SCG Data Processing Statement (Printing and Mailing Services)

Version	Date	Description	Author
1.0	24/08/2022	Initial Creation	Zephyr Brown
2.0	25/11/2025	Updated with limitation on AI use	Zephyr Brown

1.0 Purpose and Scope

This Data Processing Statement describes how SCG Limited ("SCG") processes personal information on behalf of its clients in connection with printing, production, and mailing services.

SCG acts as a data processor/service provider when handling personal information supplied by clients for the purpose of producing and distributing printed communications to participants, customers, members, or other intended recipients.

2.0 Purpose Limitation

SCG processes personal information solely for the purpose of producing, printing, and delivering the materials specified in the client's instructions or contract.

Personal information provided for distribution purposes will not be:

- Used for marketing or promotional purposes by SCG
- Used for analytics, profiling, enrichment, or data mining
- Sold, rented, or otherwise commercialised
- Retained for any unrelated internal use
- Shared with third parties for their independent purposes

Processing is strictly limited to what is necessary to fulfil the agreed printing and mailing services.

3.0 Lawful Processing

SCG processes personal information only:

- In accordance with documented client instructions
- In compliance with the New Zealand Privacy Act 2020
- In accordance with applicable contractual obligations

Clients remain responsible for ensuring that the collection and provision of personal information to SCG complies with applicable privacy laws.

4.0 Limitation on Artificial Intelligence (AI) Use

SCG does not use client personal information supplied for printing and mailing services to:

- Train, fine-tune, or improve artificial intelligence (AI) or machine learning models
- Develop, test, or enhance automated decision-making systems
- Generate synthetic data sets
- Perform behavioural profiling or predictive analytics

Client data is not uploaded to publicly available generative AI systems or external AI platforms for processing.

If AI-enabled tools are used within SCG's internal systems (for example, workflow automation or quality assurance), such tools operate strictly within SCG's secure environment and are used solely to facilitate the contracted service. They do not retain, learn from, or repurpose client personal information beyond the scope of the specific job being performed.

SCG will not introduce AI-based processing of client personal information that materially changes the nature of processing without prior client notification and, where required, contractual agreement.

5.0 Access Controls and Confidentiality

Access to personal information is restricted to authorised SCG personnel and approved subcontractors who:

- Require access to fulfil the service
- Are bound by confidentiality obligations
- Receive appropriate data protection and security training

SCG maintains appropriate physical, technical, and organisational safeguards to protect personal information from unauthorised access, disclosure, alteration, or destruction.

6.0 Sub-Processors

Where necessary to deliver mailing services (e.g., postal or courier providers), SCG may engage approved third-party service providers. Such providers are engaged solely for the purpose of

completing the distribution service and are not permitted to use the data for their own purposes.

7.0 Data Retention

Unless otherwise specified in a client contract:

- Distribution data is retained for three (3) months following completion of the printing and mailing service.
- This retention period supports reconciliation, reprints, delivery investigations, and audit requirements.
- Where a client agreement or applicable law requires a longer retention period, SCG will retain the data in accordance with those requirements.

At the conclusion of the applicable retention period, personal information is securely deleted or destroyed in accordance with SCG's information governance and security practices.

8.0 Data Security

SCG implements appropriate security measures, including:

- Secure production environments
- Access controls and authentication mechanisms
- Secure file transfer methods (where applicable)
- Controlled physical access to facilities
- Secure data destruction procedures

Security measures are proportionate to the nature and sensitivity of the information processed.

9.0 Data Subject Requests

If SCG receives a request from an individual relating to personal information processed on behalf of a client, SCG will promptly refer to the relevant client unless otherwise instructed.

10.0 Data Breach Notification

In the event of a confirmed privacy breach affecting client data, SCG will notify the affected client withing 24 - 48hrs and cooperate in good faith to support investigation and any required regulatory notifications.

11.0 Return or Destruction of Data

Upon completion of services and expiry of the applicable retention period, personal information will be securely deleted or destroyed unless:

- A longer retention period is required under contract; or
- Retention is required by law.

12.0 Applicability of Other Policies

This statement should be read in conjunction with:

- SCG Privacy Policy
- SCG Information Security Policy
- SCG Acceptable Use Policy
- SCG Incident Response Plan
- SCG Cloud Services Policy
- SCG Remote Work Security Guidelines
- SCG AI & Data Handling Guidelines
- SCG Outsourcing and Vendor Management Policy

13.0 Revision History

- Version 1.0 — 24/08/2022 — Initial creation
- Version 2.0 — 25/11/2025 — Updated with limitation on AI use