Oct 2024

GLOBAL BINDING CORPORATE RULES (EU)

APPENDIX 5

AUDIT PROTOCOL (PROCESSOR)

1. Introduction

1.1.1. Reinsurance Group of America Inc.'s ("**RGA**") "Binding Corporate Rules: Controller Policy" and "Binding Corporate Rules: Processor Policy" (together the "**Policies**" or, respectively, the "**Controller Policy**" and the "**Processor Policy**") safeguard Personal Information transferred between the RGA BCR Members ("BCR **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 BCR 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 (Processor) describes the formal assessment process adopted by RGA to ensure compliance with the Processor Policy as required by the Supervisory Authorities, this is only one way in which RGA ensures that the provisions of the Processor 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 (not the DPO) is responsible for determining the audit plan and 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 Privacy Officer and relevant senior executives and that any corrective actions are determined and implemented within a reasonable time. The persons in charge of audits are guaranteed independence as to the performance of their duties related to these audits.

2.2. Where RGA acts as a Processor, the Controller (or auditors acting on its behalf) may audit RGA for compliance with the commitments made in the Processor Policy and may extend such audits to any sub-processors acting on RGA's behalf in respect of such Processing, in accordance with the terms of the Controller's contract with RGA.

Frequency of audit

2.3. Audits of compliance with the Processor Policy are conducted:

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

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

2.3.3. as determined necessary by RGA's Data Protection Team (for example, in response to a specific incident); and/or

2.3.4. (with respect to audits of the Processor Policy), as required by the terms of the Controller's contract with RGA.

Scope of audit

2.4. 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.

2.5. In the event that a Controller exercises its right to audit RGA for compliance with the Processor Policy, the scope of the audit shall be limited to the data processing facilities, data files and documentation relating to that Controller. RGA will not provide a Controller with access to systems that Process Personal Information of another Controller.

Auditors

2.6. 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. RGA may engage an external auditor to perform that work. Internal Audit may also bring in external auditors to supplement if RGA does not have bandwidth or requires additional expertise.

2.7. In the event that a Controller exercises its right to audit RGA for compliance with the Processor Policy, such audit may be undertaken by that Controller, or by independent and suitably experienced auditors selected by that Controller, as required by the terms of the Controller's contract with RGA.

2.8. In addition, RGA agrees that Competent Supervisory Authorities may audit BCR Members for reviewing compliance with the Policies (including any related procedures and controls) in accordance with the terms of the Cooperation Procedure (Processor).

Issue Resolution

2.9. Any issues, and the action plans for their resolution, are tracked by both Internal Audit and the Global Data Protection Office in formal issue tracking systems. Prior to the agreed-upon deadline for the action plans, Audit follows up with management to determine if the issue has been remediated, or if additional work needs to be done. Once an issue is addressed, Audit and the Global Data Protection Office close the issue in their respective tracking systems.

Reporting

2.10. Data privacy audit reports are submitted to RGA's Chief Privacy Officer, European Data Protection Officer and to the Board of Directors of RGA International Reinsurance Company DAC, and as appropriate, summaries to Reinsurance Group of America, Inc.

2.11. Upon request, RGA will:

2.11.1. provide copies of the results of data privacy audits of the Policies (including any related procedures and controls) to a Competent Supervisory Authority; and

2.11.2. to the extent that an audit relates to Personal Information RGA Processes on behalf of a Controller, report the results of any audit of compliance with the Processor Policy to that Controller.

2.12. RGA's Data Protection Team is responsible for liaising with the Competent Supervisory Authorities for the purpose of providing the information outlined in section 2.11.

Change Log

Date	Change
October 2021	Added 'EU' to distinguish from UK BCRs
May 2022	No updates – date refresh only
Oct 2024	Capitalized terms defined in Definitions section of BCR-P Policy Noted Global Audit team's responsibility for determining the audit plan and noted DPO is not responsible for auditing Noted specific RGA legal entities who receive audit reports Updated "Group Members" to "BCR Members" and "Data Protection Authority" to "Supervisory Authority" Added language re guaranteed independence Noted context for engaging an external auditor Added detail re Audit Issue Resolution