September 2023

BINDING CORPORATE RULES (UK):

APPENDIX 5

AUDIT PROTOCOL (UK) (CONTROLLER)

1 INTRODUCTION

1.1 RGA's "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**") safeguard Personal Information transferred between the RGA group members ("**Group Members**").

1.2 RGA must audit its compliance with the Policies on a regular basis, and the purpose of this document is to describe how and when RGA will perform such audits.

1.3 The role of RGA's Data Protection Team is to provide guidance about the Processing of Personal Information subject to the Policies and to assess the Processing of Personal Information by Group Members for potential privacy-related risks. The Processing of Personal Information with the potential for a significant privacy impact is, therefore, subject to detailed review and evaluation on an on-going basis. Accordingly, although this Audit Protocol (UK) (Controller) describes the formal assessment process adopted by RGA to ensure compliance with the Controller Policy as required by the Information Commissioner, this is only one way in which RGA ensures that the provisions of the Controller Policy are observed and corrective actions taken as required.

2 APPROACH

Overview of audit

2.1 Compliance with the Policies is overseen on a day to day basis by RGA's Data Protection Team. RGA's Global Audit Team is responsible for performing and/or overseeing independent audits of compliance with the Policies and ensures that such audits address all aspects of the Policies. RGA's Global Audit Team is responsible for ensuring that any issues or instances of non-compliance arising from audit and assurance activity are brought to the attention of RGA's Data Protection Team and RGA's Chief Security and Privacy Officer and relevant senior executives and that any corrective actions are determined and implemented within a reasonable time.

Frequency of audit

2.2 Audits of compliance with the Controller Policy are conducted:

2.2.1 at least annually in accordance with RGA's audit procedures; and/or

2.2.2 at the request of RGA's Chief Security and Privacy Officer and / or the Board of Directors; and/or

2.2.3 as determined necessary by RGA's Data Protection Team (for example, in response to a specific incident).

Scope of audit

2.3 RGA's Global Audit Team will conduct a risk-based analysis to determine the scope of an audit, which will consider relevant criteria, such as: areas of current regulatory focus; areas of specific or new risk for the business; areas with changes to the systems or Processes used to safeguard information; areas where there have been previous audit findings or complaints; the period since the last review; and the nature and location of the Personal Information Processed.

Auditors

2.4 Audit of the Policies (including any related procedures and controls) will be undertaken by RGA's Global Audit Team. In addition, RGA may appoint independent and experienced professional

auditors acting under a duty of confidence as necessary to perform audits of the Policies (including any related procedures and controls) relating to data privacy.

2.5 In addition, RGA agrees that Information Commissioner may audit Group Members for reviewing compliance with the Policies (including any related procedures and controls) in accordance with the terms of the Cooperation Procedure (Controller).

Reporting

2.6 Data privacy audit reports are submitted to RGA's Chief Security and Privacy Officer, the RGA DPO, and to the Boards of Directors of RGA UK Services, RGA International Reinsurance Company DAC, and as appropriate, summaries to Reinsurance Group of America, Inc.

2.7 Upon request RGA will provide copies of the results of data privacy audits of the Policies (including any related procedures and controls) to the Information Commissioner.

2.8 RGA's Data Protection Team is responsible for liaising with the Information Commissioner for the purpose of providing the information outlined in section 2.7.