EU Binding Corporate Rules
RGA Controller Policy (Summary Statement)

Effective November 2024

PART I - INTRODUCTION

The RGA group companies are committed to the protection of the personal information we collect, store, use and share in connection with the services we provide and we believe strongly in upholding the highest standards in respect of data privacy.

This statement explains RGA's approach to compliance with data protection law when processing personal information for our own purposes and where such personal information originates in the EEA, specifically with regards to transfers of personal information between RGA BCR members.

RGA's Controller Policy applies to all personal information that we process as a controller for the purposes of carrying out legitimate business activities, employment administration, customer management and vendor management. As such, the personal information to which the Controller Policy applies includes: RGA workforce member personal information; customer relationship management data; policyholder data; supply chain management data; and other third party data.

All RGA BCR members and their workforce must comply with and respect the Controller Policy when processing personal information, irrespective of the country in which they are located.

The Controller Policy applies only to personal information that RGA processes as a controller (for our own purposes). We have a separate BCR: Processor Policy that applies when we process personal information as a processor to provide a service to a third party (such as a customer).

If you have any questions about the provisions of the Controller Policy, your rights under the Controller Policy, or any other data protection issues, you may contact RGA's Global Security and Privacy Office using the contact information below:

Attention: Global Security and Privacy Office
Email: Privacy@rgare.com
Address: 16600 Swingley Ridge Road, Chesterfield, Missouri, 63017 USA

PART II - CONTROLLER OBLIGATIONS

The Controller Policy applies in all situations where an RGA BCR member processes personal information as a controller. Part II of the Controller Policy is divided into three sections:

- Section A identifies and describes the data protection principles that RGA observes at any time we process personal information as a controller.
- Section B specifies the practical commitments to which RGA adheres in connection with the Controller Policy.
- Section C describes the third party beneficiary rights RGA provides to individuals under the Controller Policy.

Section A: Basic Principles

Rule 1 – Lawfulness of processing: RGA will ensure that all processing is carried out in accordance with applicable data protection laws.

Rule 2 – Fairness and transparency: RGA will ensure individuals are provided with a fair notice and sufficient information regarding the processing of their personal information.

Rule 3 – Purpose limitation:

a) RGA will obtain and process personal information only for those purposes outlined in the privacy information provided to individuals in accordance with its transparency obligations.
b) RGA will process personal information only for specified, explicit and legitimate purposes and not further process that information in a manner that is incompatible with those

purposes unless such further processing is consistent with the applicable data protection law of the country in which the personal information was collected.

Rule 4 – Data minimisation and accuracy:

- **a)** RGA will keep personal information accurate and up to date.
- **b)** RGA will only process personal information that is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

Rule 5 – Limited retention of personal information:

- **a)** RGA will only keep personal information for as long as is necessary for the purposes for which it is collected and further processed.

Rule 6 – Security and confidentiality:

- **a)** RGA will implement appropriate technical and organizational measures to ensure a level of security around personal information that is appropriate to the risk for the rights and freedoms of the individuals.
- **b)** RGA will ensure that providers of services to RGA also adopt appropriate and equivalent security measures.
- **c)** RGA will comply with data security breach notification requirements under applicable data protection laws.

Rule 7 – Honouring individuals' data privacy rights:

- **a)** RGA will adhere to the Data Subject Rights Procedure (Controller) and will respond to any requests from individuals to access their personal information in accordance with applicable data protection laws.
- **b)** RGA will also deal with requests to rectify or erase personal information, or to restrict or object to the processing of personal information, and to exercise the right of data portability in accordance with the Data Subject Rights Procedure (Controller).

Rule 8 – Ensuring adequate protection for transborder transfers: RGA will not transfer personal information to third countries outside the EEA without ensuring adequate protection for the personal information in accordance with the standards set out by the Controller Policy.

Rule 9 – Safeguarding the use of sensitive personal information: RGA will only process sensitive personal information collected in the EEA where the individual's explicit consent has been obtained, unless RGA has an alternative legitimate basis for doing so consistent with the applicable data protection laws of the EEA country in which the personal information was collected.

Rule 10 – Legitimising direct marketing: RGA will provide customers with the opportunity to opt-in to receiving marketing information and will ensure that the right of individuals to object to the use of their personal information for direct marketing purposes is honoured.

Rule 11 – Automated individual decisions: Individuals have the right not to be subject to a decision based solely on automated processing and to contest such decision.

Section B: Practical Commitments

Rule 12 – Compliance:

- **a)** RGA will have appropriate workforce members and support to ensure and oversee privacy compliance throughout the business.
- **b)** RGA will maintain records of the processing activities it carries out for its own purposes.
- **c)** RGA carries out a data protection impact assessment where the processing is likely to result in a high risk for the data subjects.

Rule 13 – Privacy training: RGA will provide appropriate and up-to-date privacy training to workforce members who have permanent or regular access to personal information, who are involved in the processing of personal information or in the development of tools used to process personal information in accordance with the Privacy Training Program (Controller).

Rule 14 – Audit: RGA will verify compliance with the Controller Policy and will carry out data protection audits on a regular basis in accordance with the Audit Protocol (Controller).

Rule 15 – Complaint Handling: RGA will ensure that individuals may exercise their right to file a complaint and will handle such complaints in accordance with the Complaint Handling Procedure (Controller).

Rule 16 – Cooperation with data protection authorities: RGA agrees to comply with the advice and to abide by a formal decision of any competent supervisory authority on any issues relating to the interpretation and application of the Controller Policy under applicable data protection laws, notwithstanding its right to appeal such decisions in accordance with applicable procedural laws, as set out in the Cooperation Procedure (Controller).

Rule 17 – Updates to the Controller Policy: RGA will report changes to the Controller Policy to the supervisory authority in accordance with the Updating Procedure (Controller).

Rule 18 – Non-Compliance with the Controller Policy: RGA will ensure that where a data importer is in breach of, or unable to comply with, the Controller Policy for any reason, that importer will inform the data exporter.

Rule 19 – Action Where National Legislation Prevents Compliance with the Controller Policy: RGA will ensure that where it believes legislation applicable to it prevents it from fulfilling its obligations under the Controller Policy or such legislation has a substantial effect on its ability to comply with the Controller Policy (which may include a legally binding request for disclosure of Personal Information by a law enforcement authority or state security body in a third country), the BCR member acting as data importer will promptly inform: the BCR members acting as data exporter; the Chief Privacy Officer; and RGA International Reinsurance Company dac; unless otherwise prohibited by a law enforcement authority.

Rule 20 - Action Where Government Access Request Prevents Compliance with the Controller Policy: If a BCR member acting as data importer receives a legally binding government access request for disclosure of personal information, the importer will promptly notify: the BCR member acting as data exporter and, where possible, the data subject (if necessary with the help of the data exporter), unless prohibited from doing so by a law enforcement authority or agency.
The importer will also notify the exporter if the importer becomes aware of any direct access by public authorities to personal information. If prohibited from performing any of the notification(s), the data importer will use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as possible, and as soon as possible, to the data exporter and/or the data subject.

Section C: Third Party Beneficiary Rights

Under applicable data protection laws, individuals whose personal information is processed in the EEA by an RGA BCR member acting as a controller (an "**EEA Entity**") and/or transferred to a BCR member located outside the EEA (and which BCR member may transfer onward to any other BCR member outside the EEA) under the Controller Policy (a "**Non-EEA Entity**") have certain rights. The principles that individuals may enforce as third party beneficiaries are those that are set out in the Intra-Group Agreement (EU), available upon request, and under the following sections of the Controller Policy:

- Part I (Background and Scope);
- Part II Section A (Basic Principles); and
- Part II Section B (Practical Commitments) Rules:
    - 12B (Records),
    - 15 (Complaint Handling, see Appendix 6 for the procedure),
    - 16 (Cooperation with Supervisory Authorities, see Appendix 7 for the procedure),
    - 17 (Updating Procedure, see Appendix 8 for the procedure),
    - 19 (National Legislation preventing compliance), and
    - 20 (Government Access Request preventing compliance)

- Part II Section C (Third Party Beneficiary Rights):

In such cases, the individual's rights are as follows:

- *Complaints*: Individuals may submit complaints to any EEA Entity in accordance with the Complaint Handling Procedure (Controller) (Appendix 6) and may also lodge a complaint with an EEA supervisory authority in the jurisdiction of their habitual residence, place of work, or place of the alleged infringement;
- *Proceedings*: Individuals have the right to an effective judicial remedy if their rights under the Controller Policy have been infringed as a result of the processing of their personal information in non-compliance with the Controller Policy. Individuals may bring proceedings against RGA International Reinsurance Company dac (Ireland) to enforce compliance with the Controller Policy, whether in relation to non-compliance by an EEA Entity or Non-EEA Entity, before the competent courts of the EEA Member State (either the jurisdiction where the controller or processor is established or where the individual has his/her habitual residence);
- *Compensation*: Individuals who have suffered material or non-material damage as a result of an infringement of the Controller Policy have the right to receive redress and compensation from the controller or processor for the damage suffered. In particular, in case of non-compliance with the Controller Policy by a Non-EEA Entity, individuals may exercise these rights and remedies against RGA International Reinsurance Company dac (Ireland) and, where appropriate, receive compensation from RGA International Reinsurance Company dac (Ireland) for any material or non-material damage suffered as a result of an infringement of the Controller Policy, in accordance with the determination of a court or other competent authority; and
- *Transparency*: Individuals also have the right to obtain a copy of the Controller Policy and the Intragroup Agreement entered into by RGA or any other EEA Entity on request.
- *Representation*: Individuals may be represented by a not-for-profit body, organization or association in both *Complaints* and *Proceedings* as described above.

Where individuals can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a non-compliance with the Controller Policy, it will be for RGA International Reinsurance Company dac (Ireland) to prove that the Non-EEA Entity was not responsible for the non-compliance with the Controller Policy giving rise to those damages or that no such non-compliance took place.

PART III – APPENDICES

Appendix 1 – List of RGA BCR Members (Controller): A list of the RGA entities bound by the Controller Policy.
Appendix 2 – Data Subject Rights Procedure (Controller): This document outlines how RGA will respond to any data subject rights requests received from individuals whose personal information we process and transfer under the Controller Policy.
Appendix 3 – Privacy Compliance Structure (Controller): This document outlines RGA's global compliance structure in respect of data protection and privacy.
Appendix 4 – Privacy Training Program (Controller): This document outlines how RGA provides training to its workforce on the requirements of the Controller Policy.
Appendix 5 – Audit Protocol (Controller): This document outlines the formal assessment process adopted by RGA to ensure compliance with the Controller Policy.
Appendix 6 – Complaint Handling Procedure (Controller): This document outlines the practical steps individuals whose personal information is processed by RGA under the Controller Policy may take to submit complaints and how such complaints are dealt with by RGA.
Appendix 7 – Cooperation Procedure (Controller): This document outlines the way in which RGA will cooperate with the EEA supervisory authorities in relation to the Controller Policy.
Appendix 8 – Updating Procedure (Controller): This document outlines the way RGA will communicate changes to the Controller Policy to the EEA supervisory authorities, individual data subjects, controllers and BCR members.
Appendix 9 – In Scope Data Transfers (Controller): This document outlines the personal data transfers covered by the Controller Policy including the entities and their roles, and the countries, purposes, types of data subjects and data elements involved.

RGA reserves the right to amend its BCRs and/or this BCR Summary Statement without prior notice to reflect technological advancements, legal and regulatory changes, and good business practices. If we change our privacy practices or our BCRs, an updated version of this BCR Summary Statement will

reflect those changes and we will inform you of such changes by updating the effective date at the top of this BCR Summary Statement.