

UK Binding Corporate Rules RGA Controller Policy (Summary Statement)

Effective November 2023

INTRODUCTION

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

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

RGA's Global Binding Corporate Rules (UK): Processor Policy describes how RGA will comply with Applicable Data Protection Laws with respect to processing Personal Information as a Processor.

The Information Commissioner has regulatory oversight of the functioning of the RGA Binding Corporate Rules (UK) and RGAs compliance to this Policy. This Controller Policy does not replace any specific data protection requirements that might apply to a business area or function.

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

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 Global Security and Privacy Office using the contact information below:

Attention: Global Security and Privacy Office
Email: Privacy@rgare.com
Address: 16600 Swingley Ridge Road, Chesterfield, Missouri, 63017, USA

PART II: CONTROLLER OBLIGATIONS

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

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

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

- Section C describes the third-party beneficiary rights RGA provides to Data Subjects under this Controller Policy.

SECTION A: BASIC PRINCIPLES

RULE 1 – LAWFULNESS OF PROCESSING

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

RULE 2 – FAIRNESS AND TRANSPARENCY

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

RULE 3 – PURPOSE LIMITATION

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

3B RGA will Process Personal Information only for specified, explicit and legitimate purposes and not further Process that information in a manner that is incompatible with those purposes unless such further Processing is consistent with Applicable Data Protection Laws.

RULE 4 – DATA MINIMISATION AND ACCURACY

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

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.

RULE 5 – LIMITED RETENTION OF PERSONAL INFORMATION

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

RULE 6 – SECURITY AND CONFIDENTIALITY

6A RGA will implement appropriate technical and organizational measures to ensure a level of security around Personal Information that is appropriate to the risk for the rights and freedoms of the Data Subjects.

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

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

RULE 7 – HONOURING DATA SUBJECTS' DATA PRIVACY RIGHTS

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

RULE 8 – ENSURING ADEQUATE PROTECTION FOR TRANSBORDER TRANSFERS

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

RULE 9 – SAFEGUARDING THE USE OF SENSITIVE PERSONAL INFORMATION

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

RULE 10 – LEGITIMISING DIRECT MARKETING

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

RULE 11 – AUTOMATED DECISION MAKING, INCLUDING PROFILING

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

SECTION B: PRACTICAL COMMITMENTS

RULE 12 – COMPLIANCE

- 12A** RGA will have appropriate Workforce Members and support to ensure and oversee privacy compliance throughout the business.
- 12B** RGA will maintain records of the Processing activities it carries out for its own purposes.
- 12C** RGA will carry out a data protection impact assessment where the Processing is likely to result in a high risk for the data subjects.

RULE 13 – PRIVACY TRAINING

RGA will provide appropriate privacy training to Workforce Members who have permanent or regular access to Personal Information, who are involved in the Processing of Personal

Information or in the development of tools used to Process Personal Information in accordance with the Privacy Training Program (UK) (Controller) attached as Appendix 4.

RULE 14 – AUDIT

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

RULE 15 – COMPLAINT HANDLING

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

RULE 16 – COOPERATION WITH THE INFORMATION COMMISSIONER

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

RULE 17 – UPDATES TO THE CONTROLLER POLICY

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

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

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.

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.

SECTION C: THIRD PARTY BENEFICIARY RIGHTS

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

- Part I (Background and Scope);
- Part II section A (Basic Principles); and
- Part II section B (Practical Commitments) rules:
 - 12B (Records),
 - 15 (Complaint Handling (see Appendix 6 for the procedure),
 - 16 (ICO Co-operation),
 - 18 (National Legislation preventing compliance)
 - The Liability, compensation and jurisdiction provisions (below).

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

Liability, Compensation and Jurisdiction provisions:

- Controller Third Party Beneficiaries who have suffered material or non-material damage as a result of an infringement of this Policy have the right to receive remedy and compensation.
- Where a Controller Third Party Beneficiary can demonstrate that they have suffered damage and establish facts which show it is likely that the damage has occurred because of a non-compliance with this Policy by a Non-UK BCR Entity or external sub-processors outside the UK, it will be for RGA UK Services to prove that the Non-UK BCR Entity was not responsible for the non-compliance with this Policy giving rise to those damages or that no such non-compliance took place,
- In particular, in case of non-compliance with this Policy by a non-UK BCR Entity, a Controller Third Party Beneficiary may exercise these rights and remedies against RGA UK Services and, where appropriate, receive remedy and compensation from RGA UK Services for any material or non-material damage suffered as a result of an infringement of this Policy.
- A Controller Third Party Beneficiary may bring proceedings against RGA UK Services to enforce compliance with this Policy before a competent UK Court,
- Data Subjects may lodge a complaint with the Information Commissioner,

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

PART III: APPENDICES

- APPENDIX 1 LIST OF RGA GROUP MEMBERS (UK) (CONTROLLER)
- APPENDIX 2 DATA SUBJECT RIGHTS PROCEDURE (UK) (CONTROLLER)
- APPENDIX 3 PRIVACY COMPLIANCE STRUCTURE (UK) (CONTROLLER)
- APPENDIX 4 PRIVACY TRAINING PROGRAM (UK) (CONTROLLER)
- APPENDIX 5 AUDIT PROTOCOL (UK) (CONTROLLER)
- APPENDIX 6 COMPLAINT HANDLING PROCEDURE (UK) (CONTROLLER)
- APPENDIX 7 COOPERATION PROCEDURE (UK) (CONTROLLER)
- APPENDIX 8 UPDATING PROCEDURE (UK) (CONTROLLER)
- APPENDIX 9 In Scope Data Transfers (UK) (CONTROLLER)