

Gen Re Global Vendor Code of Conduct

(as per August 2026)

Introduction

At Gen Re, we are committed to maintaining the highest standards of integrity, transparency, and accountability in our business operations. This Vendor Code of Conduct (“Vendor Code”) outlines the minimum requirements we have for our vendors. It is designed to ensure that our vendors and all related parties adhere to ethical practices, comply with applicable laws and regulations, and contribute to the resilience, sustainability and security of our operations.

1. Ethical Business Practices

We expect our vendors to act with honesty, fairness and transparency in all their dealings with us and with others. Our vendors must not engage in any form of bribery, corruption, fraud, money laundering, tax evasion, sanctioned activity or other illegal or unethical practices. Our vendors must also avoid any conflicts of interest or situations that may compromise their objectivity or loyalty to Gen Re.

2. Compliance with Laws, Regulations and Gen Re Policies and Procedures

We expect our vendors to comply with all applicable laws and regulations in the countries where they operate and where they provide services or products to the relevant Gen Re entity. This includes, but is not limited to, laws and regulations related to labor and human rights, health and safety, environmental protection, intellectual property, embargoes, trade restrictions and trade sanctions. Where relevant, our vendors must also following Gen Re company policies and procedures and cooperate with any audits or investigations that we may conduct.

3. Artificial Intelligence

Gen Re expects all of its vendors to inform Gen Re of any planned or actual use of artificial intelligence (AI) systems as part of services provided to Gen Re. This notification should include information regarding the purpose and operation of the AI system and state whether any Gen Re data will be processed by these AI systems and relevant details regarding the processing.

Vendor use of AI systems as part of services for Gen Re should be ethical, transparent, and comply with applicable laws and regulatory requirements. Gen Re expects its vendors to promote fairness, prevent bias, and prohibit any form of illegal discrimination when using AI systems.

4. Labor Practices and Human Rights

We expect our vendors to commit to providing a safe and healthy work environment for their employees, contractors and visitors, and take appropriate measures to prevent accidents, injuries and illnesses. When working on our premises or sites our vendors must follow our health and safety policies and procedures.

Our vendors must respect the labor rights of their employees and contractors and treat them fairly and respectfully. We expect our vendors to ensure equal employment opportunities for all employees and applicants, regardless of any characteristics protected by law. Our vendors must not use any form of forced labor, child labor, human trafficking or modern slavery in their operations or supply chain. Our vendors must also comply with all applicable labor laws and regulations, such as those relating to wages, social security contributions, working hours, benefits, non-discrimination, diversity, harassment, grievance mechanisms and freedom of association. Vendors must ensure they possess and maintain all necessary legal authorizations and permits required to deliver their services, including permissions to allocate resources to Gen Re.

5. Data Protection and Information Security

We expect our vendors to protect the confidentiality, integrity and availability of the information that they access, process or store on our behalf or that belongs to a Gen Re entity, our clients or any Gen Re agent or representative. Our vendors must implement appropriate technical and organizational measures to comply with applicable information security laws and regulations, including but not limited to preventing unauthorized access, use, disclosure, modification or loss of such information, and, where required, promptly notify Gen Re of any actual or suspected security incident affecting Gen Re information. Our vendors must also comply with all applicable data protection laws and regulations and obtain our prior written consent before transferring any personal data across borders or disclosing it to third parties. Vendors are expected to:

- Implement robust security measures to protect the confidentiality, integrity, and availability of information assets. Identify and remediate security vulnerabilities promptly and maintain secure configurations of systems handling Gen Re data.
- Process Gen Re data only for the purposes defined by Gen Re and limit collection, use and retention to what is necessary to perform agreed services in compliance with applicable data protection laws, regulations and contractual obligations.
- Retain data only for as long as necessary and securely delete or return data upon request or upon termination of the engagement.
- Protect data using appropriate encryption or equivalent safeguards for data in transit and at rest, where applicable.
- Not engage sub-processors or subcontractors that access Gen Re data without prior written approval and ensuring equivalent security and data protection obligations.
- Ensure personnel with access to Gen Re data are appropriately trained on information security and confidentiality obligations.
- Upon request, participate in security risk assessments conducted by Gen Re which are reviewed and updated periodically, and provide information and supporting documentation to support such assessments.
- Upon request, provide independent assurance reports (e.g., SOC 2 Type II, ISO 27001 certification) or equivalent evidence of the effectiveness of security controls.

6. Information and Communication Technology (ICT) Vendors

Gen Re expects ICT Vendors to:

- Understand and Manage Information and Communication Technology (ICT) Risks: Vendors must understand and manage their risk exposure to cybersecurity threats related to ICT applications, infrastructure, and third-party providers that enable critical business processes.
- Vendors must have a business continuity management program commensurate to the nature, size and complexity of their business which includes an internal governance and control framework that ensures effective and prudent management of their ICT risk to achieve operational resilience
- Regular Risk Assessments: Vendors must perform thorough due diligence and risk assessments before engaging with ICT third-party service providers to ensure alignment with Gen Re's information security standards.

7. Sustainability

Vendors are encouraged to align with Gen Re's commitment to sustainability and responsible business practices proportionate to their business model or industry. This includes reducing environmental impact, promoting social welfare, and practicing good governance. The Gen Re website provides comprehensive information on the company's commitment to sustainability and responsible business practices. ([ESG](#))

8. Monitoring, Auditing and Reporting

We reserve the right to monitor and audit our vendors' compliance with this Vendor Code and expect our vendors to fully cooperate with us in this regard. The failure to comply with this Vendor Code gives the relevant Gen Re entity the right to terminate the contractual relationship with the vendor.

We also expect our vendors to inform us promptly about violations of this Vendor Code and to take corrective actions to address any identified non-compliance issues. In addition, vendors must ensure that their employees and subcontractors are aware of and comply with this Vendor Code.

Conclusion

Gen Re is committed to building strong, ethical, and sustainable relationships with its vendors. By adhering to this Vendor Code, vendors contribute to the mutual success and integrity of our business operations. This also includes the discipline to commence providing services to Gen Re and to invoice the cost of such services only after the respective service contract has been concluded in writing.

We appreciate your cooperation. These principles will be incorporated into your contract as appropriate.