DATED

GLOBAL BINDING CORPORATE RULES:

CONTROLLER POLICY

Contents

INTRODUCTION **3**

Definitions **4**

PART I: BACKGROUND AND SCOPE **6**

PART II: CONTROLLER OBLIGATIONS **9**

PART III: APPENDICES **20**

INTRODUCTION

This Binding Corporate Rules: Controller Policy ("**Controller Policy**") establishes RGA's approach to compliance with data protection laws when Processing Personal Information for its own purposes and where such Personal Information originates in Europe, specifically with regard to transfers of Personal Information between members of the RGA group of entities. In this Controller Policy, we use "**RGA**" to refer to RGA group members ("**Group Members**").

This Controller Policy does not apply to Personal Information that RGA is processing as a Processor, which instead is protected in accordance with RGA's Binding Corporate Rules: Processor Policy.

This Controller Policy does not replace any specific data protection requirements that might apply to a business area or function.

A summary of 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 territory from which a Group Member initially transfers Personal Information under this Controller Policy. Where a European Group Member transfers Personal Information under this Controller Policy to a non-European Group Member, the term Applicable Data Protection Laws shall include the European data protection laws applicable to that European Group Member;
"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;
"Europe"	as used in this Controller Policy refers to the Member States of the European Economic Area – i.e. the 28 Member States of the European Union plus Norway, Lichtenstein and Iceland;
"Group Members"	means any of the members of RGA's group of companies listed in Appendix 1;
"Personal Information"	means any information relating to an identified or identifiable natural person. An identifiable natural personal 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 personal;
"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;
"Sensitive Personal Information"	means information that relates to an individual'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 includes information about an individual's criminal offences or convictions, as well as any other information deemed sensitive under Applicable Data Protection Laws; and
"Workforce Members"	refers to all employees, new hires, individual contractors and consultants, and temporary members of the workforce engaged by any RGA 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 individuals 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 national data protection authorities and courts. The Processing of any Personal Information of a natural individual by or on behalf of RGA globally is covered and regulated by Applicable Data Protection Laws.

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, when an organization Processes Personal Information only on behalf of a Controller, that organization is deemed to be a *Processor* of the Personal Information. In this case, the Controller of the Personal Information will be primarily responsible for meeting the legal requirements.

This Controller Policy describes how RGA will comply with Applicable Data Protection Laws with respect to Processing Personal Information as a Controller. RGA's Binding Corporate Rules: Processor Policy describes how RGA will comply with Data Protection Laws with respect to processing Personal Information as a Processor.

HOW DOES DATA PROTECTION LAW AFFECT RGA INTERNATIONALLY?

Applicable Data Protection Laws in Europe prohibit the transfer of Personal Information outside Europe to countries that do not ensure an adequate level of data protection. Only certain non-European countries in which RGA operates and to which Personal Information may be transferred from Europe are regarded by European data protection authorities as providing an adequate level of protection for individuals' privacy and data protection rights.

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 Europe.

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, customer management and vendor management. As such, the Personal Information to which this Controller Policy applies includes:

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

- Customer relationship management data: including Personal Information of representatives of business customers who use RGA's business services and customer support platform;

- Policyholder data: including Personal Information of individuals 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 from 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.

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 collection, use or transfer of Personal Information as a Controller or as a Processor acting on behalf of another Group Member 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 RGA Group Members in their capacity as either a Controller or a Processor.

RGA has a separate Binding Corporate Rules: Processor Policy that applies when it Processes Personal Information as a Processor on behalf of a Controller that is not an RGA Group Member. When a RGA Group Member Processes Personal Information as a Processor on behalf of a third party Controller, it must comply with the Processor 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, Personal Information as a Controller or Processor, such Group Member must contact the Chief 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 RGA's Chief Privacy Officer using the contact information below. All inquiries will be dealt with directly by the Chief Privacy Officer or delegated to the RGA Workforce Member or department best positioned to address such inquiry.

Attention:	Dean C. Bryant, Vice President, Chief Privacy Officer
Email:	dbryant@rgare.com
Address:	16600 Swingley Ridge Road, Chesterfield, Missouri, 63017, USA

RGA's Chief Privacy Officer is responsible for ensuring that any changes to this Controller Policy are communicated to all RGA Group Members and to individuals 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 (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.

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 individuals 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 Data Protection Laws, including any laws governing the protection of Personal Information (e.g. in Europe, the General Data Protection Regulation 2016/679 and any national data protection laws) and will ensure that all Personal Information is Processed in accordance with Applicable Data Protection Laws.

RGA will ensure all Processing of Personal Information has a legal basis (such as the individual's consent, the necessity to execute the terms of a contract, or the obligation to comply with any applicable law) in compliance with any Applicable Data Protection Law including any laws governing the protection of personal information in the country where the data is originally collected.

To the extent that any Applicable Data Protection Law 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.

As such:

- where Applicable Data Protection Laws exceed the standards set out in this Controller Policy, RGA must comply with those laws; but
- where there is no data protection law, or where the 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.

RULE 2 – FAIRNESS AND TRANSPARENCY

Rule 2 – RGA will ensure individuals are provided with a fair notice and sufficient information at the time when their Personal Information is collected, regarding the Processing of their Personal Information.

Where required by Applicable Data Protection Laws, RGA shall implement appropriate measures to inform individuals 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.

- Personal Information that are obtained directly from individuals:

Where required by Applicable Data Protection Laws, RGA shall, at the time when it collects Personal Information from individuals, provide individuals with the following information necessary to ensure fair and transparent Processing in respect of the individual (unless such individuals 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 Europe intends to **transfer** Personal Information to a Group Member outside Europe 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 individuals 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 **individuals' 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 competent supervisory authority;

- 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 individual 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 individuals 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 individuals.

  - Personal Information that are not obtained from individuals:

Where Personal Information has not been obtained directly from the individuals concerned, and where the Applicable Data Protection Law requires, RGA shall provide those individuals, in addition to the information above, with the following information:

- 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.

Where the Personal Information are not obtained from the individuals, RGA shall provide the above information to those individuals:

- 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 individual, at the latest at the time of the first communication to that individual; or if a disclosure to another recipient is envisaged, at the latest when the Personal Information are first disclosed.

RGA will follow Rule 2 unless (a) the individual 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.

A summary of this Controller Policy (and any updates thereof) will be accessible on RGA's website at http://www.rgare.com.

RULE 3 – PURPOSE LIMITATION

Rule 3A – 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.

RGA will specify the purposes for which it intends to Process Personal Information and make them known to the individuals when and from whom such information is obtained, or, if not practicable to do so at the point of collection, as soon as possible after collection, in accordance with Rule 3B below.

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 the Applicable Data Protection Law of the country in which the Personal Information was collected.

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 individuals 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 individual'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 individuals; and

(e) the existence of any appropriate safeguards that are implemented by RGA.

In certain cases, for example, where the Processing is of Sensitive Personal Information, RGA will, to the extent required by law and where no exceptions or exemptions apply, obtain the individual's consent 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 each specific purpose of the processing 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 individuals and data 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 individuals.

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 of RGA 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 service provider to Process Personal Information on its behalf, RGA must impose strict contractual obligations, in writing, on the service provider that require it:

- to act only on RGA's instructions when Processing that information, including with regard to transfers of Personal Information outside Europe;
- 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.

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, RGA will notify the competent regulator 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 high risk to the rights and freedoms of the individuals whose Personal Information was involved in the breach, RGA will also notify those affected individuals without undue delay and in accordance with the requirements of Applicable Data Protection Laws.

RULE 7 – HONOURING INDIVIDUALS' DATA PRIVACY RIGHTS

Rule 7A – 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.

Individuals 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 (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).

Individuals may ask RGA to rectify Personal Information RGA holds about them where individuals believe such Personal Information is inaccurate. In other circumstances, individuals 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, individuals 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 an individual 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 Europe without ensuring adequate protection for the Personal Information in accordance with the standards set out by this Controller Policy.

In principle, cross-border transfers of Personal Information to third parties outside the RGA group of entities are not allowed unless Personal Information is transferred to a third country that is deemed to have an adequate level of protection by the European Commission or RGA provides appropriate safeguards 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 collected in Europe 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 European country in which the Personal Information was collected.

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 an individual'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 individual's explicit consent to collect and Process his/her Sensitive Personal Information, unless RGA is otherwise authorized to do so by Applicable Data Protection Laws or has another legitimate basis for doing so consistent with the Applicable Data Protection Laws of the European country in which the Personal Information was collected.

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

RULE 10 – LEGITIMISING DIRECT MARKETING

Rule 10 – 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.

All individuals have the right to object, free of charge, to the use of their Personal Information for direct marketing purposes and RGA will honour all such opt-out requests in accordance with Applicable Data Protection Laws. RGA will inform individuals 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 INDIVIDUAL DECISIONS

Rule 11 – Individuals have the right not to be subject to a decision based solely on automated Processing and to contest such decision.

Under Applicable Data Protection Laws, no decision that produces legal effects concerning an individual, or significantly affects that individual, can be based solely on the automated Processing of that individual's Personal Information, unless such decision is authorized by law, or is necessary for entering into, or performing, a contract between RGA and that individual, or is based on the individual's explicit consent. In the two latter situations, RGA shall implement suitable measures to protect the legitimate interests of the individual, 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 Privacy Officer to oversee and ensure compliance with this Controller Policy. The Chief Privacy Officer will report to the Board of Directors. The Chief 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.

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 data protection authorities on request.

Rule 12C – RGA carries 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 carries 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 competent supervisory authority 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 (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 (Controller) set out in Appendix 5.

RULE 15 – COMPLAINT HANDLING

Rule 15 – 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) set out in Appendix 6.

RULE 16 – COOPERATION WITH DATA PROTECTION AUTHORITIES

Rule 16 – RGA agrees to comply with the advice and to abide by a formal decision of any competent data protection authority on any issues relating to the interpretation and application of the Policies 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) in Appendix 7.

RULE 17 – UPDATES TO THE CONTROLLER POLICY

Rule 17 – RGA will report changes to this Controller Policy to the data protection authorities in accordance with the Updating Procedure (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 Privacy Officer and RGA International Reinsurance Company dac;**
- **the competent data protection authority;**

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 Privacy Officer will make a responsible decision on the action to take and will consult the data protection authority with competent jurisdiction in case of doubt, unless prohibited from doing so by a law enforcement authority or agency.

RGA uses reasonable 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 competent data protection authorities. Where such prohibition cannot be waived, despite RGA's efforts, RGA provides the competent data protection authorities 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, individuals whose Personal Information is Processed in Europe by a Group Member acting as a Controller (an "**EEA Entity**") and/or transferred to a Group Member located outside Europe 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 under Part I; section A of Part II; and Rules 12B, 15, 16 and 18 under section B of Part II.

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) and may also lodge a complaint with a European data protection authority in the jurisdiction of their habitual residence, or place of work, or place of the alleged infringement;

- *Proceedings*: Individuals have the right to an effective judicial remedy if their rights under this Controller Policy have been infringed as a result of the Processing of their Personal Information in non-compliance with this Controller Policy. Individuals may bring proceedings against RGA International Reinsurance Company dac (Ireland) to enforce compliance with this 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 this Controller Policy have the right to receive compensation from the Controller or Processor for the damage suffered. In particular, in case of non-compliance with this 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 this 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.

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 this 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 this Policy giving rise to those damages or that no such non-compliance took place.

PART III: APPENDICES

APPENDIX 1

LIST OF RGA GROUP MEMBERS (CONTROLLER)

APPENDIX 2

DATA SUBJECT RIGHTS PROCEDURE (CONTROLLER)

APPENDIX 3

PRIVACY COMPLIANCE STRUCTURE (CONTROLLER)

APPENDIX 4

PRIVACY TRAINING PROGRAM (CONTROLLER)

APPENDIX 5

AUDIT PROTOCOL (CONTROLLER)

APPENDIX 6

COMPLAINT HANDLING PROCEDURE (CONTROLLER)

APPENDIX 7

COOPERATION PROCEDURE (CONTROLLER)

APPENDIX 8

UPDATING PROCEDURE (CONTROLLER)

October 2021

BINDING CORPORATE RULES (EU):

APPENDIX 1

LIST OF RGA GROUP MEMBERS (CONTROLLER)

APPENDIX 1: LIST OF RGA GROUP MEMBERS

Note: If no direct legal entity email is listed please contact privacy@rgare.com.

The 'EU BCR Entities' are as follows:

Name of entity	Registered address	Principle place of business	Registration number	Telephone/Email
RGA INTERNATIONAL REINSURANCE COMPANY DESIGNATED ACTIVITY COMPANY ("RGAI")	3rd Floor, Block C, Central Park, Leopardstown, Dublin 18, D18 X5T1 Ireland	3rd Floor, Block C, Central Park, Leopardstown, Dublin 18, D18 X5T1 Ireland	372722	T: 353.1.290.2900 F: 353.1.290.2901
RGA International Reinsurance Company dac, Branch to France	31-33 rue de la Baume, 6th Floor, Paris, 75008, France	31-33 rue de la Baume, 6th Floor, 75008 Paris, France Other: 2 boulevard Marie et Alexandre Oyon, 72100 Le Mans, France	499883148	T: 33.1.55.07.97.81 F: 33.1.55.07.80.96 F: 33.2.43.28.07.23 (Le Mans office)
RGA International Reinsurance Company dac Germany Branch Office	Hohenzollernring 72, 50672 Cologne, Germany	Hohenzollernring 72, 50672 Cologne, Germany	HRB 63901	T: 49.221.96.49.980 F: 49.221.9649.9899
RGA International Reinsurance Company dac, Italian Branch	Via Melchiorre Gioia, 8, 20124, Milan, Italy	Via Melchiorre Gioia, 8, 20124, Milan, Italy	97446620151	T: 39.02.88.21.0501 F: 39.02.76.01.8353 rgaintreinscodac@legalmail.it
RGA International Reinsurance Company dac, Branch in Poland	Atrium Garden, Al. Jana Pawła II, 19, 00-854, Warsaw, Poland	Atrium Garden, Al. Jana Pawła II, 19, 00-854, Warsaw, Poland	341920	T: 48.22.370.1220

				F: 48.22.370.1221
RGA International Reinsurance Company dac, Branch in Spain	Paseo de Recoletos, 16. Planta 5, 28001 Madrid, Spain-	Paseo de Recoletos, 16, Planta 5, 28001 Madrid, Spain	N0071890H	T: 34.91.640.4340 F: 34.91.640.4341
RGA International Reinsurance Company dac, Branch Office for The Netherlands	WTC Amsterdam, Tower H, Zuidplein 168, 1077 XV Amsterdam, Netherlands	WTC Amsterdam, Tower H, Zuidplein 168, 1077 XV Amsterdam, Netherlands	30267682	T: 31.20.333.7431

The 'Non-EU BCR Entities' are as follows:

Name of entity	Registered address	Principle place of business	Registration number	Telephone/Fax/E mail
APEXA CORP.	60 Adelaide Street East, Suite 1300, Toronto, Ontario M5C 3E4, Canada	60 Adelaide Street East, Suite 1300 Toronto, Ontario M5C 3EA Canada	002418443	T: 647.800.8679 System support T: 1.855.294.2541
Hodge Life Assurance Company Ltd	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	00837457	T: 44.20.7710.6700
RGA Capital Ltd	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	03095865	T: 44.20.7710.6700
RGA UK Services Limited ("RGA UK Services")	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	03086510	T: 44.20.7710.6700 E:
RGA International Reinsurance Company Designated Activity Company, U.K. Branch Office	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	UK Branch No. BR010326; UK Company No. FC028797	T: 44.20.7710.6700
RGAX EMEA Limited	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	11113491	T: 44.20.7710.6700

				E: rgaxemea@rgare.com
Omnilife Insurance Company Limited	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	Level 45, 22 Bishopsgate, London, EC2N 4BQ, United Kingdom	02294080	
AURORA NATIONAL LIFE ASSURANCE COMPANY	c/o CT Corporation System, 818 West 7th Street, Los Angeles, California 90017, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States Mailing Address: 16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States Administrative Office: 55 Heartland Street, East Hartford, Connecticut 06108, United States	C0413144	T: 1.800.265.2652
Castlewood Reinsurance Company	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	01233405	T: 636.736.7000
Chesterfield Reinsurance Company	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	I001401432	T: 636.736.7000
COOKHOUSE LAB INC.	60 Adelaide Street East, Suite 1300, Toronto, Ontario M5C 3E4, Canada	60 Adelaide Street East, Suite 1300, Toronto, Ontario M5C 3E4, Canada	002546962	T: 416.340.7435 F: 416.340.9977
ELITE SALES PROCESSING, INC.	c/o CT Corporation System, 5601 South 59th Street, Lincoln, Nebraska 68516	11205 Wright Circle, Suite 120, Omaha, Nebraska 68144, United States Other: 1205 7th Street, Harlem, Iowa 51537, United States	10080132	T: 402.933.1758 F: 402.965.4043 E: cgracey@espsvcs.com

GREENHOUSE LIFE INSURANCE COMPANY	c/o CT Corporation System, 3800 N. Central Avenue, Suite 460, Phoenix, Arizona 85012, United States	8601 N. Scottsdale Rd. #300, Scottsdale, Arizona 85253, United States Mailing address: 16600 Swingley Ridge Road, Chesterfield, MO 63017-1706, United States	00861679	T: 866.493.8991 E: info@getgreenhouse.com
LOGiQ^3 CORP.	60 Adelaide Street East, Suite 1300 Toronto, Ontario M5C 3EA Canada	60 Adelaide Street East, Suite 1300 Toronto, Ontario M5C 3E4 Canada	001812296	T: 416.340.7435 F: 416.340.9977
LOGIQ3 Inc.	77 King Street West, Suite 2200, Toronto, Ontario M5K 1H6 Canada	60 Adelaide Street East, Suite 1300 Toronto, Ontario M5C 3EA Canada	1059969-7	T: 416.340.7435 F: 416.340.9977 E: info@logiq3.com
MANOR REINSURANCE, LTD.	c/o Chancery Chambers, Chancery House, High Street, Bridgetown, Barbados, BB11128	c/o Strategic Risk Solutions, Barbados, Letchworth House, The Garrison, St. Michael, Barbados, BB14038	33694	
My Life Covered LLC	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	LC001455819	T: 636.728.9447 E: info@mylifecoveredagency.com
Parkway Reinsurance Company	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	00842271	T: 636.736.7000
Reinsurance Company of Missouri, Incorporated	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	I00462032	T: 636.736.7000
RGA Americas Reinsurance Company, Ltd.	c/o Estera Services (Bermuda) Limited, Victoria Hall 5th Floor, 31 Victoria Street, PO Box HM 1624, Hamilton, HM 10, Bermuda	c/o Marsh Management Services (Bermuda) Ltd., Power House, 7 Par-la-Ville Road, Hamilton, HM 11, Bermuda	49524	T: 441.292.4402 F: 441.292.1563
RGA ATLANTIC REINSURANCE COMPANY LTD.	c/o Chancery Chambers, Chancery House, High Street, Bridgetown, Barbados BB11128	c/o Strategic Risk Solutions, Barbados, Letchworth House, The Garrison, St. Michael, Barbados BB14038	29679	T: 246.537.9768 F: 246.538.0246

RGA AUSTRALIAN HOLDINGS PTY LIMITED	Grosvenor Place, Level 23, 225 George Street, Sydney, NSW 2000, Australia	Grosvenor Place, Level 23, 225 George Street, Sydney, NSW 2000, Australia	071 125 507	T: 61.2.8264.5800 F: 61.2.8264.5999
RGA Enterprise Services Company	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	001364165	T: 636.736.7000
RGA Global Reinsurance Company, Ltd.	c/o Conyers Dill & Pearman Limited, Clarendon House, 2 Church Street, Hamilton, HM CX, Bermuda	c/o Marsh Management Services (Bermuda) Ltd., Power House, 7 Par-la-Ville Road, Hamilton, HM 11, Bermuda	37662	T: 441.292.4402 F: 441.292.1563
RGA Global Reinsurance Company, Ltd. - escritório de representação no Brasil Ltda.	Av. das Nações Unidas, 14.171-15˚ andar, Marble Tower, São Paulo - SP 04794-000, Brazil	Edificio Igarassu, Rua Surubim, 577-21˚ conj. 212, Cidade Monções, São Paulo - SP 04571-050, Brazil	18.120.916/0001-40	T: 55.11.4862.5000 T: 55.11.3568.2125 F: 55.11.3568.2200
RGA Global Reinsurance Company, Ltd. Labuan Branch (Retakaful Window)	Unit 30-3 & 30-A, Level 30, Menara Etiqa, No. 3, Jalan Bangsar Utama 1, 59000, Bangsar, Kuala Lumpur, Malaysia	Unit 30-3 & 30-A, Level 30, Menara Etiqa, No. 3, Jalan Bangsar Utama 1, 59000, Bangsar, Kuala Lumpur, Malaysia		T: 60.87.451688 F: 60.87.453688
RGA Global Reinsurance Company, Ltd., Labuan Branch	c/o ZICOlaw Trust Limited, Unit Level 13(A), Main Office Tower, Financial Park Labuan, Jalan Merdeka, 87000, Labuan, Malaysia	c/o ZICOlaw Trust Limited, Unit Level 13(A), Main Office Tower, Financial Park Labuan, Jalan Merdeka, 87000, Labuan, Malaysia Co-location: Unit No. A-33, Level 33, Tower A, Manara UOA Bangsar, Kuala Lumpur, Malaysia	IS200893	T: 60.87.451688 Co-location: T: 603.2712.0007
RGA Global Reinsurance Company Limited Taiwan Branch	Room 2008, 20F, No. 333, Sec. 1, Keelung Road, Xinyi District, Taipei, Taiwan, R.O.C. 110, Taiwan	Room 2008, 20F, No. 333, Sec. 1, Keelung Road, Xinyi District, Taipei, Taiwan, R.O.C. 110, Taiwan	27948865	T: 886.2.8789.2217 F: 886.2.8789.6018

RGA GLOBAL SHARED SERVICES INDIA PRIVATE LIMITED	302 Akruti Centre Point, MIDC Central Road, Andheri (East), Mumbai, Maharashtra, India 400 093	302 Akruti Centre Point, MIDC Central Road, Andheri (East), Mumbai, Maharashtra, India 400 093	U67200MH2005PTC153973	T: 91.2267.092550 E: tsaraf@rgare.com
RGA INTERNATIONAL CORPORATION	Suite 900, Purdy's Wharf Tower One, 1959 Upper Water Street, P.O. Box 997, Halifax, Nova Scotia B3J 3N2, Canada	77 King Street, Suite 2200, Toronto, Ontario M5K 1H6, Canada	3051635	T: 416.943.6770 F: 416.943.0880
RGA International Division Sydney Office Pty Limited	Grosvenor Place, Level 23, 225 George Street, Sydney, NSW 2000, Australia	Grosvenor Place, Level 23, 225 George Street, Sydney, NSW 2000, Australia	100 532 938	T: 61.2.8264.5800 F: 61.2.8264.5999
RGA International Reinsurance Company dac, Singapore Branch	5 Temasek Boulevard #05-03/04 Suntec Tower Five, Singapore 038985	5 Temasek Boulevard #05-03/04 Suntec Tower Five, Singapore 038985	T15FC0099D	T: 65.6692.9380 F: 65.6692.9370
RGA Life Reinsurance Company of Canada	77 King Street West, Suite 2300, Toronto, Ontario M5K 1H6, Canada	1981 McGill College Ave, Montreal, Quebec H3A 3A8, Canada Other: 77 King Street West, Suite 2300, Toronto, Ontario M5K 1H6, Canada	Unknown	T: 416.682.0000 F: 416.777.9526
RGA Life Reinsurance Company of Canada India Branch	302, Akruti Centre Point, MIDC Central Road, Andheri (East), Mumbai, Maharashtra 400 093, India	302, Akruti Centre Point, MIDC Central Road, Andheri (East), Mumbai, Maharashtra 400 093, India	F06152	T: 91.22.6709.2590 F: 91.22.6709.2551
RGA Partners Japan GK	Midtown Tower 41F,9-7-1 Akasaka Minato-ku, Tokyo 107-6241, Japan	Midtown Tower 41F,9-7-1 Akasaka Minato-ku, Tokyo 107-6241, Japan	0104-03-020435	T: 813.3479.7191 F: 813.3479.7196
RGA Real Estate Investments LLC	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	LC1239283	T: 636.736.7000

RGA ReCap Incorporated	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017, United States Branch Addresses: 20 Pacifica, Suite 625, Irvine, California 92618-7488, United States 2303 Camino Ramon, Suite 150, San Ramon, California 94583, United States	001371514	T: 636.736.5901 E: joconnor@rgare.com (general questions)
RGA Reinsurance Company	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	I00233357	T: 636.736.7000
RGA REINSURANCE COMPANY (BARBADOS) LTD.	c/o Chancery Chambers, Chancery House, High Street, Bridgetown, Barbados, BB11128	c/o Strategic Risk Solutions, Barbados, Letchworth House, The Garrison, St. Michael, Barbados BB14038	10895	T: 246.537.9768 F: 246.538.0246
RGA Reinsurance Company Beijing Representative Office	Unit 1504, 15F, Office Tower W1, Oriental Plaza, No. 1 East Chang An Avenue, Dong Cheng District, Beijing, 100738, China	Unit 1504, 15F, Office Tower W1, Oriental Plaza, 1 East Chang An Ave. Dong Cheng District, Beijing, China 100738, China	N/A	T: 86.10.8518.2528 F: 86.10.8518.2532
RGA Reinsurance Company Hong Kong Branch	29th Floor, Dorset House, TaiKoo Place, 979 King's Road, Hong Kong	29th Floor, Dorset House, TaiKoo Place, 979 King's Road, Hong Kong	F0006982	T: 852.2511.8688 F: 852.2511.8827
RGA Reinsurance Company Japan Branch	Midtown Tower 41F, 9-7-1 Akasaka Minato-ku, Tokyo, Japan 107-6241, Japan	Midtown Tower 41F, 9-7-1 Akasaka Minato-ku, Tokyo, Japan 107-6241, Japan	Branch Insurance License No.: 3508	T: 813.3479.7191 F: 813.3479.7196
RGA Reinsurance Company Korea Branch	Seoul Finance Center 12F, 136, Sejong-daero, Jung-gu, Seoul,04520, Korea	Seoul Finance Center 12F, 136, Sejong-daero, Jung-gu, Seoul, 04520, Korea	Unknown	T: 82.2.6730.1350 F: 82.2.6730.1370

RGA Reinsurance Company Middle East Limited	1801, 18th Floor, Al Fattan Currency House, Tower – II, Dubai International Financial Centre, Dubai, 506539, United Arab Emirates	1801, 18th Floor, Al Fattan Currency House, Tower – II, Dubai International Financial Centre, Dubai, United Arab Emirates	1082	T: 971.4.3896000 F: 971.4.3896001
RGA Reinsurance Company New Zealand Branch	Level 13, Resimac House, 45 Johnston Street, Wellington 6011, New Zealand	Level 13, Resimac House, 45 Johnston Street, Wellington 6011, New Zealand	836164 NZBN: 9429038190827	T: 64.4.4738868
RGA REINSURANCE COMPANY OF AUSTRALIA LIMITED	Grosvenor Place, Level 23, 225 George Street, Sydney, NSW 2000, Australia	Grosvenor Place, Level 23, 225 George Street, Sydney, NSW 2000, Australia Other: Suite 3, Level 6, 276 Flinders Street, Melbourne VIC 3000, Australia	ASIC: 072 292 712 ABN: 14 072 292 712	T: 61.2.8264.5800 F: 61.8264.5999
RGA Reinsurance Company of Australia Limited New Zealand Branch	Level 13, Resimac House, 45 Johnston Street, Wellington 6011, New Zealand	Level 13, Resimac House, 45 Johnston Street, Wellington 6011, New Zealand	3658254 NZBN: 9429030881105	T: 64.4.4738868
RGA REINSURANCE COMPANY OF SOUTH AFRICA LIMITED	7th Floor, The Terraces, Black River Park, 2 Fir Street, Observatory, 7925, Cape Town, South Africa	7th Floor, The Terraces Black River Park, 2 Fir Street, Observatory, 7925, Cape Town, South Africa Other: 1st Floor, Sentinel House Sunnyside Office Park 32 Princess of Wales Terrace Parktown, 2193 Johannesburg, South Africa	Reg. No. 1997/020948/06	T: 27.21.486.1700 F: 27.21.486.1800
RGA Reinsurance Company Oficina de Representación en México	Torre Reforma 342, Av. Paseo de la Reforma 342, Piso 23-B, Col. Juárez, Mexico City, Mexico, D.F. 06600, Mexico	Torre Reforma 342, Av. Paseo de la Reforma 342, Piso 23-B, Col. Juárez 06600, Mexico City, Mexico	RGRE-376-94-316539	T: 52.55.2881.7200 F: 52.55.2881.7216

RGA Reinsurance Company Shanghai Branch	Unit ABEF, 10F, Mirae Asset Tower, No. 166 Lu Jia Zui Ring Road, Shanghai 200120, China	Unit ABEF, 10F, Mirae Asset Tower, No. 166 Lu Jia Zui Ring Road, Shanghai 200120, China	Unknown	T: 86.21.2067.0666 F: 86.21.2067.0601
RGA SERVICES (SINGAPORE) PTE. LTD.	5 Temasek Boulevard #05 03/04 Suntec Tower Five, Singapore 038985	5 Temasek Boulevard #05 03/04 Suntec Tower Five, Singapore 038985	200920073H	T: 65.6692.9380 F: 65.6692.9370
RGA Technology Partners, Inc.	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	00519471	T: 636.736.7000
RGA WORLDWIDE REINSURANCE COMPANY, LTD.	c/o Chancery Chambers, Chancery House, High Street, Bridgetown, Barbados, BB11128	c/o Strategic Risk Solutions, Barbados, Letchworth House, The Garrison, St. Michael, Barbados BB14038	16050	T: 246.537.9768 F: 246.538.0246
RGAx LLC	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	LC001454614	T: 636.736.7000
River's Edge Turnkey Services, Inc.	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	00177562	T: 636.736.7000
Rockwood Reinsurance Company	c/o CT Corporation System, 120 South Central Avenue, Clayton, Missouri 63105, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	01040835	T: 636.736.7000
SALT Associates, LLC	c/o CT Corporation System, 128 State Street #3, Augusta, Maine 04330, United States	16600 Swingley Ridge Rd. Chesterfield, MO 63107-1706 Mailing Address: Third Floor of 106 Lafayette Street, Yarmouth, Maine 04096, United States	20021269DC	T: 207.846.9779 F: 207.846.9778

Swyvyl Corp.	60 Adelaide Street East, Suite 1300, Toronto, Ontario M5C 3E4 Canada	60 Adelaide Street East, Suite 1300, Toronto, Ontario M5C 3E4 Canada	2489232	T: 416.340.7435 F: 416.340.9977
Timberlake Reinsurance Company II	c/o Marsh Management Services, Inc., 151 Meeting Street, Suite 301, Charleston, South Carolina 29401, United States	16600 Swingley Ridge Road, Chesterfield, Missouri 63017-1706, United States	NONE	T: 636.736.7000
TINDALL ASSOCIATES, INC.	c/o CT Corporation System, 208 South LaSalle Street, Suite 814, Chicago, Illinois, 60604, United States	18927 Hickory Creek Drive, Unit #100, Mokena, Illinois 60448, United States	5400-392-7	T: 708.403.7775

Change Log

Date	Change
Dec 2020	UK addresses changed (to temporary Chiswell Street address)
June 2021	Removal of Leidsche on its leaving the RGA Group
October 2021	Added ‘EU’ to distinguish from UK BCRs UK Addresses changed (to final location in 22 Bishopsgate) Addition of Hodge Life Assurance Company to RGA Group Change of details for RGA Chief Security & Privacy Officer Split table into EU and non-EU entities Added additional ‘default’ contact point

October 2021

BINDING CORPORATE RULES (EU):

APPENDIX 2

DATA SUBJECT RIGHTS PROCEDURE (CONTROLLER)

1 INTRODUCTION

1.1 RGA's "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard Personal Information transferred between RGA's group members ("**Group Members**").

1.2 Individuals whose Personal Information are processed by RGA under the Policies have certain data protection rights, which they may exercise by making a request to the Controller of their information (a "**Request**").

1.3 This Binding Corporate Rules (EU): Data Subject Rights Procedure (Controller) ("**Procedure**") describes how RGA will respond to any Requests it receives from individuals whose Personal Information are Processed and transferred under the Controller Policy.

2 DATA SUBJECTS' DATA PROTECTION RIGHTS

2.1 RGA must assist individuals to exercise the following data protection rights, consistent with the requirements of Applicable Data Protection Laws:

2.1.1 **Right to information**: This is the right for individuals to obtain confirmation as to whether or not Personal Information concerning them are being Processed;

2.1.2 **Right of access:** This is the right for individuals to obtain confirmation whether a Controller Processes Personal Information about them and, if so, to be provided with details of that Personal Information and access to it in an intelligible form;

2.1.3 **Right to rectification:** This is the right for individuals to obtain rectification without undue delay of inaccurate Personal Information a Controller may process about them;

2.1.4 **Right to erasure:** This is the right for individuals to require a Controller to erase Personal Information about him/her on certain grounds – for example, where the Personal Information is no longer necessary to fulfil the purposes for which it was collected;

2.1.5 **Right to restriction:** This is the right for individuals to require a Controller to restrict Processing of Personal Information about them on certain grounds;

2.1.6 **Right to object:** This is the right for individual to object, on grounds relating to their particular situation, to a Controller's Processing of Personal Information about them, if certain grounds apply;

2.1.7 **Right to data portability:** This is the right for individuals to receive Personal Information about them from a Controller in a structured, commonly used and machine-readable format and to transmit that information to another Controller, if certain grounds apply.

3 RESPONSIBILITY TO RESPOND TO A REQUEST

3.1 The Controller of an individual's Personal Information is primarily responsible for responding to a Request and for helping the individual concerned to exercise his or her rights under Applicable Data Protection Laws.

3.2 As such, when an individual contacts RGA to make any Request then where RGA is the Controller of that individual's Personal Information under the Controller Policy, it must help the individual to exercise his or her data protection rights directly in accordance with this Procedure.

4 INITIAL ASSESSMENT OF A REQUEST

4.1 Upon receiving any Request from an individual, RGA will ensure all such Requests are immediately routed to the Data Protection Team at dsr@rgare.com. The Data Protection Team (consisting of the regional compliance functions) will document the date on which such Request was received together with any other information that may assist the Data Protection Team to deal with the Request.

4.2 The Data Protection Team will make an initial assessment of the Request as follows:

4.2.1 the Data Protection Team will determine whether RGA is a Controller or Processor of the Personal Information that is the subject of the Request; and

4.2.2 where Data Protection Team determines that RGA is a Controller of the Personal Information, it will then determine whether the Request has been made validly under Applicable Data Protection Laws and whether confirmation of identity, or any further information, is required in order to fulfil the Request.

5 RESPONSE TO A REQUEST

5.1 If the Data Protection Team determines that RGA is the Controller of the Personal Information that is the subject of the Request, it will then contact the individual in writing to confirm receipt of the Request and seek confirmation of identity (if the individual's identity has not already been validated) as well as any further information it may need to action the individual's Request. RGA may Request such information, which it may reasonably require in order to confirm the identity of the individual making the Request and to locate the information which that person seeks.

5.2 If RGA is exempted under Applicable Data Protection Laws from fulfilling the Request (for example, because RGA can demonstrate that Request is manifestly unfounded or excessive), then RGA will notify the individual if it intends to decline the Request and the exemption that applies. Otherwise, the Data Protection Team will deal with the Request as explained under this Procedure.

5.3 A Request must generally be made in writing, which can include email, unless Applicable Data Protection Laws allow a Request to be made orally.

5.4 A Request does not have to be official or mention data protection law to qualify as a valid Request.

5.5 RGA must respond to a Request without undue delay and in any case no later than one month of receipt of that Request. That period may be extended by two further months where necessary, taking in account the complexity or number of Requests. RGA will inform the individual who has made a Request of any extension within one month of receipt of the Request.

5.6 RGA shall not refuse to act on a Request unless RGA can demonstrate that it is not in the position to identify the individual who is making the Request or where RGA can demonstrate that the individual has made a manifestly unfounded or excessive Request (e.g. due to its repetitive character).

6 REQUESTS FOR ACCESS TO PERSONAL INFORMATION

6.1 Overview

6.1.1 An individual has the right to obtain from RGA confirmation as to whether or not Personal Information concerning him or her are being Processed and, where that is the case, access to the Personal Information and the following information:

a) the purposes of the Processing;

b) the categories of Personal Information concerned;

c) the recipients or categories of recipient to whom the Personal Information have been or will be disclosed, in particular, recipients outside Europe;

d) where possible, the envisaged period for which the Personal Information will be stored, or, if not possible, the criteria used to determine that period;

e) the existence of the right to Request from RGA rectification or erasure of Personal Information, or restriction of Processing of Personal Information concerning him or her, or to object to such Processing;

f) the right to lodge a complaint with a supervisory authority;

g) where the Personal Information are not collected from the individual making the Request, any available information as to their source;

h) the existence of automated decision-making, including profiling; and

i) where Personal Information is transferred from Europe to a country outside of Europe, the appropriate safeguards that RGA has put in place relating to such transfers in accordance with Applicable Data Protection Laws.

6.1.2 An individual is also entitled to request a copy of his or her Personal Information from the Controller in intelligible form ("**Access Request**").

6.1.3 The Data Protection Team will engage appropriate RGA Workforce Members for support with handling an Access Request, as required or appropriate.

6.2 Exemptions to an Access Request

6.2.1 An Access Request may be refused on the following grounds:

a) if the refusal to provide the information is consistent with Applicable Data Protection Laws within the jurisdiction in which that Group Member is located;

b) where the Personal Information is held by RGA in non-automated form that is not or will not become part of a filing system; or

c) where the Personal Information does not originate from Europe, has not been Processed by any European Group Member, and the provision of the Personal Information requires RGA to use disproportionate effort.

6.2.2 The Data Protection Team will assess each Access Request individually to determine whether any of the above-mentioned exemptions applies.

6.3 Response to an Access Request

6.3.1 The Data Protection Team will conduct a search of all relevant and in-scope electronic and paper filing systems.

6.3.2 The Data Protection Team may refer any complex cases to RGA's Chief Privacy Officer for advice, particularly where the Request includes information relating to third parties or where the release of Personal Information may cause harm to the individual or prejudice commercial confidentiality or legal proceedings.

6.3.3 The information requested will be collated by the Data Protection Team into a readily understandable format (internal codes or identification numbers used at RGA that correspond to Personal Information shall be translated before being disclosed). The Data Protection Team will prepare a covering letter, which shall include all information required to be provided in response to an Access Request.

6.3.4 Where the provision of the information in permanent form is not possible or would involve disproportionate effort, there is no obligation to provide a permanent copy of the information. The other information referred to in section 6.1.1 above must still be provided. In such circumstances, the individual may be offered the opportunity to have access to the information by inspection or to receive the information in another form, such as any commonly used electronic form.

6.3.5 RGA may charge a reasonable fee based on administrative costs of providing further copies of the data.

7 REQUESTS FOR ERASURE OR RECTIFICATION OF PERSONAL INFORMATION, OR RESTRICTION OR CESSATION OF PROCESSING OF PERSONAL INFORMATION, OR DATA PORTABILITY

7.1 If RGA receives a Request to correct, update, transmit (data portability) or erase Personal Information, or to restrict or cease Processing of an individual's Personal Information where RGA is the Controller for that Personal Information, such Request must be passed to the Data Protection Team at dsr@rgare.com immediately to make an initial assessment in accordance with section 4 above.

7.2 If a Request is received advising of a change in an individual's Personal Information where RGA is the Controller for that Personal Information, such information must be rectified, updated, or erased accordingly.

7.3 When RGA rectifies or erases Personal Information, in its capacity as Controller, RGA will notify other Group Members, sub-processors, or other recipients to whom the Personal Information has been disclosed accordingly so that they can also update their records, unless this proves impossible or involves disproportionate effort. When acting as Controller, RGA shall inform the data subject about those recipients if he or she requests it.

7.4 If a Request is made to RGA as a Controller to cease Processing that individual's Personal Information (where RGA has a legitimate interest to Process such Personal Information) because the rights and freedoms of the individual are prejudiced by virtue of such Processing by RGA, the matter will be referred to RGA's Chief Privacy Officer to assess in accordance with Applicable Data Protection Laws. Where RGA can demonstrate compelling legitimate grounds for the Processing, which override the interests, rights and freedoms of the individual or for the establishment, exercise or defence of a legal claim, the Request will not be regarded as valid.

7.5 If a Request is made to RGA as a Controller to restrict Processing of that individual's Personal Information, the matter will be referred to RGA's Chief Privacy Officer to assess in accordance with Applicable Data Protection Laws.

8 REQUEST FOR DATA PORTABILITY

8.1 If a Request is made to RGA as a Controller to receive the Personal Information that an individual has provided to RGA, in a structured, commonly used and machine-readable format and to transmit directly such information to another Controller (where technically feasible), RGA's Data Protection Team will consider and deal with such Request appropriately in accordance with Applicable Data Protection Laws insofar as the Processing is based on that individual's consent or on the performance of, or steps taken at the request of the individual prior to entry into, a contract.

9 QUESTIONS ABOUT THIS PROCEDURE

9.1 All queries relating to this Procedure are to be addressed to RGA's Chief Privacy Officer at dsr@rgare.com.

Change Log

Date	Change
October 2021	Added ‘EU’ to distinguish from UK BCRs

DATED

BINDING CORPORATE RULES:

APPENDIX 3

PRIVACY COMPLIANCE STRUCTURE (CONTROLLER)

1 INTRODUCTION

1.1 Reinsurance Group of America Inc.'s ("**RGA**") compliance with global data protection laws and the "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") is overseen and managed throughout all levels of the business by a global, multi-layered, cross-functional privacy compliance structure. Further information about RGA's Privacy Compliance Structure (Controller) is set out below and in the structure chart provided at Figure 1.

2 CHIEF PRIVACY OFFICER

2.1 RGA has appointed a Chief Privacy Officer who provides executive-level oversight of, and has responsibility for, ensuring RGA's compliance with Applicable Data Protection Laws and the Policies. The Chief Privacy Officer reports directly to RGA's Board of Directors (including the Board of Directors in Ireland) on all material or strategic issues relating to RGA's compliance with Applicable Data Protection Laws and the Policies and is accountable to RGA's independent Audit Committee. The Chief Privacy Officer leads, and is supported by, RGA's Data Protection Team. The Chief Privacy Officer fulfils the role and tasks of a Data Protection Officer (DPO) and liaises with RGA's additional DPOs (Section 3).

2.2 The Chief Privacy Officer's key responsibilities include:

2.2.1 Ensuring that the Policies and other privacy related policies, objectives and standards are defined and communicated;

2.2.2 Providing clear and visible senior management support and resources for the Policies and for privacy objectives and initiatives in general;

2.2.3 Evaluating, approving and prioritizing remedial actions consistent with the requirements of the Policies, strategic plans, business objectives and regulatory requirements;

2.2.4 Periodically assessing privacy initiatives, accomplishments, and resources to ensure continued effectiveness and improvement;

2.2.5 Ensuring that RGA's business objectives align with the Policies and related privacy and information protection strategies, policies and practices;

2.2.6 Facilitating communications on the Policies and privacy topics with RGA's Board of Directors and independent Audit Committee; and

2.2.7 Dealing with any escalated privacy complaints in accordance with the Global Binding Corporate Rules: Complaint Handling Procedure (Controller or Processor, as applicable).

3 DATA PROTECTION OFFICERS

3.1 In addition to the Chief Privacy Officer (Section 2), RGA has appointed a European Data Protection Officer plus several Data Protection contacts within our various offices to further ensure compliance with Applicable Data Protection Laws and the Policies. Each of these contacts maintain a certain level of independence and report directly to the Chief Privacy Officer, and our European Data Protection Officer reports both to the Chief Privacy Officer and to the Board of Directors in Ireland.

3.2 The DPO is involved in issues that relate to the protection of Personal Information. In particular, the tasks of the DPO are:

3.2.1 To inform and advise RGA and the Workforce Members who Process and/or handle Personal Information of their obligations under Applicable Data Protection Laws;

3.2.2 To monitor compliance with Applicable Data Protection Laws, and with the policies of RGA (including the Policies) that relate to the protection of Personal Information, including the assignment of responsibilities, awareness raising, and training of Workforce Members involved in Processing operations, and the related audits;

3.2.3 To provide advice, where requested, as regards data protection impact assessments and to monitor the performance of the data protection impact assessment process;

3.2.4 To cooperate with the national data protection authorities (DPA); and

3.2.5 To be the point of contact for the DPA on issues relating to Processing, including in the context of a prior consultation, and to consult, where appropriate, with regard to any other matter; and the DPO shall, in the performance of his or her tasks, have due regard to the risks associated with Processing operations, taking into account the nature, scope, context, and purposes of Processing.

4 DATA PROTECTION TEAM

4.1 RGA's Data Protection Team is comprised of RGA's Chief Privacy Officer, the Global Data Protection Office (functionally situated in RGA's Global Risk and Compliance organization) and RGA's Data Protection and Privacy Counsel (functionally situated within RGA's Global Legal Services organization). Incorporating members from both RGA's Risk and Compliance and Legal Services teams ensures appropriate independence and oversight of duties relating to all aspects of RGA's data protection compliance. The Data Protection Team is accountable for managing and implementing RGA's data privacy program internally (including the Policies), advising the organization on Applicable Data Protection Laws and privacy risks, providing recommendations and advice for complying with Applicable Data Protection Laws and for ensuring that effective data privacy controls are in place for any third party service provider RGA engages. In this way, the Data Protection Team is actively engaged in addressing matters relating to RGA's privacy compliance on a routine, day-to-day basis. The responsibilities of the Data Protection Team include:

4.1.1 Providing guidance about the collection and use of Personal Information subject to the Policies and to assess the Processing of Personal Information by RGA Group Members for potential privacy-related risks;

4.1.2 Responding to inquiries and compliance actions relating to the Policies from Workforce Members, Customers, and other third parties raised directly with the Data Protection Team or through its dedicated e-mail address at privacy@rgare.com;

4.1.3 Working closely with the Privacy Committee (defined at point 5 below) in sustaining compliance with the Policies and related policies and practices at a functional and local country level and in evaluating privacy risks involved in certain Processing activities providing guidance related to data protection and privacy and responding to questions and/or issues related to data protection and privacy;

4.1.4 Supporting regular audits of the Policies, coordinating responses to audit findings and supporting remediation of any issues raised by audit findings;

4.1.5 Responding to inquiries of the data protection authorities where appropriate;

4.1.6 Monitoring changes to global privacy laws and ensuring that appropriate changes are made to the Policies and RGA's related policies and business practices;

4.1.7 Overseeing training for Workforce Members on the Policies and data protection legal requirements in accordance with the requirements of the Privacy Training Program (Controller or Processor, as applicable);

4.1.8 Promoting the Policies and privacy awareness across business units and functional areas through privacy communications and initiatives;

4.1.9 Evaluating privacy processes and procedures to ensure sustainability and effectiveness;

4.1.10 Periodic reporting on the status of the Policies to the Chief Privacy Officer and Board of Directors and / or Audit Committee, as appropriate;

4.1.11 Ensuring that the commitments made by RGA in relation to updating, and communicating updates to the Policies as set out in the Binding Corporate Rules: Updating Procedure (Controller or Processor, as applicable), are met; and

4.1.12 Overseeing compliance with the Data Subject Rights Procedure (Controller or Processor, as applicable) and the handling of requests made thereunder.

4.2 In addition to its responsibilities as a member of the Data Protection Team outlined above, RGA's Global Data Protection Office also has a number of specific responsibilities in relation to the implementation and oversight of the Policies and privacy matters more generally, including:

4.2.1 Monitoring attendance of privacy training courses as set out in the Privacy Training Program (Controller or Processor, as applicable);

4.2.2 Performing audits and/or overseeing independent audits of compliance with the Policies as set out in the Audit Protocol and will ensure that such audits address all aspects of the Policies; and

4.2.3 Ensuring that any issues or instances of non-compliance with the Policies are brought to the attention of RGA's Data Protection Team and the Chief Privacy Officer and that any corrective actions are determined and implemented within a reasonable time.

5 PRIVACY COMMITTEE

5.1 RGA's Privacy Committee comprises of functional leads or key representatives from the main functional areas within RGA, such as Compliance, Legal, Information Technology, Information Security and Human Resources. The key responsibilities of Members of the Privacy Committee include:

5.1.1 Promoting the Policies at all levels in their functional areas;

5.1.2 Assisting the Data Protection Team with the day-to-day implementation and enforcement of RGA's privacy policies (including the Policies) within their respective areas of responsibility;

5.1.3 Escalating questions and compliance issues or communicating any actual or potential violation of relating to the Policies to the Data Protection Team; and

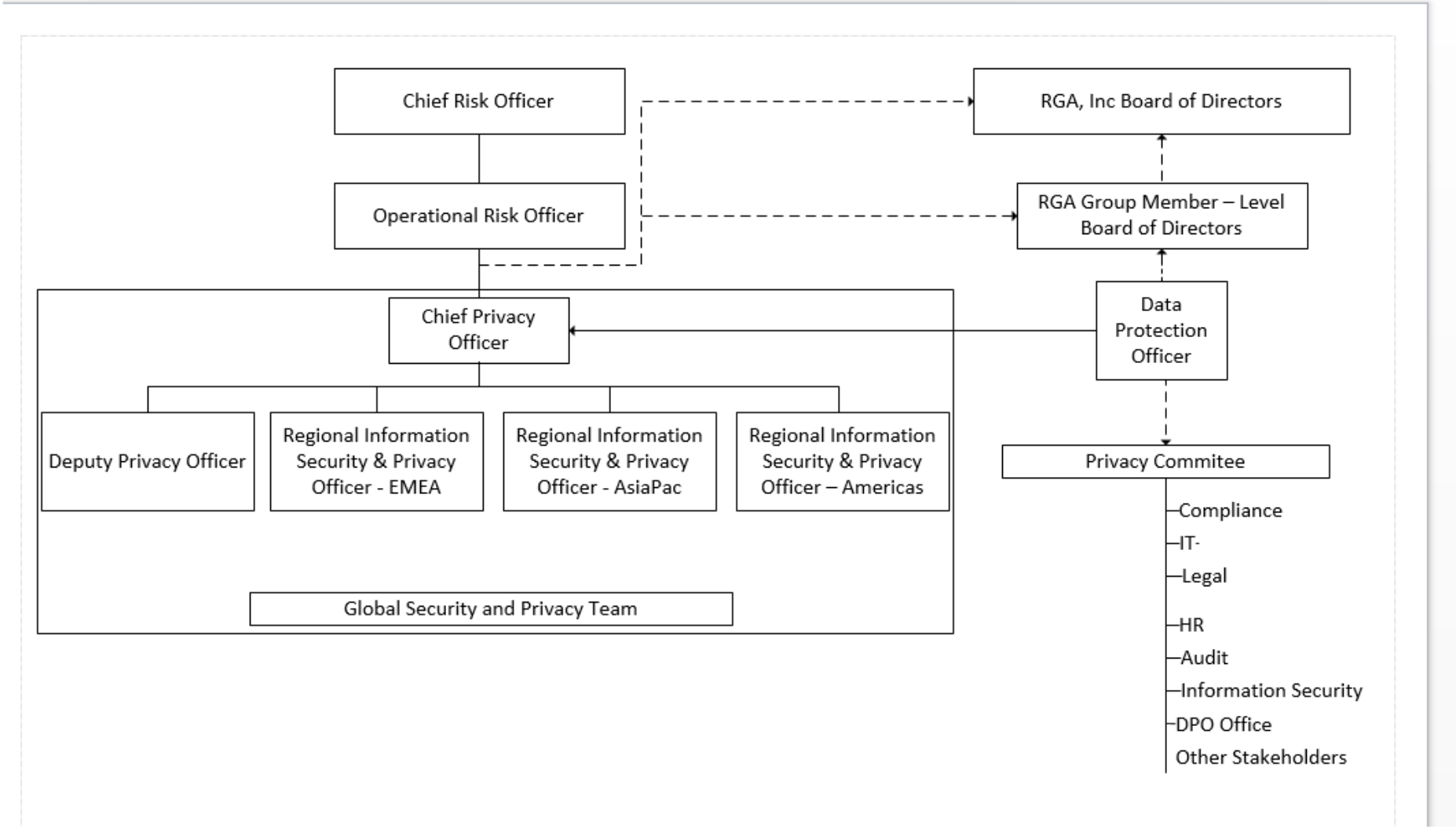
5.1.4 Through its liaison with the Data Protection Team, the Privacy Committee serves as a channel through which the Data Protection Team can communicate data privacy compliance actions to all key functional areas of the business.

5.2 The Privacy Committee will meet on a formal and regular basis, at a minimum frequency of every six months, to ensure a coordinated approach to data protection compliance across all functions.

6 RGA WORKFORCE MEMBERS

6.1 All RGA Workforce Members are responsible for supporting the functional Privacy Committee members on a day-to-day basis and adhering to RGA's privacy policies. In addition, RGA Workforce Members are responsible for escalating and communicating any potential violation of the privacy policies to the appropriate Privacy Committee Member or, if they prefer, the RGA Data Protection Team. On receipt of a notification of a potential violation of the privacy policy the issue will be investigated to determine if an actual violation occurred. Results of such investigations will be documented.

Figure 1: Overview of RGA's Data Protection & Privacy Compliance Structure



Final Version

DATED

BINDING CORPORATE RULES:

APPENDIX 4

PRIVACY TRAINING PROGRAM (CONTROLLER)

1 INTRODUCTION

1.1 The “Binding Corporate Rules: Controller Policy” and “Binding Corporate Rules: Processor Policy” (together the “**Policies**” or, respectively, the "**Controller Policy**" and the "**Processor Policy**") provide a framework for the transfer of Personal Information between Reinsurance Group of America Inc. ("**RGA**") group members ("**Group Members**"). The purpose of the Privacy Training Program (Controller) document is to provide a summary as to how RGA trains its Workforce Members on the requirements of the Controller Policy.

1.2 RGA trains its Workforce Members whose roles will bring them into contact with Personal Information, on the basic principles of data protection, confidentiality and information security awareness. It also provides specific training on particular legal obligations, such as the Health Insurance Portability and Accountability Act of 1996 ('HIPAA') in the US, and requirements and best practices, such as those specified by the International Organization for Standards (ISO) 27001 and on the General Data Protection Regulation (GDPR).

1.3 Workforce Members who have permanent or regular access to Personal Information and are involved in the Processing of Personal Information or in the development of tools to Process Personal Information receive additional, tailored training on the Policies and specific data protection issues relevant to their role. This training is further described below and is repeated on a periodic basis.

2 RESPONSIBILITY FOR THE PRIVACY TRAINING PROGRAM

2.1 RGA's Data Protection Team has overall responsibility for privacy training at RGA, with input from colleagues in other functional areas including Information Security, HR and other departments, as appropriate. They will review the training curriculum from time to time to ensure it addresses all relevant aspects of the Policies and that it is appropriate for individuals who have permanent or regular access to Personal Information, who are involved in the Processing of Personal Information or in the development of tools to Process Personal Information.

2.2 RGA's senior management supports the attendance of the privacy training courses and is responsible for ensuring that individuals within RGA are given appropriate time to attend and participate in such courses. Course attendance is monitored via regular audits of the training process. These audits are performed by RGA's Compliance team and/or independent third party auditors.

2.3 In the event these audits reveal persistent non-attendance, such findings will escalate to the Chief Privacy Officer for further action. Such action may include escalation of non-attendance to the appropriate management authority within RGA who will be responsible and held accountable for ensuring that the individual(s) concerned attend and actively participates in such training.

3 ABOUT THE TRAINING COURSES

3.1 RGA has developed mandatory electronic training courses, supplemented by additional training for Workforce Members, which could be face to face, on teleconference or video conferencing. The courses are designed to be both informative and user-friendly, generating interest in the topics covered. Workforce Members must correctly answer a series of multiple-choice questions on the electronic training courses for the course to be deemed complete.

3.2 All Workforce Members will be required to complete the training:

3.2.1 as part of their induction program;

3.2.2 as part of a regular refresher training at least once every two years (the timing of which is determined by RGA's Data Protection Team); and

3.2.3 when necessary based on changes in the law or to address any compliance issues arising from time to time.

3.3 Certain Workforce Members will receive specialist training, including those who are involved in particular Processing activities such as those who work in HR Business Development, Operations, Claims, Underwriting, Pricing, GFS and RGAx, or whose business activities include Processing Sensitive Personal Information. Specialist training is delivered in the form of additional modules to the basic training package, which will be tailored depending on the course participants.

4 TRAINING ON THE POLICIES

4.1 RGA's training on the Policies will cover the following main areas:

4.1.1 Background and rationale:

a) What is data protection law?

b) How data protection law will affect RGA internationally.

c) The scope of the Policies.

d) Terminology and concepts.

4.1.2 The Policies:

a) An explanation of the Policies.

b) Practical examples.

c) The rights that the Policies give to individuals.

d) The privacy implications arising from Processing Personal Information for clients.

4.1.3 Where relevant to a Workforce Member's role, training will cover the following procedures under the Policies:

a) Data Subject Rights Procedure (Controller or Processor, as applicable).

b) Updating Procedure (Controller or Processor, as applicable).

c) Cooperation Procedure (Controller or Processor, as applicable).

d) Complaint Handling Procedure (Controller or Processor, as applicable).

5 FURTHER INFORMATION

Any queries about training under the Policies should be addressed to RGA's Data Protection Team at privacy@rgare.com.

DATED

BINDING CORPORATE RULES:

APPENDIX 5

AUDIT PROTOCOL (CONTROLLER)

1 INTRODUCTION

1.1 Reinsurance Group of America Inc.'s ("**RGA**") “Binding Corporate Rules: Controller Policy” and “Binding Corporate Rules: Processor Policy” (together the “**Policies**” or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard Personal Information transferred between the RGA group members ("**Group Members**").

1.2 RGA must audit its compliance with the Policies on a regular basis, and the purpose of this document is to describe how and when RGA will perform such audits.

1.3 The role of RGA's Data Protection Team is to provide guidance about the Processing of Personal Information subject to the Policies and to assess the Processing of Personal Information by Group Members for potential privacy-related risks. The Processing of Personal Information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol (Controller) describes the formal assessment process adopted by RGA to ensure compliance with the Controller Policy as required by the data protection authorities, this is only one way in which RGA ensures that the provisions of the Controller Policy are observed and corrective actions taken as required.

2 APPROACH

Overview of audit

2.1 Compliance with the Policies is overseen on a day to day basis by RGA's Data Protection Team. RGA's Global Audit Team is responsible for performing and/or overseeing independent audits of compliance with the Policies and ensures that such audits address all aspects of the Policies. RGA's Global Audit Team is responsible for ensuring that any issues or instances of non-compliance arising from audit and assurance activity are brought to the attention of RGA's Data Protection Team and RGA's Chief Privacy Officer and relevant senior executives and that any corrective actions are determined and implemented within a reasonable time.

Frequency of audit

2.2 Audits of compliance with the Controller Policy are conducted:

2.2.1 at least annually in accordance with RGA's audit procedures; and/or

2.2.2 at the request of RGA's Chief Privacy Officer and / or the Board of Directors; and/or

2.2.3 as determined necessary by RGA's Data Protection Team (for example, in response to a specific incident).

Scope of audit

2.3 RGA's Global Audit Team will conduct a risk-based analysis to determine the scope of an audit, which will consider relevant criteria, such as: areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or Processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature and location of the Personal Information Processed.

Auditors

2.4 Audit of the Policies (including any related procedures and controls) will be undertaken by RGA's Global Audit Team. In addition, RGA may appoint independent and experienced professional auditors acting under a duty of confidence as necessary to perform audits of the Policies (including any related procedures and controls) relating to data privacy.

2.5 In addition, RGA agrees that European data protection authorities may audit Group Members for reviewing compliance with the Policies (including any related procedures and controls) in accordance with the terms of the Cooperation Procedure (Controller).

Reporting

2.6 Data privacy audit reports are submitted to RGA's Chief Privacy Officer, European Data Protection Officer and to the Board of Directors.

2.7 Upon request and subject to applicable law, RGA will provide copies of the results of data privacy audits of the Policies (including any related procedures and controls) to a competent European data protection authority.

2.8 RGA's Data Protection Team is responsible for liaising with the European data protection authorities for the purpose of providing the information outlined in section 2.7.

DATED

BINDING CORPORATE RULES:

APPENDIX 6

COMPLAINT HANDLING PROCEDURE (CONTROLLER)

1 INTRODUCTION

1.1 Reinsurance Group of America Inc.'s ("**RGA**") "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard Personal Information transferred between the RGA group members ("**Group Members**"). In order to affect individuals' third party beneficiary rights under the Binding Corporate Rules, RGA maintains a Complaint Handling Process for individuals to directly contact RGA regarding its compliance with the Policies. The purpose of this Complaint Handling Procedure (Controller) is to describe 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.

1.2 This procedure will be made available to individuals whose Personal Information is Processed by RGA under the Controller Policy.

2 HOW INDIVIDUALS CAN BRING COMPLAINTS

Individuals may bring complaints in writing by contacting RGA's Chief Privacy Officer at privacy@rgare.com.

3 COMPLAINTS WHERE RGA IS A CONTROLLER

Who handles complaints?

3.1 RGA's Data Protection Team will handle all complaints arising under the Controller Policy. RGA's Chief Privacy Officer will liaise with colleagues from relevant business and support units as appropriate to address the issues raised in the complaint.

What is the response time?

3.2 RGA's Data Protection Team will acknowledge receipt of a complaint to the individual concerned within 5 working days by sending a Complaint Receipt and Acknowledgment response email to the complainant individual. Thereafter, RGA will investigate the merits of the complaint, the underlying facts and circumstances surrounding the issues raised and will provide a substantive response within one month of the receipt of the complaint.

3.3 If, due to the complexity of the complaint or number of requests, a substantive response cannot be provided within this period, RGA's Data Protection Team will advise the complainant accordingly and provide a reasonable estimate (not exceeding a maximum of two further months) for the timescale within which a response will be provided. Every effort will be made to provide a substantive response to the individual without unreasonable delay and RGA shall at all times consider the interests of the individual.

What happens if a complainant disputes a finding?

3.4 If the complainant disputes the response from RGA's Data Protection Team or any aspect of a finding and notifies RGA's Data Protection Team, the matter will be referred to RGA's Chief Privacy Officer. The Chief Privacy Officer will review the case and advise the complainant of his/her decision either to accept the original finding or to substitute a new finding. The Chief Privacy Officer will respond to the complainant within one month of the receipt of the complaint. As part of the review, the Chief Privacy Officer may arrange to meet the parties to the complaint in an attempt to resolve it. If, due to the complexity of the complaint, a substantive response cannot be given within this period, the Chief Privacy Officer will advise the complainant accordingly and provide a reasonable estimate for the

timescale within which a response will be provided which will not exceed three months from the date the complaint was referred.

3.5 If the complainant persists in disputing the substantive response and/or resolution proposed by the Chief Privacy Officer, the Chief Privacy Officer will arrange for any necessary steps to be taken as a consequence, including involvement of the European Data Protection Officer.

4 RIGHT TO COMPLAIN TO A EUROPEAN DATA PROTECTION AUTHORITY AND/OR TO LODGE A CLAIM WITH A COURT OF COMPETENT JURISDICTION

4.1 Regardless of whether or not they have first complained directly to RGA, individuals have the right at all times to complain to a competent data protection authority and/or to lodge a claim with a court of competent jurisdiction in accordance with Applicable Data Protection Laws.

4.2 Individuals may lodge a complaint with the data protection authority of the individual's habitual residence, the data subject's place of work or the place of the alleged infringement.

4.3 In the event that the matter relates to Personal Information which was collected and / or used by a Group Member in Europe, but then transferred to a Group Member outside Europe and an individual wants to make a claim against RGA, the claim may be made against the Group Member in Europe responsible for Processing and exporting of the Personal Information. The claim can also be made to the courts of the Member State where the individual has his or her habitual residence.

DATED

BINDING CORPORATE RULES:

APPENDIX 7

COOPERATION PROCEDURE (CONTROLLER)

1 INTRODUCTION

Reinsurance Group of America Inc.'s ("**RGA**") "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard Personal Information transferred between RGA group members ("**Group Member**"). This Cooperation Procedure (Controller) sets out the way in which RGA will cooperate with the European data protection authorities in relation to the Controller Policy.

2 COOPERATION PROCEDURE

2.1 Where required, RGA will make the necessary Workforce Members available for dialogue with European data protection authorities in relation to the Policies.

2.2 RGA will actively review and consider:

2.2.1 any decisions made by relevant European data protection authorities on any Applicable Data Protection Law issues that may affect the Policies; and

2.2.2 the views of the European Data Protection Authorities in connection with Binding Corporate Rules for Processors and Binding Corporate Rules for Controllers, as outlined in its published Binding Corporate Rules guidance.

2.3 Subject to applicable law, RGA will provide upon request copies of the results of any audit of the Policies to a relevant European data protection authority.

2.4 RGA agrees that any Group Member may be audited for compliance with the Policies by the competent European data protection authority in accordance with the Applicable Data Protection Laws of its jurisdiction:

2.4.1 For compliance with the BCR Controller Policy: by the data protection authority competent for the RGA Group Member who is Processing Personal Information as a Controller or Processor.

2.5 RGA agrees to comply with the advice and to abide by a formal decision of any competent data protection authority on any issues relating to the interpretation and application of the Policies under Applicable Data Protection Laws, notwithstanding its right to appeal such decision in accordance with applicable procedural laws.

Final Version

DATED

BINDING CORPORATE RULES:

APPENDIX 8

UPDATING PROCEDURE (CONTROLLER)

1 INTRODUCTION

1.1 Reinsurance Group of America Inc.'s ("**RGA**") "Binding Corporate Rules: Controller Policy" ("**Controller Policy**") and "Binding Corporate Rules: Processor Policy" ("**Processor Policy**") (together the "**Policies**") safeguard Personal Information transferred between the RGA group members ("**Group Members**"). This Updating Procedure (Controller) sets out the way in which RGA will communicate changes to the Controller Policy to the European data protection authorities, individual data subjects, Controllers and to the Group Members.

1.2 Any reference to RGA in this procedure is to the Chief Privacy Officer who will ensure that the commitments made by RGA in this Updating Procedure (Controller) are met.

2 MATERIAL CHANGES TO THE POLICIES

2.1 RGA will communicate any material changes to the Policies (including any modification that would possibly affect the level of protection offered by the Binding Corporate Rules or significantly affect the Binding Corporate Rules including as a result of any change in Applicable Data Protection Laws) without undue delay to the competent Data Protection Authority and to any other relevant European data protection authorities.

3 ADMINISTRATIVE CHANGES TO THE POLICIES

3.1 RGA will communicate changes to the Policies which:

3.1.1 are administrative in nature (including changes in the list of Group Members); or

3.1.2 have occurred as a result of either a change of Applicable Data Protection Laws in any European country or due to any legislative, court or supervisory authority measure;

to the competent Data Protection Authority and to any other relevant European data protection authorities at least once a year. RGA will also provide a brief explanation to the competent Data Protection Authority and to any other relevant data protection authorities of the reasons for any notified changes to the Policies.

4 COMMUNICATING CHANGES TO THE POLICIES

4.1 RGA will communicate all changes to the Policies, whether material or administrative in nature:

4.1.1 to the Group Members bound by the Policies via written notice (which may include e-mail)*;* and

4.1.2 systematically to Controllers and the individuals who benefit from the Policies via www.rgare.com.

4.2 RGA will maintain and update a list of Group Members bound by the Policies. This information will be available on request from RGA.

5 LOGGING CHANGES TO THE POLICIES

The Policies contain a change log which sets out the date each Policy is revised and the details of any revisions made. RGA will maintain an up-to-date list of the changes made to the Policies.

6 NEW GROUP MEMBERS

RGA will ensure that all new Group Members are bound by and have implemented the Policies before a transfer of Personal Information to them takes place.