Privacy Policy

Contents

Policy Owner and Approval	▪ The Owner of this Policy is the Chief Executive. ▪ This Policy has been approved by the Board. ▪ The Committee responsible is the Audit and Risk Committee.
Review Date	June 2025
Effective Date	14 May 2012

Introduction

Purpose and Scope

The purpose of this Privacy Policy ("**Policy**") is to ensure that Southern Response manages Personal Information in a manner that complies with the Privacy Act 2020 ("**Act**").

This Policy outlines Southern Response's internal policy standards and principles for the collection, storage, use, and disclosure of Personal Information.

This Policy applies to all Personnel.

Breaches of this Policy may be considered a disciplinary matter by Southern Response.

This Policy accords with the values and other core principles of Southern Response.

Definitions

For the purpose of this Policy:

"**Personnel**" includes all employees and other personnel providing services to Southern Response (including, for example, independent contractors and Directors).

"**Personal Information**" means information about an identifiable Individual and can include any information in physical, electronic, or oral form about any individual including, for example, Southern Response customers or Personnel (past, present, or prospective).

"**Individual**" means a natural person, other than a deceased natural person.

"Privacy Incident" means a Privacy Breach or Near Miss.

"**Privacy Breach**" means:

- unauthorised or accidental: access, disclosure, alteration, loss or destruction of Personal Information; or
- an action or event that prevents Southern Response from accessing Personal Information (on either a temporary or permanent basis) due, for example, to an internal system outage or an external hack.

"**Near Miss**" means a situation where a Privacy Breach is narrowly avoided.

Collection of Personal Information

Collection for lawful purposes

Southern Response only collects Personal Information when it is necessary to do so for lawful purposes connected with Southern Response's primary functions of:

- ensuring the fair, timely and enduring resolution of insurance claims by AMI policyholders for earthquake damage which occurred during the Canterbury Earthquake Sequence prior to 5 April 2012; and
- complying with Southern Response's legal and other obligations as a Crown-owned entity and employer.

Collection from the Individual concerned

Southern Response will collect Personal Information directly from the Individual concerned unless it believes on reasonable grounds that one of the exceptions in the Act applies.

Transparency about collection

Southern Response will take reasonable steps to ensure that the Individual concerned is aware (at or before the time Personal Information is collected from them) of:

- the fact that the Personal Information is being collected;
- the purpose for which the Personal Information is being collected;
- the intended recipient of the Personal Information;
- the name and contact details of Southern Response (as the entity collecting and holding the Personal Information) and its Privacy Officer;
- whether the collection of Personal Information is authorised or required by law;
- the consequences (if any) of not providing the requested Personal Information; and
- that the Individual concerned has a right to access and correct his or her Personal Information.

Southern Response is also transparent about the collection of Personal Information by publishing this Policy and a Transparency Statement on the Southern Response website.

Collection in a lawful manner

Southern Response only collects Personal Information by means that:

- are lawful;
- are fair in the circumstances; and
- do not intrude to an unreasonable extent upon the personal affairs of the Individual concerned.

Storage, accuracy, access and disposal of Personal Information

Storage and security

Southern Response stores Personal Information securely to prevent loss, unauthorised access, use, modification, disclosure, or other misuse.

Access to Personal Information is limited to Personnel who reasonably require access to fulfil their duties and must only be accessed by those Personnel when there is a legitimate business need.

Southern Response also takes reasonable steps to protect Personal Information that Southern Response provides to third parties (in the course of fulfilling its functions) from unauthorised use or disclosure.

Access of Individual concerned	Southern Response provides Individuals with access to their own Personal Information in a manner that is compliant with the Act. Southern Response does not charge Individuals for access to their Personal Information. Personnel who receive a request for Personal Information must refer the request to the Privacy Officer as soon as possible after receiving it. Requests for access to Personal Information are managed by the Privacy Officer in accordance with the *Information Request Process*.
Overlap with Official Information Act 1982	The Personal Information of an individual may also be "Official Information" under the Official Information Act 1982 ("**OIA**"). Requests for information to which the OIA applies will be dealt with in accordance with Southern Response's *Official Information Policy*.
Correction of Personal Information	An Individual can request correction of their Personal Information held by Southern Response. Personnel who receive a request for correction of Personal Information must refer the request to the Privacy Officer as soon as possible after receiving it.
Accuracy of information	Before using or disclosing Personal Information, Southern Response will take reasonable steps to ensure that the Personal Information is accurate, relevant, up to date, complete, and not misleading.
Retention of information no longer than necessary	Southern Response does not keep Personal Information for longer than is necessary for the purpose for which the Personal Information was collected. Subject to any law or regulation requiring retention of Personal Information, Southern Response will securely destroy or dispose of Personal Information: • when it is no longer required for the purpose for which it was obtained; • where there is no longer a lawful purpose for retaining the information; or • in accordance with any undertaking given to the Individual concerned.

Use and disclosure of Personal Information

Use of Personal Information for purpose collected	Southern Response will only use Personal Information for the purpose for which it was collected unless Southern Response believes on reasonable grounds that one of the exceptions in the Act applies.

Limits on disclosure within NZ

Personal Information will not be disclosed by Southern Response to any third party unless Southern Response believes on reasonable grounds that one of the following exceptions in the Act applies:

- the disclosure is directly related to one of the purposes for which the information was collected (including, for example, disclosure to Southern Response's agents, contractors, and advisors assisting with Southern Response's core function of resolving insurance claims);
- disclosure is to (or authorised by) the Individual concerned;
- the source of the information is publicly available, and it would not be unreasonable or unfair, in the circumstances of the case, to disclose the information;
- disclosure is necessary for a purpose associated with the maintenance of the law or conduct of legal proceedings;
- disclosure is necessary to prevent or lessen a serious threat to:
    - public health or safety; or
    - the life and safety of an Individual; or
- the information is to be used in a form in which the Individual concerned is not identified or is to be used for statistical or research purposes and will not be published in a form that could be reasonably expected to identify the Individual concerned.

Limits on disclosure outside NZ

Southern Response will not disclose Personal Information outside of New Zealand unless Southern Response believes on reasonable grounds:

- the disclosure is to the Individual concerned;
- the information is from a publicly available source, and it would not be unreasonable or unfair, in the circumstances of the case, to disclose the information;
- the overseas recipient is carrying on business in New Zealand or for some other reason is legally required to protect the Personal Information in a way that, overall, provides comparable safeguards to those provided under the Act in New Zealand; or
- the disclosure is authorised by the Individual concerned after being expressly informed by Southern Response that the overseas recipient may not be required to protect the Personal Information in a way that, overall, provides comparable safeguards to those provided under the Act in New Zealand.

General Exceptions

Need for exceptions

This Policy cannot provide exhaustively for all possible circumstances and in some cases Southern Response may need to make exceptions to the general principles for the management of Personal Information that are set out in this Policy.

Requirements for exceptions

Any exceptions to this Policy will only be made if the Privacy Officer believes on reasonable grounds that one of the exceptions in the Act applies.

Unique Identifiers

Unique identifiers	Southern Response does not assign individuals unique identifiers as part of its business activities.

Complaints about interference with privacy

Complaints to Privacy Officer	An Individual can complain to Southern Response's Privacy Officer if they believe that Southern Response may have interfered with their privacy in the way Southern Response has collected, held, used, disclosed or provided access to their Personal Information.
Complaints to Privacy Commissioner	An Individual can complain to the Office of the Privacy Commissioner ("**Privacy Commissioner**") at any time if they believe that Southern Response may have interfered with their privacy in the way Southern Response has collected, held, used, disclosed or provided access to their Personal Information. Individuals are encouraged to make their complaint to the Southern Response Privacy Officer in the first instance but are not required to do so. Complaints to the Privacy Commissioner and investigations by the Privacy Commissioner will be managed by the Privacy Officer in collaboration with the Legal Team.

Privacy Incidents

Privacy Incident Response Plan	The Privacy Officer will ensure all Privacy Incidents are managed in accordance with the *Privacy Incident Response Plan*.
Privacy Breaches	Personnel must notify the Privacy Officer immediately if they become aware of any Privacy Breach, or potential breach of the Act or this Policy. If the Privacy Officer is not available, a member of the Legal Team should be notified immediately.
Notifiable Privacy Breaches	A "**Notifiable Privacy Breach**" is a privacy breach that it is reasonable to believe has caused serious harm to any affected Individual or is likely to do so. Notifiable Privacy Breaches will be identified, assessed, and managed in accordance with the *Privacy Incident Response Plan*. The Privacy Officer will manage, in collaboration with the Legal Team, Southern Response's notification of any Notifiable Privacy Breach to: • the Privacy Commissioner; and • any affected Individual (or the public if it is not reasonably practicable to notify the affected Individual).
Near Misses	A Near Miss must be reported to the Privacy Officer if it is indicative of a potential IT, system, policy, process or training issue that, if addressed, could have prevented the Near Miss from happening.

Relevant Links

Policies and Procedures

- Information Request Process
- Privacy Incident Response Plan
- Information Gathering Policy
- Code of Conduct (adopting the Standards of Integrity and Conduct for the Public Service)
- Use of Information Resources and Security Policy

Relevant References and Resources

- Privacy Act 2020
- Official Information Act 1982
- Office of the Privacy Commissioner website
- Transparency Statement on the Southern Response website

Version Control

Version	Date	Description
0.1	14/05/2012	Policy created
0.2	14/05/2012	Reviewed by Privacy Officer
1.0	17/5/2012	Chapman Tripp review
1.1	25/05/2012	CE review
1.2	10/04/2013	Changed wording to include land and house information, as reviewed by Privacy Officer
2.0	23/6/2014	Review by Legal Risk Manager
2.1	24/6/2014	CE review
3.0	11/7/2014	Review and update to align with IIS Review outcomes and the Privacy Principles
3.1	17/7/2014	Audit & Risk Committee reviewed and recommended to the Board
3.2	18/7/2014	Board reviewed and approved.
4.0	9/6/2015	Scheduled review
4.1	15/06/2015	Governance Committee approved and recommended to the Board.
4.2	19/06/2015	Board approved
5.1	31/12/2015	Review and amendment in preparation for proactive release
5.2	25/01/2016	Legal review
5.3	03/02/2016	Governance Committee reviewed and recommended to the Board, subject to agreed amendments.
5.4	19/02/2016	Board approved.
6.0	1/07/2017	GM – Legal & Strategy Review
6.1	14/07/2017	Governance Committee reviewed and recommended to the Board
6.2	21/07/2017	Board approved.
7.0	05/03/2019	Review and amendment (including to reflect the composition of Board Committees) – Senior Legal Advisor
7.1	26/03/2019	CEO and GM – Legal & Strategy review.
7.2	18/04/2019	Board approved.
7.3	26/03/2020	Board approved.
7.4	25/05/2020	Personnel definition update.
8.0	07/06/2023	Policy rewritten, simplified, and updated. Board approved 28/06/2023