Oct 2024

GLOBAL BINDING CORPORATE RULES (EU)

PROCESSOR POLICY

Contents

Table of Contents

INTRODUCTION

The Binding Corporate Rules: Processor Policy ("**Processor Policy**") establishes RGA's approach to compliance with data protection law when Processing Personal Information on behalf of and under the instructions of a non-RGA Controller and where such Personal Information originates in the EEA, specifically with regard to transfers of Personal Information between members of the RGA group entities. In this Processor Policy we use "**RGA**" to refer to RGA BCR Members ("**BCR Members**").

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

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

Definitions

For the purposes of this Processor 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 an EEA BCR Member or Controller initially transfers Personal Information under this Processor Policy. Where an EEA BCR Member, acting as a Processor, transfers Personal Information under this Processor Policy to a non-EEA BCR Member, acting as a sub-processor, the term Applicable Data Protection Laws shall include the EEA data protection laws applicable to that EEA BCR Member. Where a non-EEA BCR Member transfers onward Personal Information from an EEA BCR Member, to another non-EEA BCR Member, Applicable Data Protection Laws shall include the EEA data protection laws applicable to the original EEA BCR Member;
"BCR Member"	means any of the members of RGA's group of companies listed in Appendix 1;
"Biometric Data"	means Personal Information resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;
"Competent Supervisory Authority"	means the EEA Supervisory Authority competent for the data exporter
"Consent"	of the Data Subject, means any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by statement or by a clear affirmative action, signifies agreement to the processing of Personal Information relating to him or her;
"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's Customer is a Controller of the Personal Information that is Processed by RGA under this Processor Policy;
"Customer"	refers to the third party Controller on whose behalf RGA Processes Personal Information. It includes RGA's third party Customers when we, as Processors, Process Personal Information on their behalf in the course of providing data Processing services to them;

"Data Concerning Health"	means Personal Information related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status;
"Data Subject"	an identified or identifiable natural person as described in the definition of Personal Information;
"EEA"	as used in this Processor Policy refers to the Member States of the European Economic Area – that is, the 27 Member States of the European Union plus Norway, Lichtenstein and Iceland;
"European Union", "EU"	as used in this Controller Policy refers to the 27 Member States of the European Union;
"Exporter", "Data Exporter"	means the BCR Member from which a transfer originates;
"Filing System", "Filing Systems"	means any structured set of Personal Information which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis;
"Genetic Data"	means Personal Information relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question;
"Importer", "Data Importer"	means the BCR Member which is the recipient of a transfer from a Data Exporter;
"Lead Supervisory Authority"	means the Irish Data Protection Commission;
"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;
"Personal Information Breach", "Data Security Breach", "Breach"	means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Information transmitted, stored or otherwise processed;
"Processing", "Processed",	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,

"Process", "Processes"	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 example, RGA is a Processor of the Personal Information it Processes to provide certain services to its Customers;
"Profiling"	means any form of automated processing of Personal Information consisting of the use of Personal Information to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
"Recipient", "Recipients"	means a natural or legal person, public authority, agency or another body, to which the Personal Information are disclosed, whether a third party or not. However, public authorities which may receive Personal Information in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;
"Restriction of Processing"	means the marking of stored Personal Information with the aim of limiting their processing in the future;
"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
"Supervisory Authority"	means an independent public authority (Data Protection Authority) established by an EEA Member State to be responsible for monitoring the application of Applicable Data Protection Law(s);
"Workforce Members"	refers to all employees, new hires, individual contractors and consultants, and temporary members of the Workforce engaged by any RGA BCR Member. All Workforce Members must comply with this Processor Policy.

PART I: BACKGROUND AND SCOPE

WHAT IS DATA PROTECTION LAW?

Applicable Data Protection Laws give individuals certain rights in connection with the way in which their Personal Information is used. If organizations do not comply with Applicable Data Protection Laws, they may be subject to sanctions and penalties imposed by member state Supervisory Authorities and the courts. When RGA Processes Personal Information to provide a service to a Controller, this activity and the Personal Information in question are 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 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 (i.e. RGA's Customer) will be primarily responsible for meeting the legal requirements.

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

HOW DOES DATA PROTECTION LAW AFFECT RGA INTERNATIONALLY?

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

In the absence of Adequacy regulations permitting a transfer then RGA will base its transfers (those identified in Appendix 10 to this policy) on this Processor Policy.

WHAT IS RGA DOING ABOUT IT?

RGA must take proper steps to ensure it Processes Personal Information in a legitimate, fair and lawful manner wherever it operates or undertakes business. This Processor 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 BCR Members in the EEA and transferred to BCR Members outside the EEA, either where the Personal Information is collected by a third-party Controller in the EEA,

or where the Personal Information is collected by a BCR Member in the EEA as a Processor.

SCOPE OF THE PROCESSOR POLICY

This Processor Policy applies to all Personal Information that RGA Processes as a Processor in the course of providing services to a third party Controller (i.e. a Customer). This includes Processing by RGA of the following categories of Personal Information:

- Policyholder data: including Personal Information of individuals who are parties to or beneficiaries of primary individual or group insurance and pension policies; and
- RGA Workforce Member Personal Information: including Personal Information of past and current RGA Workforce Members, individual consultants, independent contractors, temporary Workforce Members, and job applicants that RGA may Process on behalf of the Controller, e.g. for payroll purposes.

RGA will apply this Processor Policy in all cases where RGA Processes Personal Information as a Processor by both manual and automatic means. Please see EU Appendix 10 In Scope Data Transfers (Processor) for additional details.

MANAGEMENT COMMITMENT AND CONSEQUENCES OF NON-COMPLIANCE

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

All BCR Members and their Workforce Members must comply with and respect, this Processor Policy when Processing Personal Information, irrespective of the country in which they are located. All BCR Members that engage in the collection, use or transfer of Personal Information as a Processor to provide services to a third party Controller, must comply with the Rules set out in **Part II** of this Processor Policy together with the policies and procedures set out in the appendices in **Part III** of this Processor Policy.

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

RESPONSIBILITY TOWARDS THE CONTROLLER

When RGA Processes Personal Information as a Processor, the Controller on whose behalf RGA Processes Personal Information will have responsibility for complying with the Applicable Data Protection Laws that apply to it. As a consequence, the Controller will pass certain data protection obligations on to RGA in its contract appointing RGA as its Processor. If RGA fails to comply with the terms of its Processor appointment, this may put the Controller in non-compliance with its Applicable Data Protection Laws and the Controller may initiate proceedings against RGA for breach of contract, resulting in the payment of compensation or other judicial remedies.

In particular, where a Controller demonstrates that it has suffered damage, and that it is likely that the damage has occurred due to a non-compliance with this Processor Policy (whether by a BCR Member or a third party Processor appointed by a BCR Member), RGA will be responsible for demonstrating that such BCR Member is not responsible for the non-compliance, or that no such non-compliance took place. For EEA Controllers, this burden of proof for demonstrating that the BCR Member is not responsible for the non-compliance, or that no such non-compliance took place, shall fall to RGA International Reinsurance Company dac (Ireland).

When a Controller transfers Personal Information to a BCR Member for Processing in accordance with this Processor Policy, a copy of this Processor Policy shall be incorporated into the contract with that Controller. If a Controller chooses not to rely upon this Processor Policy when transferring Personal Information to a BCR Member outside the EEA, that Controller is responsible for implementing other appropriate safeguards in accordance with Applicable Data Protection Laws.

RELATIONSHIP BETWEEN THE CONTROLLER AND PROCESSOR POLICIES

This Processor Policy applies only to Personal Information that RGA Processes as a Processor in order to provide a service to a third party Controller (i.e. a Customer).

RGA has a separate Binding Corporate Rules: Controller Policy that applies when it Processes Personal Information as a Controller (i.e. for its own purposes). When an RGA BCR Member Processes Personal Information either as a Controller, or as a Processor (but only where acting on behalf of another BCR Member), it must comply with the Controller Policy.

Some BCR Members may act as Controllers under some circumstances and as Processors under different circumstances. Such BCR Members must comply with this Processor Policy and the Controller Policy, as appropriate.

If at any time it is not clear to a BCR 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 BCR 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 Processor Policy, your rights under this Processor 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:	Chris Cooper, Vice President, Global Chief Security and Privacy Officer

Email:	ccooper@rgare.com
Address:	16600 Swingley Ridge Road, Chesterfield, Missouri, 63017, USA

RGA's Chief Privacy Officer is responsible for ensuring that changes to this Processor Policy are communicated to the Controller 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 (Processor), which is outlined in Part III, Appendix 6.

PART II: PROCESSOR OBLIGATIONS

This Processor Policy applies in all situations where a BCR Member Processes Personal Information as a Processor on behalf of a third party Controller.

Part II of this Processor 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 Processor on behalf of a third party Controller.
- Section B specifies the practical commitments to which RGA adheres in connection with this Processor Policy.
- Section C describes the third party beneficiary rights RGA provides to individuals under this Processor Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS OF PROCESSING

Rule 1A – 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 the EEA, 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.

To the extent that any Applicable Data Protection Laws require a higher level of protection than is provided for in this Processor Policy, RGA acknowledges that it will take precedence over this Processor Policy.

As such:

- where Applicable Data Protection Laws exceed the standards set out in this Processor Policy, RGA will comply with those laws; but
- where there is no data protection law, or where the law does not meet the standards set out by this Processor Policy, RGA will Process Personal Information in accordance with the Rules in this Processor Policy.

Rule 1B – RGA will cooperate with and assist a Controller in complying with its obligations under Applicable Data Protection Laws in a reasonable time and to the extent reasonably possible.

RGA will assist such Controller in complying with its obligations under Applicable Data Protection Laws, within a reasonable time and as required under the terms of its contract with the Controller. This may include, for example, a responsibility to comply with certain instructions stipulated in the contract with a Controller, such as assisting the Controller in meeting its obligation to keep Personal Information accurate and up to date. RGA will immediately inform the Controller if, in its opinion, an instruction infringes applicable data protection law.

RULE 2 – FAIRNESS AND TRANSPARENCY

Rule 2 – RGA will, to the extent reasonably possible, assist a Controller in complying with the requirement to inform and explain to individuals how their Personal Information will be processed at the time their Personal Information is collected.

The Controller has a duty to inform individuals, at the time their Personal Information is collected, or shortly after, how that information will be used. Such information should be given to individuals in a concise, transparent, intelligible and easily accessible form. The information shall be provided in writing or by other means, including, where appropriate,

by electronic means. This is usually done by means of an easily accessible fair processing statement.

RGA will provide assistance and information to the Controller as may be required under the terms of its contract with such Controller to support its compliance with this requirement. For example, RGA may be required under the terms of the contract with a particular Controller to provide information about any sub-processors appointed by RGA to Process Personal Information on its behalf.

RULE 3 – PURPOSE LIMITATION

Rule 3 – RGA will only Process Personal Information on behalf of, and in accordance with, the instructions of the Controller.

RGA will only Process Personal Information on behalf of the Controller and in compliance with the terms of the contract it has in place with that Controller. RGA will not Process the Personal Information for any purpose other than or beyond the purposes determined by the Controller.

If for any reason, RGA is unable to comply with this Rule or its obligations under this Processor Policy, RGA will inform the Controller promptly of this fact who may then suspend the transfer of Personal Information to RGA and/or terminate the contract, depending upon the terms of its contract with RGA.

In such circumstances, RGA will act in accordance with the instructions of the Controller and return, destroy or store the Personal Information, including any copies of the Personal Information, in a secure manner or as otherwise required, in accordance with the terms of its contract with that Controller.

In the event that legislation prevents RGA from returning the Personal Information to a Controller, or destroying it, RGA will maintain the confidentiality of the Personal Information and will not Process the Personal Information otherwise than in accordance with the terms of its contract with that Controller.

RULE 4 – DATA MINIMISATION AND ACCURACY

Rule 4 – RGA will assist a Controller in keeping the Personal Information accurate and up to date.

RGA will comply with any instructions from a Controller, as required under the terms of its contract with that Controller, in order to assist that Controller in complying with its obligation to keep Personal Information accurate and up to date and, in particular, to ensure that all Personal Information are accurate, having regard to the purposes for which they are Processed, and/or are erased or rectified without delay.

When required to do so on instruction under the terms of its contract with that Controller, RGA will delete, anonymise, update or correct Personal Information.

RGA will notify other BCR Members or any third party sub-processors to whom the Personal Information has been legitimately disclosed accordingly so that they can also update their records.

RULE 5 – LIMITED RETENTION OF PERSONAL INFORMATION

Rule 5 – RGA will assist a Controller in complying with the obligation to retain Personal Information no longer than is necessary for the purposes for which it was collected and further Processed.

RGA will enable the Controller to comply with its record retention obligations either under law or in accordance with the Controller's record retention policies and guidelines, unless Applicable Data Protection Laws require otherwise.

RULE 6 – SECURITY AND CONFIDENTIALITY

Rule 6A – RGA will implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk of the Personal Information Processing that is carried out on behalf of a Controller.

Where RGA provides a service to a Controller involving the Processing of Personal Information, the contract between RGA and that Controller shall dictate the security and organizational measures required to safeguard that information consistent with Applicable Data Protection Laws, where applicable.

In any event, RGA will apply appropriate security and organisational measures to ensure a level of security that is appropriate to the risk of the Processing that is carried out on behalf of the Controller.

Rule 6B – RGA will notify a Controller without undue delay of any data security breach affecting the Personal Information that RGA is Processing on behalf of the Controller in accordance with the terms of the contract with that Controller.

RGA will notify a Controller of any data security breach, as required under Applicable Data Protection Laws, affecting the Personal Information Processed on behalf of that Controller without undue delay; after becoming aware of it and as required to do so under the terms of the BCR Member's contract with that Controller.

RULE 7 – ENGAGING SUB-PROCESSORS

Rule 7A – RGA will notify and obtain the prior specific or general written consent from the Controller before appointing any sub-processor.

RGA will inform a Controller where Processing undertaken on its behalf will be conducted by a sub-processor and will obtain the Controller's prior approval to do so as set out under the terms of its contract with that Controller. RGA will ensure that up to date

information regarding its appointment of sub-processors is available to a Controller at all times so that its general consent is obtained.

If, upon reviewing this information, a Controller objects to the appointment of a sub-processor to Process Personal Information on its behalf, that Controller will be entitled to take such steps as are consistent with the terms of its contract with RGA.

Rule 7B – RGA will ensure that sub-processors are (i) engaged on the same contractual terms as those executed between RGA and the Controller; and (ii) required to comply with this Processor Policy, particularly obligating the sub-processor to implement and maintain appropriate technical and organisational measures for the protection of the Personal Information consistent with this Processor Policy.

BCR Members must only appoint sub-processors who provide sufficient guarantees with respect to the commitments made by RGA in this Processor Policy. In particular, such sub-processors must be able to provide appropriate technical and organizational measures that will govern their use of the Personal Information to which they will have access in accordance with the terms of the BCR Member's contract with the Controller.

To comply with this Rule, where a sub-processor has access to Personal Information Processed on behalf of RGA, RGA will take steps to ensure that the sub-processor has in place appropriate technical and organizational security measures to safeguard the Personal Information and will impose strict contractual obligations, in writing, on the sub-processor, which provide:

- commitments on the part of the sub-processor to comply with the same data protection contractual provisions as between RGA and the Controller;
- commitments on the part of the sub-processor regarding the security of that Personal Information, consistent with those contained in this Processor Policy (and in particular Rules 6A and 6B above) and with the terms of the contract RGA has with the Controller in respect of the Processing in question;
- that the sub-processor will act only on RGA's instructions in the course of Processing the Personal Information; and
- such obligations as may be necessary to ensure that the commitments on the part of the sub-processor reflect those made by RGA in this Processor Policy, and which, in particular, provide for adequate safeguards with respect to the privacy and fundamental rights and freedoms of individuals with respect to transfers of Personal Information from a BCR Member in the EEA to a sub-processor established outside the EEA.

RULE 8 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

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

In principle, transfers of Personal Information to third countries are not permitted unless:

- Personal Information is transferred to a third country that is deemed to have an adequate level of protection by the European Commission, or
- Prior to the transfer, RGA will:

    1. Assess if the level of protection required by EU law and this Processor Policy is respected in the third country concerned, taking into account:

        - the laws and practices of the third country which may affect the respect of the commitments contained in the BCRs, while understanding that laws and practices that:
            - respect the essence of the fundamental rights and freedoms, and
            - do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR (e.g. national or public security),

          are not in contradiction to the BCR-P;

        - the specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same third country or to another third country, including:

            - purposes for which the data are transferred and processed,
            - types of entities involved in the processing,
            - the economic sector in which the transfer(s) occur,
            - categories and format of the personal data transferred,
            - location of the processing including storage, and
            - transmission channels used;

        - the laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards; and

- any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCRs, including measures applied during the transmission and the processing of the personal data in the country of destination;

2. use or implement appropriate safeguards such as:
    - use this Policy for internal transfers, or
    - enter into standard contractual clauses with a third party who is receiving the data or
    - ensure that any relevant third party can provide adequate protection through other means (e.g. approved code of conduct, approved certification mechanism), and
3. where any supplementary measures in addition to the safeguards envisaged under the BCRs should be put in place, the Data Protection Officer and Data Privacy Officer for those BCR member(s) in the EEA with data protection responsibility will be informed and involved in the assessment. BCR members will be informed of the subsequently agreed actions for application to other transfers of the same type.

Where effective supplementary measures cannot be put in place, the transfers at stake will be suspended or ended.

RGA's documented assessment will take into account any transit locations, possible interference with Data Subjects' fundamental rights created by third country legislation and the possibility of legal access requests. The assessments will be available to Supervisory Authorities upon request.

RGA commits to monitor, on an ongoing basis, developments in third countries that may affect the initial assessment of the level of protection.

RULE 9 – HONOURING INDIVIDUALS' DATA PRIVACY RIGHTS

Rule 9 – RGA will assist a Controller with responding to queries or requests made by individuals in connection with their Personal Information.

RGA will act in accordance with the instructions of the Controller as required under the terms of its contract with that Controller and undertake any reasonably necessary measures to enable a Controller to comply with its duty to respect the rights of individuals. In particular, if any BCR Member receives a request by a Data Subject to exercise his/her rights over the Processing of his or her Personal Information, the BCR Member will transfer such request promptly to the relevant Controller and not respond to such a request unless authorised to do so or required by law (in accordance with Appendix 2).

SECTION B: PRACTICAL COMMITMENTS

RULE 10 – COMPLIANCE

Rule 10A – RGA will have appropriate Workforce Members and support to ensure and oversee privacy compliance throughout the business.

RGA has appointed its Chief Privacy Officer as the person to oversee and ensure compliance with this Processor 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 Processor Policy on a day-to-day basis, enjoying the highest management support for the fulfilling of this task. A summary of the roles and responsibilities is set out in Appendix 3.

Rule 10B – RGA will maintain records of the Processing activities carried out on behalf of the Controller.

RGA shall maintain and update a record of all the Processing activities carried out on behalf of a Controller. This record will be maintained in writing (including in electronic form) and will be made available to the Supervisory Authorities on request.

RULE 11 – TRAINING

Rule 11 – RGA will provide appropriate and up-to-date 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 (Processor) set out in Appendix 4.

RULE 12 – AUDIT

Rule 12 – RGA will verify compliance with this Processor Policy and will carry out data protection audits on a regular basis in accordance with the Audit Protocol (Processor) set out in Appendix 5.

RULE 13 – COMPLAINT HANDLING

Rule 13 – 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 (Processor) set out in Appendix 6.

RULE 14 – COOPERATION WITH SUPERVISORY AUTHORITIES

Rule 14 – RGA will cooperate with the Competent Supervisory Authorities and to comply with the advice they give on any issue related to the Processor Policy in accordance with the Cooperation Procedure (Processor) set out in Appendix 7.

RULE 15 – UPDATES TO THE PROCESSOR POLICY

Rule 15 – RGA will report changes to this Processor Policy to the Lead Supervisory Authority in accordance with the Updating Procedure (Processor) set out in Appendix 8.

RULE 16 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE PROCESSOR POLICY

Rule 16A – RGA will ensure that where it believes that the legislation applicable to it prevents it from fulfilling its obligations under this Processor Policy or such legislation has a substantial effect on its ability to comply with the Processor Policy, RGA will promptly inform:

- **the Controller as provided for by Rule 3 (unless otherwise prohibited by a law enforcement authority); and**
- **RGA's Chief Privacy Officer.**

Rule 16B – RGA will ensure that where it receives a legally binding request for disclosure of Personal Information by a law enforcement authority or state security body which is subject to this Processor Policy, RGA:

- **will notify the Controller promptly unless prohibited from doing so by a law enforcement authority; and**
- **may put the request on hold and notify the Lead Supervisory Authority and the appropriate Supervisory Authority competent for the Controller and for RGA unless prohibited from doing so by a law enforcement authority or state security body.**

RGA will use its best efforts to inform the law enforcement authority or state security body about its obligations under Applicable Data Protection Laws and to obtain the right to waive this prohibition.

In any case, transfers of Personal Information by a BCR Member 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 the EEA by a BCR Member acting as a Processor (an "**EEA Entity**") and/or transferred to a BCR Member located outside the EEA (and which BCR Member may transfer onward to any other BCR Member outside the EEA) under the Processor Policy (a "**Non-EEA Entity**") have certain rights. These rights also exist where a Non-EEA Entity BCR Member acting as a Processor receives Personal Information under the Processor Policy from a Controller located within the EEA. The principles that individuals may enforce as third party beneficiaries are those that are set out in the Intra-Group Agreement (EU), available upon request, and under the following sections of the Controller Policy:

- Part I (Background and Scope);
- Part II Section A (Basic Principles); and
- Part II Section B (Practical Commitments) Rules:
    - 10B (Records),
    - 13 (Complaint Handling, see Appendix 6 for the procedure),
    - 14 (Cooperation with Supervisory Authorities, see Appendix 7 for the procedure),
    - 15 (Updating Procedure, see Appendix 8 for the procedure)
    - 16 (National Legislation preventing compliance).
- Part II Section C (Third party Beneficiary Rights):
    - The Liability, compensation and jurisdiction provisions (below)

These individuals may directly enforce the Processor Policy as third party beneficiaries, and they may also directly enforce the Processor Policy as third party beneficiaries where they cannot bring a claim against a Controller in respect of non-compliance of any of the commitments in this Processor Policy by a BCR Member (or by a sub-processor) acting as a Processor because:

- the Controller has factually disappeared or ceased to exist in law or has become insolvent; and
- no successor entity has assumed the entire legal obligations of the Controller by contract or by operation of law.

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 (Processor) (Appendix 6) and may also lodge a complaint with an EEA Supervisory 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 Processor Policy have been infringed as a result of the Processing of their Personal Information in non-compliance with this Processor Policy. Individuals may bring proceedings against RGA International Reinsurance Company dac (Ireland) to enforce compliance with this Processor 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 Processor Policy have the right to receive redress and compensation from the Processor for the damage suffered. In particular, in case of non-compliance with this Processor Policy by a non-EEA Entity or any third party processor which is established outside the EEA, 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 damage suffered as a result of an infringement of this Processor Policy, in accordance with the determination of the court or other competent authority; and
- **Transparency**: Individuals may obtain a copy of this Processor Policy and the Intra-group Agreement entered into by RGA in connection with this Processor Policy from RGA International Reinsurance Company dac (Ireland) or any other EEA Entity upon request.
- **Representation**: Individuals may be represented by a not-for-profit body, organization or association in both *Complaints* and *Proceedings* as described above.

Where a Non-EEA Entity acts as a Processor on behalf of a third party Controller, then 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 (i) a Non-EEA Entity; or (ii) any third party sub-processor who is established outside the EEA who is acting on behalf of a Non-EEA Entity, is not responsible for the non-compliance, or that no such non-compliance took place.

RGA International Reinsurance Company dac (Ireland) will ensure that any action necessary is taken to remedy any non-compliance with the Processor Policy by a Non-EEA Entity or any third party processor which is established outside the EEA and which is Processing Personal Information on behalf of a Controller.

Where a BCR Member, acting as a Processor, and a Controller involved in the same Processing are found responsible for any damage caused by such Processing, the Data Subject shall be entitled to receive compensation for the entire damage directly from RGA International Reinsurance Company dac (Ireland).

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

Change Log

Date	Change
October 2021	Added 'EU' to distinguish from UK BCRs Updated Chief Security and Privacy Officer details
May 2022	No updates – date refresh only
Oct 2024	Incorporated EDPB, admin and rebranding changes including: Added to Definitions section, aligned with GDPR definitions, and capitalized defined terms throughout; clarified definitions of several terms including Applicable Data Protection Laws Updated 'Europe(an)' to 'EEA', 'Group Member to 'BCR Member, and 'Data Protection Authority(ies)' to 'Supervisory Authority(ies)' Noted that this Processor Policy applies in the absence of Adequacy for a given destination jurisdiction Added 'third-party' to clarify the term 'Controller' in Part I "What is RGA doing about it?" Clarified information in the "Relationship between the Controller and Processor Policies" section In Rule 6B, clarified that notification of data breach will be performed as 'required' by Applicable Data Protection Law Inserted Rule 8: Ensuring Adequate Protection for Transborder Transfers; renumbered subsequent Rules and references to Rules, e.g., in Section C: Third Party Beneficiary Rights Noted in Rule 10 that the CPO has the highest management support for fulfilling tasks Noted in Rule 11 that training content will be up-to-date In Rule 16, adjusted references to notifying the Competent Supervisory Authority since no longer required Regarding Section C: Third Party Beneficiary Rights: • Bulleted, added titles of Rules/sections for readability; • Added Rule 15 (Updating Procedure and Appendix 8) as an enforceable right; • added references to Appendix 6 and Appendix 7 for ease of cross-referencing;

	• added the term "redress" under the Compensation section for clarity; • added reference to "not-for-profit" and other bodies being permitted to represent individuals as described in both *Complaints* and *Proceedings* sections Created Appendix 10: In Scope Data Transfers

PART III: APPENDICES

(See separate documents for each Appendix)

APPENDIX 1 – LIST OF RGA BCR MEMBERS (PROCESSOR)

APPENDIX 2 – DATA SUBJECT RIGHTS PROCEDURE (PROCESSOR)

APPENDIX 3 – PRIVACY COMPLIANCE STRUCTURE (PROCESSOR)

APPENDIX 4 – PRIVACY TRAINING PROGRAM (PROCESSOR)

APPENDIX 5 – AUDIT PROTOCOL (PROCESSOR)

APPENDIX 6 – COMPLAINT HANDLING PROCEDURE (PROCESSOR)

APPENDIX 7 – COOPERATION PROCEDURE (PROCESSOR)

APPENDIX 8 – UPDATING PROCEDURE (PROCESSOR)

APPENDIX 9 – LAW ENFORCEMENT DATA ACCESS PROCEDURE (PROCESSOR)

APPENDIX 10 – IN SCOPE DATA TRANSFERS (PROCESSOR)