September 2023

GLOBAL BINDING CORPORATE RULES (UK):

CONTROLLER POLICY

Contents

INTRODUCTION

This Global Binding Corporate Rules (UK): Controller Policy ("**Controller Policy**") establishes RGA's approach to compliance with Applicable Data Protection Laws when Processing Personal Information for its own purposes and where such Personal Information originates in the United Kingdom, specifically with regard to transfers of Personal Information between members of the RGA group of entities where the recipient is not in an 'Adequate' jurisdiction. In this Controller Policy, we use "**RGA**" to refer to RGA group members ("**Group Members**").

This Controller Policy applies to personal data transfers where the non-UK RGA recipient entity is in a jurisdiction not granted UK 'Adequate' status (in which case Adequacy will be the transfer mechanism). It describes how RGA will comply with Applicable Data Protection Laws with respect to Processing Personal Information where an RGA entity is either the Controller or an internal Processor for another RGA entity which is the Controller.

RGA's Global Binding Corporate Rules (UK): Processor Policy describes how RGA will comply with Applicable Data Protection Laws with respect to processing Personal Information as a Processor. The Information Commissioner has regulatory oversight of the functioning of the RGA Binding Corporate Rules (UK) and RGAs compliance to this Policy. This Controller Policy does not replace any specific data protection requirements that might apply to a business area or function.

This Controller Policy is accessible on RGA's corporate website at: www.rgare.com.

DEFINITIONS

For the purposes of this Controller Policy, the terms below have the following meaning:

"Applicable Data Protection Law(s)"	means the data protection laws in force in the United Kingdom;
"Adequacy", "Adequate Status", "Adequate level of protection"	the UK Government can assess whether another country, territory or an international organisation provides an adequate level of data protection compared to the UK. Some countries may have a substantially similar level of data protection to the UK. In these cases, the Government can make UK adequacy regulations. This allows organisations to send personal data to that country, territory or international organisation if they wish.
"Controller"	means the natural or legal person which, alone or jointly with others, determines the purposes and means of the Processing of Personal Information. For example, RGA is a Controller of its HR records and CRM records;
"Group Members"	means any of the members of RGA's group of companies listed in Appendix 1;
"**Client"**	refers to the third-party Controller that shares information with RGA for reinsurance related business purposes. It includes RGA's third-party Clients when we, as Controller, Process Personal Information as independent Controllers during the course of providing business services to them;
"Information Commissioner"	has the meaning given to it by section 114 of the Data Protection Act 2018;
"Personal Information"	means any information relating to an identified or identifiable natural person ("**Data Subject**"). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

"Processing", "Processed", "Process", "Processes"	means any operation or set of operations which is performed on Personal Information or on sets of Personal Information, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;
"Processor"	means a natural or legal person which processes Personal Information on behalf of a Controller. For the purposes of this Controller Policy, a Processor may be either a third party service provider or another Group Member;
"RGA"	Reinsurance Group of America Inc. and all its subsidiaries collectively (the Group as a whole);
"Sensitive Personal Information"	means information that relates to a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation. It also means information about a Data Subject's criminal convictions, offences or related security measures as well as any other information deemed sensitive under Applicable Data Protection Laws;
"UK Court"	means a Court in the United Kingdom in accordance with section 180 of the Data Protection Act 2018;
"UK GDPR"	means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 as modified by the Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2019 as amended by the Data Protection, Privacy and Electronic Communications (Amendments etc)(EU Exit) Regulations 2020; and

"United Kingdom"	as used in this Controller Policy, United Kingdom (also denoted as "**UK**") refers to the country that consists of England, Scotland, Wales and Northern Ireland;
"Workforce Members"	refers to all employees, new hires, individual contractors and consultants, and temporary members of the workforce engaged by any Group Member. All Workforce Members must comply with this Controller Policy.

PART I: BACKGROUND AND SCOPE

WHAT IS DATA PROTECTION LAW?

Applicable Data Protection Laws give Data Subjects certain rights in connection with the way their Personal Information is Processed. If organizations do not comply with Applicable Data Protection Laws, they may be subject to sanctions and penalties imposed by the Information Commissioner and UK Courts. The Processing of any Personal Information of a natural person ('Data Subject') by or on behalf of RGA globally remains protected by Applicable Data Protection Laws by the application of this Controller Policy.

According to Applicable Data Protection Laws, when an organization determines the purposes for which Personal Information are to be Processed and the means by which the Personal Information are Processed, that organization is deemed to be a *Controller* of that Personal Information and is therefore primarily responsible for meeting the legal requirements under Applicable Data Protection Laws.

On the other hand, where an organization Processes Personal Information only on behalf of a Controller, that organization is deemed to be a *Processor* of the Personal Information. In those cases, whoever the Controller of the Personal Information is will be primarily responsible for meeting the legal requirements.

HOW DOES DATA PROTECTION LAW AFFECT RGA INTERNATIONALLY?

Applicable Data Protection Laws permit some transfers of Personal Information outside the UK based on Adequacy regulations. Only certain non-UK countries in which RGA operates, and to which Personal Information may be transferred from the UK, are regarded by the UK Government Secretary of State as providing an adequate level of protection for Data Subjects' privacy and data protection rights, i.e. Adequate.

In the absence of Adequacy regulations permitting a transfer then RGA will base its transfers (those identified in Appendix 9 to this policy) on this Controller Policy.

WHAT IS RGA DOING ABOUT IT?

RGA must take proper steps to ensure that it Processes Personal Information in a legitimate, fair and lawful manner wherever it operates or undertakes business. This Controller Policy sets out a framework to satisfy Applicable Data Protection Law requirements and, in particular, to provide an adequate level of protection for all Personal Information Processed by or on behalf of all Group Members located within and outside of the UK.

SCOPE OF THIS CONTROLLER POLICY

This Controller Policy applies to all Personal Information that RGA Processes as a Controller for the purposes of carrying out legitimate business activities, employment administration, client management and vendor management. As such, the Personal Information to which this Controller Policy applies includes:

- RGA Workforce Members: including Personal Information past and current RGA Workforce Members, individual consultants, independent contractors, temporary Workforce Members, and job applicants;

- Client relationship management data: including Personal Information of representatives of business clients who use RGA's business services and client support platform, event attendees, survey participants and potential business clients;

- Policyholder related data: including Personal Information of Data Subjects who are parties to or beneficiaries of primary individual or group insurance and pension policies;

- Supply chain management data: including Personal Information of individual contractors and of account managers and staff of third-party suppliers who provide services to RGA; and

- Other third-party data: including any other Personal Information related to its Directors or unaffiliated third parties such as analytics providers, consultants, investigators, insurance brokers, lawyers, and physicians with whom RGA engages for legitimate business-related purposes.

RGA will apply this Controller Policy in all cases where it Processes Personal Information through both manual and automated means and to all transfers between Group Members (including personal data subject to UK GDPR that does not originate in the UK).

MANAGEMENT COMMITMENT AND CONSEQUENCES OF NON-COMPLIANCE

RGA's management is fully committed to ensuring that all Group Members and their Workforce Members comply with this Controller Policy at all times.

All Group Members and their Workforce Members must comply with and respect this Controller Policy when Processing Personal Information, irrespective of the country in which they are located. All Group Members that engage in the processing of Personal Information as a Controller (or as a Processor acting on behalf of another Group Member that is the Controller) must comply with the Rules set out in **Part II** of this Controller Policy together with the policies and procedures set out in the appendices in **Part III** of this Controller Policy.

In recognition of the gravity of these risks, Workforce Members who do not comply with this Controller Policy may be subject to disciplinary action, up to and including dismissal.

RELATIONSHIP BETWEEN THE CONTROLLER AND PROCESSOR POLICIES

This Controller Policy applies only to Personal Information that RGA Processes as a Controller and is then transferred to Group Members in their capacity as either a Controller or a Processor.

RGA has a separate Global Binding Corporate Rules (UK): Processor Policy that applies when it Processes Personal Information as a Processor on behalf of a Controller that is not a Group Member (i.e. a third party Controller).

- When a Group Member Processes Personal Information as a Processor on behalf of a third-party Controller, it must comply with the Processor Policy, or

- When a Group Member Processes Personal Information as a Processor on behalf of another Group Member that is the Controller, it must comply with this Controller Policy.

Some Group Members may Process Personal Information as Controllers under some circumstances and as Processors under different circumstances. Such Group Members must comply with this Controller Policy and the Processor Policy, as appropriate.

If at any time it is not clear to a Group Member as to what its legal status as Controller or Processor would be and which policy applies, such Group Member must contact the Chief Security and Privacy Officer whose contact details are provided below.

FURTHER INFORMATION

If you have any questions regarding the provisions of this Controller Policy, your rights under this Controller Policy, or any other data protection issues, you may contact the Chief Security and Privacy Officer using the contact information below. All inquiries will be dealt with directly by the Chief Security and Privacy Officer or delegated to the RGA Workforce Member or department best positioned to address such inquiry.

Attention:	Chris Cooper, Vice President, Global Chief Security and Privacy Officer
Email:	ccooper@rgare.com
Address:	16600 Swingley Ridge Road, Chesterfield, Missouri, 63017, USA

The Chief Security Privacy Officer is responsible for ensuring that any changes to this Controller Policy are communicated to all Group Members, the Information Commissioner and to Data Subjects whose Personal Information is Processed by RGA in accordance with Appendix 8.

If you have concerns or would like more information regarding the way in which RGA Processes your Personal Information, you are encouraged to submit a request and/or complaint through RGA's separate Complaint Handling Procedure (UK) (Controller), which is outlined in Part III, Appendix 6.

PART II: CONTROLLER OBLIGATIONS

This Controller Policy applies in all situations where a Group Member Processes Personal Information as a Controller or on behalf of another Group Member that is the Controller.

Part II of this Controller Policy is divided into three sections:

- Section A identifies and describes the data protection principles that RGA observes at any time it Processes Personal Information as a Controller.
- Section B specifies the practical commitments to which RGA adheres in connection with this Controller Policy.
- Section C describes the third-party beneficiary rights RGA provides to Data Subjects under this Controller Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS OF PROCESSING

Rule 1 – RGA will ensure that all Processing is carried out in accordance with Applicable Data Protection Laws.

RGA will comply with all applicable local legislation governing the protection of Personal Information and will ensure that all Personal Information is Processed in accordance with Applicable Data Protection Laws.

As such:

- to the extent that any applicable local legislation governing the protection of Personal Information requires a higher level of protection than is provided for in this Controller Policy, RGA acknowledges that it will take precedence over this Controller Policy; but
- where there is no applicable local legislation governing the protection of Personal Information, or where the local law does not meet the standards set out by the Controller Policy, RGA will Process Personal Information in accordance with the Rules in this Controller Policy.

RGA will ensure all Processing of Personal Information has a legal basis (as described in the publicly available Privacy Notice) in compliance with Applicable Data Protection Laws and any applicable local legislation governing the protection of personal information where the data is originally collected.

RULE 2 – FAIRNESS AND TRANSPARENCY

Rule 2 – RGA will ensure Data Subjects are provided with a fair notice and sufficient information regarding the Processing of their Personal Information.

RGA shall implement appropriate measures to inform Data Subjects about the Processing of their Personal Information in a concise, transparent, intelligible and easily accessible form. This information shall be provided in writing, or by other means, including, where appropriate, by electronic means.

Data Subjects also have the right to obtain a copy of the Controller Policy and the Intragroup Agreement entered into by RGA or any other UK BCR entity on request. This Controller Policy (and any updates thereof) will be accessible on RGA's website at http://www.rgare.com.

UK GDPR Article 13 - Personal Information that are obtained directly from Data Subjects:

Where required by Applicable Data Protection Laws, RGA shall, at the point it collects Personal Information from Data Subjects, ensure Data Subjects have the following information necessary to ensure fair and transparent Processing in respect of the Data Subject (unless such Data Subjects have already received the information):

- the **identity** of the Controller and its contact details;
- the contact details of the **Data Protection Officer**, where applicable;
- the **purposes** of the Processing for which the Personal Information is intended as well as the **legal basis** for the Processing;
- where the Processing is based on RGA's or a third party's legitimate interests, the **legitimate interests** pursued by RGA or by the third party;

- the **recipients** or categories of recipients of their Personal Information (if any); and

- where applicable, the fact that a Group Member in the UK intends to **transfer** Personal Information to a Group Member outside the UK including a reference to the appropriate safeguards that are put in place (i.e. this Controller Policy, entering into standard contractual clauses with a third party who is receiving the data, or ensuring that such third party can provide adequate protection through other means (e.g. approved code of conduct, approved certifications mechanism), as per Rule 8 below), and the means by which to obtain a copy of the Controller Policy (and information regarding any other appropriate safeguards put in place) or where it has been made available.

In addition to the information above, where required by Applicable Data Protection Laws, RGA shall, at the time when Personal Information is obtained, provide Data Subjects with the following further information necessary to ensure fair and transparent Processing:

- the **period** for which the Personal Information will be stored, or if that is not possible, the criteria used to determine that period;

- information about the **Data Subjects' rights** to request access to, rectify or erase their Personal Information, as well as the right to restrict or object to the Processing, and the right to data portability;

- where the Processing is based on consent, the existence of the right to **withdraw consent** at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;

- the **right to lodge a complaint** with the Information Commissioner;

- whether the provision of Personal Information is a **statutory or contractual** requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Information and the possible consequences of failure to provide such information; and

- the existence of **automated decision-making**, including profiling, and, where such decisions may have a legal effect or significantly affect the Data Subjects whose Personal Information is collected, any meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for those Data Subjects.

<u>UK GDPR Article 14 - Personal Information that are not obtained from Data Subjects</u>:

Where Personal Information has not been obtained directly from the Data Subjects concerned, and where Applicable Data Protection Laws require, RGA shall provide those Data Subjects (unless (a) the Data Subject already has the information; (b) the provision of such information proves impossible or would involve a disproportionate effort; or (c) as otherwise permitted by Applicable Data Protection Laws), with the following information:

- the information specified above (UK GDPR Article 13 - Personal Information that are obtained directly from Data Subjects),

- the **categories** of Personal Information that are being Processed; and

- from which **source** the Personal Information originates, and if applicable, whether it came from publicly accessible sources.

RGA shall provide this information to those Data Subjects:

- within a reasonable period of time after obtaining the Personal Information, but at the latest within one month, having regard to the specific circumstances in which the Personal Information are processed;

- if the Personal Information are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or if a disclosure to another recipient is envisaged, at the latest when the Personal Information are first disclosed.

RULE 3 – PURPOSE LIMITATION

Rule 3A – RGA will obtain and Process Personal Information only for those purposes outlined in the privacy information provided to Data Subjects in accordance with its transparency obligations.

RGA will specify the purposes for which it intends to Process Personal Information and make this information available to Data Subjects as per Rule 2.

Rule 3B – 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 Applicable Data Protection Laws.

Where RGA intends to further Process Personal Information for a purpose other than that for which the Personal Information was initially collected, RGA shall provide relevant Data Subjects prior to that further Processing with information on that other purpose and with any relevant further information in accordance with Rule 2 above.

Where RGA has not obtained the Data Subject's consent to Process his/her Personal Information for a purpose other than that for which the Personal Information was initially collected, or such further purpose is not based on Applicable Data Protection Laws, RGA will assess whether the Processing for a different purpose is compatible with the purpose for which the Personal Information was initially collected, taking into account:

a) any link between the purposes for which the Personal Information was collected and the purposes of the intended further Processing;
b) the context in which the Personal Information was collected;
c) the nature of the Personal Information, in particular whether such information may constitute 'Sensitive Personal Information';
d) the possible consequences of the intended further Processing for the Data Subjects; and
e) the existence of any appropriate safeguards that are implemented by RGA.

In certain cases, where, for example, the proposed purpose is determined to be incompatible with the purpose for which the Personal Information was initially collected, or where the Processing is of Sensitive Personal Information and no exceptions apply, RGA will obtain the Data Subject's consent as required by Applicable Data Protection Law before Processing that information for a different purpose.

RGA shall implement appropriate technical and organizational measures for ensuring that, by default, only Personal Information which are necessary for a specific purpose are processed.

RGA shall implement appropriate technical and organizational measures, which are designed to implement the protection of Personal Information into the Processing that is carried out by RGA.

RULE 4 – DATA MINIMISATION AND ACCURACY

Rule 4A – RGA will keep Personal Information accurate and up to date.

RGA will take reasonable steps to ensure that all Personal Information that are inaccurate are erased or rectified without delay, having regard for the purposes for which they are Processed. In order to ensure that the Personal Information held by RGA is accurate and up to date, RGA shall actively encourage Data Subjects and Controllers from whom RGA received Personal Information to inform RGA when Personal Information has changed or has otherwise become inaccurate.

Rule 4B – 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.

RGA will identify the minimum amount of Personal Information necessary in order to fulfil the purposes for which it must Process the Personal Information.

RULE 5 – LIMITED RETENTION OF PERSONAL INFORMATION

Rule 5A – RGA will only keep Personal Information for as long as is necessary for the purposes for which it is collected and further Processed.

RGA will comply with RGA's record retention policies and guidelines as revised and updated on a periodic basis.

RULE 6 – SECURITY AND CONFIDENTIALITY

Rule 6A – 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 Data Subjects.

RGA will implement appropriate technical and organizational measures to protect Personal Information against unintentional or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where Processing involves transmission of Personal Information over a network, and against all other unlawful forms of Processing.

To this end, RGA will comply with the requirements in the security policies in place within RGA, as revised and updated as necessary, together with any other security procedures relevant to a business area or function.

RGA will ensure that any Workforce Members who have access to Personal Information are Processing the data only on instructions from RGA.

Rule 6B – RGA will ensure that providers of services to RGA also adopt appropriate and equivalent security measures.

Where a Group Member appoints a Processor (internal or external) to Process Personal Information on its behalf RGA must impose strict contractual obligations, in writing, on the processor that require it:

- to act only on RGA's instructions when Processing that information, including with regard to transfers of Personal Information outside the UK;
- to have in place appropriate technical and organizational security measures to safeguard the Personal Information;

- to ensure that any individuals who have access to the Personal Information are subject to a confidentiality obligation;

- to not engage a sub-processor without prior specific or general written authorisation from RGA and to ensure the agreement that is entered into with such sub-processor imposes the same obligations as those that are imposed on the service provider;

- to return to RGA or securely delete the Personal Information upon the termination of the contract;

- to assist RGA as needed to comply with RGA's obligations as a Controller;

- to make available to RGA all information necessary to demonstrate compliance with these obligations, and allow for and contribute to audits, including inspections, conducted by RGA or another auditor mandated by RGA; and

- to immediately inform RGA if, in its opinion, an instruction by RGA infringes Applicable Data Protection Laws.

This list of contractual requirements is, and will be updated to remain, compliant with UK GDPR Article 28.3 provisions.

Rule 6C – RGA will comply with data security breach notification requirements under Applicable Data Protection Laws.

In the event of a Personal Information breach, as defined under Applicable Data Protection Laws, the relevant RGA entity will notify the Chief Security and Privacy Officer and RGA UK Services without undue delay and in accordance with the requirements of Applicable Data Protection Laws.

Where the Personal Information breach is likely to result in a risk to the rights and freedoms of the Data Subjects whose Personal Information was involved in the breach RGA UK Services will, without undue delay and in accordance with the requirements of Applicable Data Protection Laws, notify the Information Commissioner.

Where the Personal Information breach is likely to result in a high risk to the rights and freedoms of the Data Subjects whose Personal Information was involved in the breach, RGA will also communicate to affected Data Subjects without undue delay and in accordance with the requirements of Applicable Data Protection Laws.

The facts of the data breach shall be documented and made available to the Information Commissioner.

RULE 7 – HONOURING DATA SUBJECTS' DATA PRIVACY RIGHTS

Rule 7A – RGA will adhere to the Data Subject Rights Procedure (Controller) and will respond to any requests from Data Subjects to access their Personal Information in accordance with Applicable Data Protection Laws.

Data Subjects may request access to, and obtain a copy of, the Personal Information RGA holds about them (including information held in both electronic and paper records). This is known as the right of subject access under Applicable Data Protection Laws. RGA will follow the steps set out in the Data Subject Rights Procedure (UK) (Controller) (see Appendix 2) when receiving and dealing with such requests.

Rule 7B – 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).

Data Subjects may ask RGA to rectify Personal Information RGA holds about them where Data Subjects believe such Personal Information is inaccurate. In other circumstances, Data Subjects may request that their Personal Information be erased, for example, where the Personal Information is no longer necessary in relation to the purposes for which it was collected.

In certain circumstances, as set out in Appendix 2, Data Subjects may also restrict or object to the Processing of their Personal Information or withdraw their consent to Process their Personal Information.

The right to data portability allows a Data Subjects to receive Personal Information about them in a structured, commonly used and machine-readable format and to transmit that information to another Controller if certain grounds apply.

In such circumstances, RGA will follow the steps set out in the Data Subject Rights Procedure (Controller) (see Appendix 2).

RULE 8 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

Rule 8 – RGA will not transfer Personal Information to third parties outside the UK without ensuring adequate protection for the Personal Information in accordance with the standards set out by this Controller Policy.

In principle, transfers and onward transfers of Personal Information to third parties outside the RGA Group Members are not allowed unless Personal Information is transferred to a third country that is deemed to have an adequate level of protection by the UK Government Secretary of State or RGA provides appropriate safeguards that are compliant with Applicable Data Protection Law requirements, such as by entering into standard contractual clauses with a third party who is receiving the data, or ensuring that such third party can provide adequate protection through other means (e.g. approved code of conduct, approved certification mechanism).

RULE 9 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 9 – RGA will only Process Sensitive Personal Information where the Data Subject's explicit consent has been obtained, unless RGA has an alternative legitimate basis for doing so consistent with Applicable Data Protection Laws.

RGA will assess whether Sensitive Personal Information is required for the intended purpose of Processing. Sensitive Personal Information includes, but is not limited to, information relating to a Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, or data concerning a natural person's sex life or sexual orientation.

In principle, RGA must obtain the Data Subject's explicit consent to collect and Process their Sensitive Personal Information, unless RGA is otherwise authorized or has another legitimate basis for doing so consistent with Applicable Data Protection Laws (i.e. Substantial Public Interest conditions relating to insurance purposes).

Consent must be given freely, and must be specific, informed and unambiguous.

RULE 10 – LEGITIMISING DIRECT MARKETING

Rule 10 – Where RGA provides Data Subjects with the opportunity to receive marketing information it will ensure that the rights of Data Subjects related to the use of their Personal Information for direct marketing purposes are honoured.

Where RGA performs Consent based marketing (Opt-in) Data Subjects have the right to withdraw their consent, free of charge, and as easily as they provided it. RGA will collect and manage consent in accordance with Applicable Data Protection Laws.

Data Subjects also have an absolute right to object, free of charge, to the use of their Personal Information for direct marketing purposes.

RGA will honour all such requests in accordance with Applicable Data Protection Laws.

RGA will inform Data Subjects about the rights they may exercise with respect to direct marketing in a privacy notice that is provided to them in accordance with Applicable Data Protection Laws.

RULE 11 – AUTOMATED DECISION MAKING, INCLUDING PROFILING

Rule 11 – Data Subjects have the right not to be subject to a decision based solely on automated Processing, including profiling, and to contest such decision.

Under Applicable Data Protection Laws, no decision that produces legal effects concerning a Data Subject, or significantly affects that Data Subject, can be based solely on the automated Processing, including profiling, of that Data Subject's Personal Information, unless such decision is authorized by Applicable Data Protection Law, or is necessary for entering into, or performing, a contract between RGA and that Data Subject, or is based on the Data Subject's explicit consent. In the two latter situations, RGA shall implement suitable measures to protect the legitimate interests of the Data Subject, at least the right to obtain human intervention, to express one's view and to contest the decision.

SECTION B: PRACTICAL COMMITMENTS

RULE 12 – COMPLIANCE

Rule 12A – RGA will have appropriate Workforce Members and support to ensure and oversee privacy compliance throughout the business.

RGA has appointed its Chief Security and Privacy Officer to oversee and ensure compliance with this Controller Policy. The Chief Security and Privacy Officer reports directly to the Reinsurance Group of America Inc Board of Directors. The Chief Security and Privacy Officer, supported by RGA's Data Protection Team, is responsible for overseeing and enabling compliance with this Controller Policy on a day-to-day basis. A summary of the roles and responsibilities of RGA's Data Protection Team is set out in Appendix 3.

Each applicable Group Member is responsible for being able to demonstrate compliance with this Policy.

Rule 12B – RGA will maintain records of the Processing activities it carries out for its own purposes.

RGA shall maintain and update a record of all the Processing activities it carries out for its own purposes. This record will be maintained in writing (including in electronic form) and will be made available to the

Information Commissioner on request. These records will maintain at least the information required by Article 30.1 of the UK GDPR.

Rule 12C – RGA will carry out a data protection impact assessment where the Processing is likely to result in a high risk for the data subjects.

Where a type of Processing is likely to result in a high risk to the rights and freedoms of natural persons (including where RGA uses new technologies), RGA will carry out an assessment of the impact of the envisaged Processing on the protection of Personal Information, prior to the Processing.

Such data protection impact assessment will take into account the nature, scope, context and purposes of the intended Processing.

Where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures taken by RGA to mitigate the risk, the Information Commissioner should be consulted prior to Processing.

RULE 13 – PRIVACY TRAINING

Rule 13 – RGA will provide appropriate 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 (UK) (Controller) attached as Appendix 4.

RULE 14 – AUDIT

Rule 14 – RGA will verify compliance with this Controller Policy and will carry out data protection audits on a regular basis in accordance with the Audit Protocol (UK) (Controller) set out in Appendix 5.

RULE 15 – COMPLAINT HANDLING

Rule 15 – RGA will ensure that Data Subjects may exercise their right to file a complaint and will handle such complaints in accordance with the Complaint Handling Procedure (UK) (Controller) set out in Appendix 6.

RULE 16 – COOPERATION WITH THE INFORMATION COMMISSIONER

Rule 16 – RGA agrees to comply with the advice and to abide by a formal decision of the Information Commissioner on any issues relating to the interpretation and application of the Policies in accordance with the Cooperation Procedure (UK) (Controller) in Appendix 7.

RULE 17 – UPDATES TO THE CONTROLLER POLICY

Rule 17 – RGA will report changes to this Controller Policy to the Information Commissioner in accordance with the Updating Procedure (UK) (Controller) set out in Appendix 8.

RULE 18 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE CONTROLLER POLICY

Rule 18A – 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), RGA will promptly inform:

- **the Chief Security and Privacy Officer and RGA UK Services;**
- **the Information Commissioner;**

unless otherwise prohibited by a law enforcement authority.

Rule 18B – RGA will ensure that where there is a conflict between the legislation applicable to it and this Controller Policy, the Chief Security and Privacy Officer will make a responsible decision on the action to take and will consult the Information Commissioner in case of doubt, unless prohibited from doing so by a law enforcement authority or agency.

RGA will use its best efforts to inform the requesting authority or agency about its obligations under Applicable Data Protection Laws and to obtain the right to waive this prohibition in order to communicate as much information as possible to the Information Commissioner.

Unless prohibited by applicable legislation, RGA will notify the Information Commissioner of any conflicts likely to have a substantial adverse effect on the guarantees provided by this policy by a legal requirement of applicable legislation. This includes any legally binding request for disclosure of the personal data by a law enforcement authority or state security body. Unless prohibited, the Information Commissioner will be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure.

Where such a prohibition cannot be waived, despite RGA's efforts, RGA will provide the Information Commissioner with an annual report providing general information about any requests for disclosure RGA may have received from a requesting authority or agency, to the extent that RGA has been authorized by said authority or agency to disclose such information.

In any case, the transfers of Personal Information by RGA to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

Under Applicable Data Protection Laws Data Subjects (a "**Controller Third Party Beneficiary**") whose Personal Information is Processed by a Group Member in the UK (**a "UK Entity"**) and transferred to a Group Member located outside the UK under the Controller Policy (a "**Non-UK Entity**") have third-party beneficiary rights to enforce the following elements of the BCRs:

- 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 (ICO Co-operation),
    - 18 (National Legislation preventing compliance)
    - The Liability, compensation and jurisdiction provisions (below).

In such cases, a Controller Third Party Beneficiary rights are as follows:

Liability, Compensation and Jurisdiction provisions:

- Controller Third Party Beneficiaries who have suffered material or non-material damage as a result of an infringement of this Policy have the right to receive remedy and compensation.

- Where a Controller Third Party Beneficiary 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 this Policy by a Non-UK BCR Entity or external sub-processors outside the UK, it will be for RGA UK Services to prove that the Non-UK BCR Entity was not responsible for the non-compliance with this Policy giving rise to those damages or that no such non-compliance took place,

- In particular, in case of non-compliance with this Policy by a non-UK BCR Entity, a Controller Third Party Beneficiary may exercise these rights and remedies against RGA UK Services and, where appropriate, receive remedy and compensation from RGA UK Services for any material or non-material damage suffered as a result of an infringement of this Policy.

- A Controller Third Party Beneficiary may bring proceedings against RGA UK Services to enforce compliance with this Policy before a competent UK Court,

- Data Subjects may lodge a complaint with the Information Commissioner,

This Policy (and any updates thereto) will be accessible on RGA's website at http://www.rgare.com

PART III: APPENDICES

APPENDIX 1

LIST OF RGA GROUP MEMBERS (UK) (CONTROLLER)

APPENDIX 2

APPENDIX 2

DATA SUBJECT RIGHTS PROCEDURE (UK) (CONTROLLER)

APPENDIX 3

PRIVACY COMPLIANCE STRUCTURE (UK) (CONTROLLER)

APPENDIX 4

PRIVACY TRAINING PROGRAM (UK) (CONTROLLER)

APPENDIX 5

AUDIT PROTOCOL (UK) (CONTROLLER)

APPENDIX 6

COMPLAINT HANDLING PROCEDURE (UK) (CONTROLLER)

APPENDIX 7

COOPERATION PROCEDURE (UK) (CONTROLLER)

APPENDIX 8

UPDATING PROCEDURE (UK) (CONTROLLER)

APPENDIX 9

In Scope Data Transfers (UK) (CONTROLLER)

CHANGE LOG

Date	Version	Change
Sep 2023	1.0	First (non-Draft) version