September 2024

GLOBAL BINDING CORPORATE RULES (UK):

CONTROLLER POLICY

Contents

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

"Processing", "Processed",
"Process", "Processes"

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

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

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

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

MANAGEMENT COMMITMENT AND CONSEQUENCES OF NON-COMPLIANCE

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

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

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

RELATIONSHIP BETWEEN THE CONTROLLER AND PROCESSOR POLICIES

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

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

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

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

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

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

FURTHER INFORMATION

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

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

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

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

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS OF PROCESSING

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

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

As such:

to the extent that any applicable local legislation governing the protection of Personal Information requires a higher level of protection than is provided for in this Controller Policy, RGA acknowledges that it will take precedence over this Controller Policy; but

where there is no applicable local legislation governing the protection of Personal Information, or where the local law does not meet the standards set out by the Controller Policy, RGA will Process Personal Information in accordance with the Rules in this Controller Policy.

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

RULE 2 – FAIRNESS AND TRANSPARENCY

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

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

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

UK GDPR Article 13 - Personal Information that are

the **recipients** or categories of recipients of their Personal I

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. 90 (d) 12 el 3.525 hu 3.525ae,-6.3 (

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;

Rule 7B – RGA will also deal with requests to rectify or erase Personal Information, or to restrict or object to the Processing of Personal Information, and to exercise the right of data portability in accordance with the Data Subject Rights Procedure (Controller).

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

In certain circumstances, as set out in Appendix 2, Data Subjects may also restrict or object to the P.

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

Rule 12C – RGA will carry

Rule 18A – RGA will ensure that where it believes legislation applicable to it prevents it from fulfilling its obligations under the Controller Policy or such legislation has a substantial effect on its ability to comply with the Controller Policy (which may include a legally binding request for disclosure of Personal Information by a law enforcement authority or state security body in a third country), RGA will promptly inform:

the Chief Security and Privacy Officer and RGA UK Services;

the Information Commissioner;

unless otherwise prohibited by a law enforcement authority.

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

RGA will use its best efforts to inform the requesting authority or agency about its obligations under Applicable Data Protection Laws and to obtain the right to waivcisid nf (ai)-8.91 (t)]TJ-0 (ai)-8.1(r)]T0 Tc 0 T0.8

Liability, Compensation and Jurisdiction provisions:

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

Where a Controller Third Party Beneficiary can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a non-compliance with this Policy by a Non-UK BCR Entity or external sub-processors outside the UK, it will be for RGA UK Services to prove that the Non-UK BCR Entity was not responsible for the non-compliance with this Policy giving rise to those damages or that no such non-compliance took place,

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

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

Data Subjects may lodge a complaint with the Information Commissioner,

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

PART III: APPENDICES

APPENDIX 1

LIST OF RGA GROUP MEMBERS (UK) (CONTROLLER)

APPENDIX 2

DATA SUBJECT RIGHTS PROCEDURE (UK) (CONTROLLER)

APPENDIX 3

PRIVACY COMPLIANCE STRUCTURE (UK) (CONTROLLER)

APPENDIX 4

PRIVACY TRAINING PROGRAM (UK) (CONTROLLER)

APPENDIX

APPENDIX 6

COMPLAINT HANDLING PROCEDURE (UK) (CONTROLLER)

APPENDIX 7

COOPERATION PROCEDURE (UK) (CONTROLLER)

APPENDIX 8

UPDATING PROCEDURE (UK) (CONTROLLER)

CHANGE LOG

Date	Version	Change
Sep 2023	1.0	