FMG Advice & Insurance

FMG Privacy Policy

1. Introduction

1.1 Purpose

This Policy forms part of FMG's Governance and Internal Control System.

FMG places a great deal of importance on the privacy of its Clients, Employees, and Third-Parties. This Policy has been developed to help you understand what information FMG collects, why it collects it, how it is collected and what it is to be used for.

It also has an effect on all technology devices owned by FMG and provided to its Employees. Any material uploaded, downloaded or stored on an FMG device is subject to this Policy and can be reviewed at any time by FMG. The Privacy Act 2020 does not protect personal information that has been:

- voluntarily stored or required to be stored on a device or system belonging to an Employer;
- voluntarily uploaded on social media platforms.

1.2 Scope

This Policy applies to all FMG Employees (current and former), Directors, Contractors, Clients (including prospects) and Third-Parties, and it may be varied from time-to-time.

1.3 Policy Objectives

Effective privacy controls and processes enable FMG to demonstrate:

- The privacy concepts and controls embedded in the organisation;
- Compliance with regulation and regulatory expectations;
- Assurance to the Chief Executive that risks to the Mutual's privacy are being adequately managed.

1.4 Governance

This Policy is owned by the Head of Regulation, Client Resolutions and General Counsel reporting through to the Enterprise Risk and Compliance Committee.

2. Privacy Principles

2.1 What is 'personal information'

Personal information is information about a living, identifiable individual and includes facts or an opinion which identifies the individual or is capable of identifying the individual. Individual means a natural person, other than a deceased natural person.

2.2 Collection of personal information

FMG collects personal information about its Clients, Employees, and Third-Parties and holds this information as a record. FMG will only collect personal information that is relevant to its business and its recruitment processes.

Wherever possible, FMG collects personal information about its Clients and Employees directly from them. If collecting personal information directly from Clients is not possible, FMG collects it from reputable external sources, such as the Ministry of Justice, Insurance Claims Register or the New Zealand Transport Agency's Motor Vehicle register etc. FMG notifies Clients about the direct and indirect collection of their information through its interactive voice recordings, disclaimers on its website, product application forms and Disclosure Statement. The information is then processed and stored by FMG to provide the associated services. FMG collects and records Clients' communications, including, but not limited to call recordings, emails and correspondence.

The type of personal information FMG collects includes, but is not limited to, Client names, contact details, physical address, insurance history and any additional information FMG requires to underwrite the relevant risk or provide advice or relevant services to Clients. Failure to obtain the information may result in the inability to underwrite risk, settle a claim or provide advice to Clients.

FMG may collect or be provided with personal information about another person or Third-Party who is involved in a claim made by a Client. FMG will use this information in accordance with this Policy.

When FMG collects personal information in relation to Natural Hazard Commission (NHC) or Natural Hazard Insurance (NHI) claims managed by FMG, that personal information can be used under the relevant provisions of the NHI Act and may be disclosed to the Insurance Claims Register and used to evaluate the provision of insurance, including for underwriting purposes. This information will be disclosed to NHC.

2.3 Storage and security of personal information

FMG uses Third-Party Providers to provision, store and process FMG's data. FMG and associated Third Parties store personal information collected and generated electronically on Cloud services located in countries that will protect the information with **comparable privacy safeguards** to those in New Zealand.

The information contained in these systems is strictly confidential and must not be accessed unless there is a **legitimate purpose**; this includes but is not limited to servicing a Client's account, managing a claim or complaint or using it for a legitimate purpose for which the information was collected.

Accessing personal information without a **legitimate purpose** constitutes a breach under the Privacy Act 2020.

2.4 Access to personal information

Clients, Employees, and Third-Parties have a right to access any personal information held about them in accordance with the Privacy Act 2020. However, they are entitled to, and can only access their own personal information.

FMG will respond to the person requesting access to the personal information within twenty (20) working days after a request is received. The response will include whether or not their personal information is held by FMG and if it can be disclosed to them.

2.5 Correction of personal information

An individual can request that their personal information held by FMG be corrected.

2.6 Accuracy of personal information

FMG relies on the accuracy of its Clients', Employees' and Third-Parties' personal information to efficiently provide its services. FMG is continually improving its Clients' data quality to ensure that any personal information it collects, uses, or discloses is accurate, complete and up-to-date.

2.7 Retention of personal information

FMG keeps personal information for seven (7) years or as long as there is a business need and/ or legislative requirements to retain it.

2.8 Limits on use of personal information

FMG will not use personal information obtained in connection with one purpose for any other purpose, unless it believes on reasonable grounds that any one of the exceptions set out in Principle 10 of the Privacy Act 2020 applies.

Using or accessing personal information for **a non-legitimate purpose** by FMG's Employees constitutes a breach of the Privacy Act. This will also potentially be regarded as misconduct, within the meaning of the Standards of Conduct Policy and the failure to adhere to other internal policies.

2.9 Disclosure of personal information

FMG may disclose personal information to some external service providers, including, but not limited to the Insurance Claims Register, Insurance Fraud Bureau, external assessors, repair agents, claims suppliers, claims repairers, payroll processors, superannuation providers, insurance companies underwriting personal insurance products, banks, Crown Departments, External Disputes Resolutions Schemes and Credit Check companies.

FMG will disclose personal information to such Third-Party Providers while the disclosure is in connection with the Client's insurance policy or FMG's internal processes, including, but not limited to recruitment.

FMG may also disclose personal information where it believes on reasonable grounds, that any one of the exceptions set out in Principle 11 of the Privacy Act 2020 applies.

In relation to an EQC/ NHC or NHI claim managed by FMG, personal information can be used under the relevant provisions of the NHI Act or EQC Act. and may be disclosed to the Insurance Claims Register and used to evaluate the provision of insurance, including for underwriting purposes.

3. Disputes

To make a privacy-related complaint, please contact FMG's Privacy Officer. Their contact details are:

FMG, PwC Centre, Level 1, 10 Waterloo Quay, Pipitea, Wellington 6011 (ATTENTION PRIVACY OFFICER) or 0800 366 466.

If you are not satisfied with FMG's response, you can refer your complaint to the Privacy Commissioner. Their contact details are available on their website www.privacy.org.nz.

4. Related Policies

Related policies include, but are not limited to:

Code of Ethics,

Information Management Policy,

Respectful Workplace Policy,

Standards of Conduct Policy,

Vehicle Policy.

5. Policy Compliance and Monitoring

FMG must ensure that it is able to demonstrate compliance to the principles and requirements of this Policy by implementing appropriate policies, processes, procedures and frameworks.

As a minimum the following compliance monitoring should be performed:

- Review and confirm compliance at least every three years.
- Review and approved annually by the Enterprise Risk and Compliance Committee.

Any non-compliance must be reported to the Head of Regulation, Client Resolutions and General Counsel and/ or Enterprise Risk and Compliance Committee.

6. Roles and Responsibilities

Role	Responsibilities
Enterprise Risk and Compliance Committee/ Head of Regulation, Client Resolutions and General Counsel/	• Reviews and approves the Policy; • Escalation point for breaches of the Policy.

Head of Compliance	
All Employees/ Contractors/ Directors	• Identify, measure, manage, monitor and report on all known privacy issues and/ or breaches. • Escalate as per above.

7. Definitions

Term	Definition
Employee	• Employee – any person who is employed in a part or full-time capacity.
Contractor	• Contractor – a Contractor that is in the position to act on behalf of FMG and which offers service to FMG in exchange for payment.
Director	• Director – a Member Director or Appointed Director per the definition of the Farmers' Mutual Group Act and Constitution.
Client	• Client – a Client of the Mutual that holds a policy of insurance.
Prospect	• Prospect – a potential Client of FMG that has provided personal information to the Mutual in relation to obtaining insurance cover.
Third-Party(ies)	• Third-Party(ies) - entities that may have a claim in relation to a Client's insurance policy.
Third-Party Providers	• Third Party Providers – those listed in the scope of this Policy.

Key Contacts	Executive Policy Owner: Chief Financial and Investments Officer Policy Managing Owner: Head of Regulation, Client Resolutions and General Counsel	
Approval Authority	Enterprise Risk and Compliance Committee	
Version / Dates	Date of last review: February 2026 Date of next review: February 2029	Prior Published: June 2025