Oct 2024

GLOBAL BINDING CORPORATE RULES (EU)

CONTROLLER POLICY

Contents

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 the EEA, 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 BCR members ("**BCR 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.

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 an EEA BCR Member initially transfers Personal Information under this Controller Policy. Where an EEA BCR Member transfers Personal Information under this Controller Policy to a non-EEA BCR Member, 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, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Information; where the purposes and means of such processing are determined by Union or Member State law, the

	controller or the specific criteria for its nomination may be provided for by Union or Member State law;
"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 Controller Policy refers to the Member States of the European Economic Area – i.e. 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", "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, public authority, agency or other body 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 BCR Member;
"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 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 member state SupervisoryAuthorities 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 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 9 to this policy) on this Controller Policy.

WHAT IS RGA DOING ABOUT IT?

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

SCOPE OF THE 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 of past and current RGA Workforce Members, Workforce Members' children, senior level executives, 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, event attendees, survey participants, consumers and potential business clients;
- Policyholder data: including Personal Information of individuals who are parties to or beneficiaries, including children, of primary individual or group insurance and pension policies;
- Supply chain management data: including Personal Information of individual contractors and of account managers and staff of third-party suppliers who provide services to RGA; and
- Other third party data: including any other Personal Information related to its Directors or unaffiliated third parties such as analytics providers, borrows (lenders), consultants, investigators, insurance brokers, lawyers, office visitors, 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. Please see EU Appendix 9 In Scope Data Transfers (Controller) 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 Controller Policy at all times.

All BCR 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 BCR Members that engage in the collection, use or transfer of Personal Information as a Controller or as a Processor acting on behalf of another BCR 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 BCR 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 BCR Member, i.e., a third-party Controller. When RGA Processes Personal Information on behalf of a RGA BCR Member it must comply with the Controller Policy.

Some BCR Members may Process Personal Information as Controllers under some circumstances and as Processors under different circumstances. Such BCR Members must comply with this Controller Policy and the Processor 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 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:	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 any changes to this Controller Policy are communicated to all RGA BCR 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 BCR 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 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.

RGA will ensure all Processing of Personal Information has a legal basis (as described in the publicly available Privacy Notice)) in compliance with Applicable Data Protection Law and any applicable local legislation 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 regarding the Processing of their Personal Information.

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.

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

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, ensure individuals have 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 BCR Member in the EEA intends to **transfer** Personal Information to a BCR Member outside the EEA 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.

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 BCR 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 the EEA;
- 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, the relevant RGA entity will notify the Chief Privacy Officer, RGA International Reinsurance Company dac (Ireland), and the controller (if relevant entity is a processor), without undue delay and in accordance with the requirements of Applicable Data Protection Laws.

RGA will notify the competent regulator without undue delay; where feasible, not later than 72 hours after having become aware of the personal data breach; 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.

The facts of the data Breach shall be documented and made available to the competent regulator.

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 countries outside the EEA without ensuring adequate protection for the Personal Information in accordance with the standards set out by this Controller 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 Controller 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-C;

- 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 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

Rule 9 – RGA will only Process Sensitive Personal Information collected in the EEA where the individual's explicit Consent has been obtained, unless RGA has an alternative legitimate basis for doing so consistent with the Applicable Data Protection Laws of the EEA country in which the Personal Information was collected.

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 EEA 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, enjoying the highest management support for the fulfilling of this task. 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 Supervisory Authorities on request. These records will maintain at least the information required by Articles 30(1) and 30(2) GDPR.

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 and up-to-date privacy training to Workforce Members who have permanent or regular access to Personal Information, who are involved in the Processing of Personal Information or in the development of tools used to Process Personal Information in accordance with the Privacy Training Program (Controller) 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 SUPERVISORY AUTHORITIES

Rule 16 – RGA agrees to comply with the advice and to abide by a formal decision of any Competent Supervisory Authority on any issues relating to the interpretation and application of the 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 Lead Supervisory Authority in accordance with the Updating Procedure (Controller) set out in Appendix 8.

RULE 18 – NON-COMPLIANCE WITH THE CONTROLLER POLICY

Rule 18 – RGA will ensure that where a Data Importer is in breach of, or unable to comply with, the Controller Policy for any reason, that Importer will inform the Data Exporter.

The Exporter should suspend the transfer(s) until compliance is again ensured or the transfer is ended.

If compliance cannot be restored within one month, or

- the Importer is in substantial or persistent breach of the Controller Policy, or
- the Importer fails to comply with a binding decision of a competent court or Competent Supervisory Authority regarding its obligations under the Controller Policy,

the transfers will be ended immediately and data transferred previously, and any copies thereof, will be immediately returned to the Exporter or destroyed entirely,

at the choice of the BCR Member acting as Exporter. In the case of destruction, the Importer should certify to the Exporter that the data has been deleted.

Until the data is deleted or returned, the data importer should continue to ensure compliance with the Controller Policy.

In case of local laws applicable to the Importer that prohibit the return or deletion of the transferred personal data, the Importer should warrant that it will continue to ensure compliance with the Controller Policy, and will only process the data to the extent and for as long as required under that local law.

RULE 19 – ACTION WHERE NATIONAL LEGISLATION PREVENTS COMPLIANCE WITH THE CONTROLLER POLICY

Rule 19 – RGA will ensure that where it believes legislation applicable to it prevents it from fulfilling its obligations under the Controller Policy or such legislation has a substantial effect on its ability to comply with the Controller Policy (which may include a legally binding request for disclosure of Personal Information by a law enforcement authority or state security body in a third country), the BCR Member acting as Data Importer will promptly inform:

- **the BCR Members acting as Data Exporter;**
- **the Chief Privacy Officer and**
- **RGA International Reinsurance Company dac;**

unless otherwise prohibited by a law enforcement authority.

Where a Data Importer or Data Exporter believes legislation applicable to itself or the other party prevents it from fulfilling obligations under the Controller Policy, the Data Exporter, the Chief Privacy Officer and RGA International Reinsurance Company dac, will promptly seek to identify supplementary measures to be adopted by the Data Exporter and/or Data Importer to enable them to fulfil their obligations under the Controller Policy. If RGA determines that despite supplementary measures the Controller Policy cannot be complied with for any reason, or if instructed by the Competent Supervisory Authority, the Exporter commits to suspending the transfer(s), until compliance is again ensured or the transfer(s) are ended. If compliance cannot be restored within one month, the transfers will be ended and data transferred previously will be returned to the Exporter or destroyed entirely, at the choice of the BCR Member acting as Exporter. RGA will communicate to other BCR Members that conduct similar transfers other supplementary measures that need to be implemented or to cease transfers.

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

RULE 20 – ACTION WHERE GOVERNMENT ACCESS REQUEST PREVENTS COMPLIANCE WITH THE CONTROLLER POLICY

Rule 20 – If a BCR Member acting as Data Importer receives a legally binding government access request for disclosure of Personal Information, the Importer will promptly notify:

- **the BCR Member acting as Data Exporter and,**
- **where possible, the Data Subject (if necessary with the help of the Data Exporter),**

unless prohibited from doing so by a law enforcement authority or agency.
The Importer will also notify the Exporter if the Importer becomes aware of any direct access by public authorities to Personal Information.

If prohibited from performing any of the notification(s), the Data Importer will use its best efforts to obtain a waiver of this prohibition in order to communicate as much information as possible, and as soon as possible, to the Data Exporter and/or the Data Subject.

Notification regarding a legally binding request shall include:

- information about the personal data requested,
- the requesting body,
- the legal basis for the request, and
- the response provided.

Notification regarding any direct access will include all information available to Data Importer.

Additionally, the Data Importer will provide the Data Exporter, at regular intervals, with as much relevant information as possible regarding the requests received, in particular: number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of the challenges, etc.).

The Data Importer shall document its best efforts in order to be able to demonstrate those efforts upon request of the Data Exporter. If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will without undue delay, inform the Data Exporter accordingly. The Data Importer will also preserve the abovementioned information for as long as the Personal Information is subject to the safeguards of this Policy, as well as make it available to the Competent Supervisory Authorities upon request.

The Data Importer will review the legality of the disclosure request, challenge the request, and pursue possibilities of appeal if it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the destination country and applicable international law. The Data Importer will seek interim

measures to suspend the effects of the request until the competent judicial authority has ruled. The Data Importer will not disclose the Personal Information requested until required to do so under the applicable procedural rules.

The Data Importer will document its legal assessment and any challenge to the request for disclosure. To the extent permissible under the laws of the country of destination, the Data Importer will make the documentation available to the Data Exporter, as well as the Competent Supervisory Authorities upon request.

The Data Importer will provide the minimum amount of information permissible when responding to a disclosure request, based on a reasonable interpretation of the request. 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 the EEA by a BCR Member acting as a Controller (an "**EEA Entity**") and/or transferred to a BCR Member located outside the EEA (and which BCR Member may transfer onward to any other BCR Member outside the EEA) under the Controller Policy (a "**Non-EEA Entity**") have certain rights. The principles that individuals may enforce as third party beneficiaries are those that are set out in the Intra-Group Agreement (EU), available upon request, and under the following sections of the Controller Policy:

- Part I (Background and Scope);
- Part II Section A (Basic Principles); and
- Part II Section B (Practical Commitments) Rules:
    - 12B (Records),
    - 15 (Complaint Handling (see Appendix 6 for the procedure),
    - 16 (Cooperation with SupervisoryAuthorities, see Appendix 7 for the procedure),
    - 17 (Updating Procedure, see Appendix 8 for the procedure),
    - 19 (National Legislation preventing compliance)
    - 20 (Government Access Request preventing compliance)
- Part II Section C (Third Party Beneficiary Rights):
    - The Liability, compensation and jurisdiction provisions (below)

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

- **Complaints**: Individuals may submit complaints to any EEA Entity in accordance with the Complaint Handling Procedure (Controller) (Appendix 6) and may also lodge a complaint with an EEA Supervisory Authority in the jurisdiction of their habitual residence, 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 redress, and 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.
- **Representation**: Individuals may be represented by a not-for-profit body, organization or association in both *Complaints* and *Proceedings* as described above.

Where individuals can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a non-compliance with 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.

Change Log

Date	Change
October 2021	Added 'EU' to distinguish from UK BCRs Updated Chief Security and Privacy Officer details
January 2022	Re-included definition of "Applicable Data Protection Laws" Updated Rule 8 – Transborder Transfers
May 2022	Minor update in formatting in rule 2
Feb 2023	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 definition of several terms including Applicable Data Protection Laws Updated 'Europe(an)' to 'EEA' and 'Group Member' to 'BCR Member' Noted that this Controller Policy applies in the absence of Adequacy for a given destination jurisdiction Expanded in-scope Data Subjects Simplified and clarified "Relationship between the Controller and Processor Policies" section Added reference to publicly available Privacy Notice outlining legal bases relied upon Broadened Rule 2 beyond just when Personal Information is collected, and noted Data Subjects' right to obtain copies of the Controller Policy and Intragroup Agreement upon request Added detail to Rule 6C regarding Breach notification, including 72 hour timeframe Updated Rule 8 to reference "third countries" in place of "third parties" and noted additional detail addressed in transfer assessments Noted in Rule 12A that the CPO has the highest management support for fulling tasks Added level of detail kept in records of Processing activities to Rule 12B Noted in Rule 13 that training content will be up-to-date

	Replaced Rule 18A with Rule 18 covering actions related to any non-compliance with BCRs Replaced Rule 18B with Rule 19 regarding actions to be taken if unable to comply with Controller Policy due to National Legislation Added Rule 20 regarding Government Access Requests including the Data Importer's responsibilities to notify the Data Exporter and use "best efforts" instead of "reasonable efforts" to fulfil those responsibilities Removed references to notifying the Competent Supervisory Authority which is no longer required. Regarding Section C: Third Party Beneficiary Rights: • Bulleted, added titles of Rules/sections for readability; • Added Rule 17 (Updating Procedure and Appendix 8) as an enforceable right; • Added references to Appendix 6 and Appendix 7 for ease of cross-referencing; • Added Rule 20 (Government Access Request preventing compliance) as an enforceable right; • 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

PART III: APPENDICES

(See separate documents for each Appendix)

APPENDIX 1 – LIST OF RGA BCR 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)

APPENDIX 9 – IN SCOPE DATA TRANSFERS (CONTROLLER)