Personal Information Management Policies of

RGA Reinsurance Company Korea Branch

The RGA Reinsurance Company Korea Branch (hereinafter "Company") has the following policy to protect personal information, privacy, and the interests of a subject of information and to address claims or grievances of a subject of information related to personal information pursuant to the Personal Information Protection Act (hereinafter "The Act").

Definitions:

"Data Subject" An individual who can be identified, whether directly or indirectly, by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, or cultural or social identity.

"Personal Data" Information from which an individual can be identified, either from the data itself or from the data in combination with other information.

"Workforce Member" Any regular or temporary employee of the Company, including any contractor, consultant or other individual representing or acting on behalf of the Company.

"Non-Workforce Member" Any individual who is not a Workforce Member as noted above.

Article 1. Purpose of Personal Information Management

Personal Data of non-Workforce Members may be processed and subsequently used or further communicated only for purposes outlined below or as subsequently authorized by the Data Subject:

- Providing underwriting administration services
- Providing assumed cession administration services
- Providing claims management administration services
- Providing contracts of further reinsurance
- Providing technical support to the administrative functions and systems
- Enabling Head Office of Company to maintain and carry out audit controls
- Ensuring compliance of the Company with laws of the State of Missouri (USA) and any other applicable international, national, federal, state, and local laws as well as international treaties, where applicable Decision-making with regard to the development and operation of the Company and Head Office
- Used on an ongoing basis for the limited purposes of research and development
- Providing data for valuation and pricing processes

Personal Data of Workforce Members may be processed and subsequently used or further communicated to authorized individuals only for employment purposes including, but not limited to, recruiting, hiring, background checks, pay and benefits administration, performance evaluations, crisis handling, separation from the Company, and where properly approved, personnel investigations.

The following RGA Entities currently access data on behalf of the Company:

RGA Reinsurance Company – Head Office, St. Louis, Missouri, USA

RGA Reinsurance Company – Tokyo Branch, Japan

RGA Reinsurance Company – Hong Kong Branch, Hong Kong

RGA International Corporation, Toronto, Canada

RGA Reinsurance Company of Australia Limited, Sydney, Australia

RGA International Division Sydney Office Pty Limited, Sydney, Australia

Article 2. Personal Information Managed by the RGA Korea Branch

Personal data transferred concern the following categories:

Date of birth, gender, marital status, country, national insurance number (in certain jurisdictions only), prefix, first name, middle name, last name, suffix, current address, employer, business title, business type, reinsurance amount, personal net worth, benefit type, insurance type, claims history, personal identifiers.

The use of "linking identifiers" for the purposes of de-personalizing data managed by the Company will be used in such a manner as to render the Personal Data itself depersonalized for the purposes of this Policy. "Linking identifiers" are used as a means to create a link between the original data information and the "new" data record. The use of Linking Identifiers is undertaken before any data is used or transferred to any third party. The "new" data record would be considered depersonalized and would not contain Personal Data as such is defined under the Act.

Article 3. Retention Period for Information Management and Storage

Personal Data must be accurate and, where necessary, kept up to date. The Personal Data must be adequate, relevant, and not excessive in relation to the purposes for which it is transferred and further processed.

Article 4. Provision of Information to a Third Party

In principle, the Company will manage Personal Data only for the purpose described in Article 1 (Purpose of Managing Personal Information) and will not manage it beyond its original purpose or disclose it to a third party without the consent of a Data Subject. Under traditional best practices in the reinsurance industry globally, the Company as the reinsurer relies upon the consent obtained by the ceding company from any Data Subject as part of the initial application process to fulfill the purposes of consent for the transfer of any data, including specifically, Personal Data, as it relates to any transactions between the Company and a ceding insurance company. The Company applies the provisions of this Personal Information Management Policy to all third parties with which it does business.

However, for the following, Personal Data can be provided:

- Where it is unavoidable to comply with specific provisions of the law and regulations, or meet the requirements of legal obligations
- Where it is unavoidable to enable public authorities to do their duty according to the law
- Where it is accepted to manage personal information for a subject of information or a third party's urgent needs related to his/her life, body or property when the prior consent of subject of information (including his/her representative) cannot be obtained for reasons of an inability to express will or an unknown contact information

Article 5. Rights and Duties of a Subject of Information and How to Exercise Them

If Data Subjects are entitled to be provided with information about the purposes of processing and transfer of data related to them under the relevant local legislation, any Workforce Member who receives such a request must contact the local Company compliance officer prior to responding to any request from a Data Subject.

Where data is processed for employment purposes, Workforce Members may request to inspect and verify the accuracy of non-Confidential information in the presence of a Human Resources representative. However, Workforce Members may not remove any item from a file or review a file that is not their own without the Company's approval unless applicable law provides otherwise.

Article 6. Destruction of Personal Information

In principle, the Company will destroy Personal Data without delay when its purpose is achieved. Destruction will be performed as follows:

- Procedure: After its purpose is achieved, Personal Data will be transferred to a separate database (or separate file in case of printout) for storage or destruction according to the Company's practice or applicable laws. Personal Data transferred to the database will not be managed for any other purposes than those specified in the law.
- Period: When Personal Data expires, it will be destroyed in accordance with the Company's usual data retention destruction period of five years after its expiration. If Personal Data becomes unnecessary as its purpose is achieved or relevant service is closed, it will be destroyed in accordance with the Company's usual data retention destruction period of five years when it has been found to be unnecessary.
- Printed Personal Data will be shredded or incinerated.
- Electronic files containing Personal Data will be destroyed in an unrecoverable way.

Article 7. Measures for Securing the Safety of Personal Information

The Company has technical and organizational security measures in place that are adequate to address the risks presented by processing, including measures against accidental or unlawful destruction, loss, alteration, unauthorized disclosure or access. All use of or access to Company data, which specifically includes any Personal Data collected or received, must be based on one's need to know the underlying information. According to Article 29 of the

Act, the Company has undertaken the following technical, administrative and physical measures for securing the safety of personal information.

- Minimizing the number of employees who have access to personal information: Only the relevant employee can access personal information.
- Regular audit: An in-house audit is conducted annually for the security of personal information.
- Internal management plan: An internal management plan is established and practiced for the security of personal information.
- Limit on access to personal information: Rights for access to the personal information database are allowed, modified and deleted for the security of personal information. A firewall is in place to prevent unauthorized access from outside.
- Training of all Workforce Members regarding best practices around information security and the handling of Personal Data.

The Company shall consider additional and further measures (e.g., relating to security) and implement those necessary to protect Personal Data.

Article 8. Personal Information Protection Manager

The Company has appointed the following personnel to protect personal information and handle relevant complaints according to Article 31 (1) of the Personal Information Protection Act.

Department: Compliance

Personal Information Protection Manager: Ray Keuntaeg Lee

Tel: 02-6730-1350

E-mail: rlee2@rgare.com

Article 9. Amendment of Personal Information Management Policy

This policy becomes effective from the date of enforcement. If an addition, deletion or alteration is made according to applicable laws and guidelines, it will notify all subjects by updating the public website of the Company.

Article 10. Remedy for Infringement

To remedy infringement of personal information, a subject of information can request dispute mediation with Korean Information Security Agency (KISA) Personal Information Dispute Mediation Committee for settlement or consultation.

Article 11. Enforcement Date

This policy has been enforced since 30th September, 2011 (Initial enforcement).