samples or combination with other data such as a client's records or secondary data in the public domain).
3. They must take all reasonable precautions to ensure that personal data is held **securely**. It must be protected against risks such as loss, unauthorised access, destruction, misuse, manipulation or disclosure.
4. Personal data is to be held **no longer** than is necessary for the purpose for which it was collected or used. If personal data is to be transferred to subcontractors or other service providers, researchers must ensure that the recipients employ at least an equivalent level of security measures.
5. They must **not share** a data subject's personal data with a client unless the data subject has given consent to do so and has agreed to the specific purpose for which it will be used.
6. In the event of a **data breach** containing personal data researchers have a duty of care for the data subjects involved and must follow all applicable data breach notification laws.



## 2.0 Data protection and privacy practices

This section is based on how Rangahau Aotearoa meets the policy outlined in the previous section.

### 2.1 Ethics approval

Subject to the objectives of a research project, Rangahau Aotearoa may obtain formal ethical approval before proceeding:

1. Ethics approval will be applied to the appropriate ethics body (e.g., Health & Disability Ethics Committee).

### 2.2 Privacy Impact Assessment

For significantly larger research projects, including monitors, as a matter of best practise:

1. A **Privacy Impact Assessment** (PIA) will be completed.
2. The PIA will be completed using the Privacy Commission's template.
3. The PIA will be followed by an 'action plan' that addresses the prioritised risks identified in the PIA.

### 2.3 Informed consent

Informed consent will always be sought from data subjects (respondents):

1. Informed consent will be sought **prior** to a research project taking place; this may be as part of the prenotification about the project (see below).
2. Informed consent will be obtained by way of a **prenotification email or letter**, typically cobranded with the client's and Rangahau branding.
3. The pre-notification will be written from the **client's perspective** and provide the following information: the purpose of the research; why and how prospective respondents have been selected; and what participation involves.
4. Importantly, it will state that participation is **voluntary; confidential** and that the information prospective respondents provide will be aggregated with that of other respondents for analysis and reporting purposes. That is, individual respondents will **not** be identifiable.
5. Where it is of benefit to specifically **identify** individual respondents' responses, respondents will be asked to provide their **formal consent**.
6. Where a prospective respondent commences a survey, it will be **assumed** they have provided their **consent**. However, in other cases, **written consent** will be obtained (e.g., a qualitative research project) and/or the information in the prenotification email or letter may be augmented with a **Participant Information Sheet**.
7. In the case of a qualitative research projects, **formal consent** to **audio record** the discussions/interviews will be obtained. Respondents will be specifically told this will be for analytical purposes.
8. Where the client wishes to have a recording as well, or a summary, **formal consent** to provide this will also be obtained.

## 2.4 Contact databases

For some research project, clients provide a contact database of their clients, constituents, stakeholders, etc.:

1. The database will contain the **minimal amount** of information required by us to contact a prospective respondent, and/or to categorise them for analytical purposes.
2. The database will be provided via our **secure client portal** (or equivalent), in an encrypted password protected form.
3. The password will be delivered **separately** from the delivery of the contact database.
4. On receipt it will be saved in the relevant project folder. Access to this folder will be **restricted** and managed via **permissions**.
5. The database (original and copies) will be **deleted** from our system as soon as practically possible, after the fieldwork for the project has been completed and verification processes have been completed.

## 2.5 Data collection

During the data collection/interviewing/fieldwork for a project:

1. At the commencement of an interview, respondents will be briefly reminded of the purpose of the project and that their participation is voluntary and confidential. In the case of an online survey, for example, they will also be provided with a link to our **privacy statement**.
2. Respondents will be given the option of **not** answering every question, **withdrawing** from an interview and asking that their completed interview **not** be submitted.
3. Respondents may also **request a copy** of their interview.

## 2.6 Post-interviewing

Following the completion of the data collection/interviewing/fieldwork for a project:

1. Any information capable of identifying a respondent will be **removed** (e.g., contact information, references to names, places, events, etc. in the response to open-ended questions).
2. In the case of surveys, restrictions will be placed on the **smallest sub-group** of respondents that analysis and reporting will be completed for. This is so that respondents are **not** indirectly identified.
3. Similar restrictions will be placed on clients' ability to analyse the raw data in a dashboard or e-report.

## 2.7 Data transfer

Clients for whom we have completed a survey typically ask for a datafile:

1. On request, clients will be provided with a **depersonalised** dataset.
2. This will be delivered via our **secure client portal** (or equivalent), in an encrypted password protected form.
3. The password will be delivered **separately** from the delivery of the dataset.

## 2.8 Data storage

Post-interviewing:

1. Survey datasets will be saved, indefinitely, in a **depersonalised** form.
2. Datasets will be saved with a **government-approved local cloud provider**, in Aotearoa New Zealand.