September 2023

BINDING CORPORATE RULES (UK):

APPENDIX 3

PRIVACY COMPLIANCE STRUCTURE (UK) (CONTROLLER)

1 INTRODUCTION

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

2 CHIEF SECURITY AND PRIVACY OFFICER

2.1 RGA has appointed a Chief Security and Privacy Officer who provides executive-level oversight of, and has responsibility for, ensuring RGA's compliance with Applicable Data Protection Laws and the Policies. The Chief Security and Privacy Officer reports directly to Reinsurance Group of America Inc. Board of Directors on all material or strategic issues relating to RGA's compliance with Applicable Data Protection Laws and the Policies and is accountable to RGA's independent Audit Committee. The Chief Security and Privacy Officer leads, and is supported by, RGA's Data Protection Team. The Chief Security and Privacy liaises with RGA's EMEA located DPO (Section 3).

2.2 The Chief Security and Privacy Officer's key responsibilities include:

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

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

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

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

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

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

2.2.7 Dealing with any escalated privacy complaints in accordance with the Binding Corporate Rules (UK): Appendix 6 - Complaint Handling Procedure (UK) (Controller);

2.2.8 Reviewing and responding to Data Production Requests.; and

2.2.9 Advising the Data Protection Team on complex Data Subjects Rights requests (i.e. complex access, objection to processing or restriction of processing requests) in accordance with the Binding Corporate Rules (UK): Appendix 2 – Data Subject Rights Procedure (UK) (Controller).

3 DATA PROTECTION OFFICERS

3.1 In addition to the Chief Security and Privacy Officer (Section 2), RGA has appointed a Data Protection Officer to further ensure compliance with Applicable Data Protection Laws and the Policies. The DPO, employed by RGA UK Services, maintains a certain level of independence and

reports to the Chief Security and Privacy Officer and the Board of Directors of RGA UK Services (and Boards of other Group Members in EMEA).

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

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

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

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

3.2.4 To cooperate with the Information Commissioner; and

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

4 DATA PROTECTION TEAM

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

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

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

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

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

4.1.5 Responding to inquiries of the Information Commissioner where appropriate;

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

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

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

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

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

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

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

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

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

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

4.2.2 Performing its own reviews and/or overseeing independent 3rd party assessments of compliance with the Policies and will ensure that such reviews address all aspects of the Policies; and

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

5 PRIVACY COMMITTEE

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

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

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

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

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

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

6 RGA WORKFORCE MEMBERS

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

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