

ARAG Third Party Code of Conduct



1. Introduction

The **ARAG UK Third Party Code of Conduct** (the ‘**Code**’) sets out our expectations for how those we do business with will conduct themselves and is applicable to all third parties without exception.

In this Code, a ‘third party’ is any organisation that transacts business with or provides goods or services to any entity within the ARAG UK Group (being ARAG UK Holdings Limited and each subsidiary of such company) and reference to ‘ARAG’ in this Code shall be construed accordingly. We ask that all third parties, and their employees and subcontractors, comply with the standards and expectations within this Code.

Non-compliance with this Code may constitute a material breach of contract and may adversely affect a third party’s future commercial relationship with ARAG. A third party must, upon written request from ARAG, certify to ARAG in writing that it is complying with this Code and provide such supporting evidence of compliance as ARAG may reasonably request. A third party must maintain written records that demonstrate its compliance with this Code.

In the event of conflict or contradiction between this Code and the terms of any contract entered into between ARAG and the third party, the terms of the contract shall prevail except to the extent that this Code imposes a higher or more detailed standard to the corresponding term in the contract, in which case this Code shall prevail.

2. ARAG Standards & Expectations

ARAG acts ethically and with integrity in all business transactions, including treating third parties with honesty, fairness and respect. **Corporate Social Responsibility** is of relevance to all our business and activities. We actively seek to engage with third parties who are culturally aligned with our approach. We expect all third parties to comply with these standards, including but not limited to:

- Maintain the highest integrity in all business relationships (including respecting confidentiality);
- Promoting the eradication of unethical business practices;
- Ensuring full compliance with laws and regulations;
- Achieving the highest standards of health and safety;
- Committing to minimise, mitigate and manage environmental impacts;

- Supporting the communities in which we operate;
- Awareness of, and avoiding the use of forced labour (modern slavery);
- Procurement based on best total value including but not limited to quality (not just cost);
- Incorporating ecological and social aspects in the procurement of goods and services;
- Communicating expectations to suppliers openly and sharing our goals;
- Avoiding conflict and building trust with third parties through collaboration to create value;
- Identifying, mitigating and managing risks appropriately;
- Supporting effective whistleblowing processes;
- Avoid offering or accepting any gift or hospitality which might give the appearance of influencing a business decision relating to a third party arrangement;
- Aligning with the Chartered Institute of Procurement & Supply (CIPS) Corporate Code of Ethics. Please see www.cips.org/employers/services/ethical-services/corporate-code-of-ethics for more information;
- Supporting the principles of diversity and inclusion;
- Promoting good customer outcomes; and
- Adapting behaviours and processes appropriately to best manage (and, as appropriate, safeguard the interests of) all categories of customer, including without limitation any vulnerable customers.

3. Anti-Bribery, Anti-Corruption & Fraud

At ARAG's request, third parties must disclose the persons or entities that own a controlling interest, report any changes and disclose any potential conflict with ARAG or any ARAG employees. Third parties must not submit a bid/proposal/quote/recommendation to ARAG based on any agreement to impair competition and/or take advantage of any other illicit restraints of competition, including without limitation any third party agreements that restrain competition. Third parties must report any pending or impending proceedings under anti-trust law, competition law, pecuniary offences and current or pending competition breach disqualifications.

Third parties must ensure that no benefits in any form whatsoever have been or will be offered, promised or guaranteed to obtain a wrongful advantage from any other party connected with any negotiations, performance or agreements. In particular, third parties must ensure that no benefits in any form whatsoever have been or will be offered, promised or guaranteed to a domestic or foreign public officials or civil servants, persons particularly connected to public authorities, politicians, representatives of other public institutions in such a way that would cast doubt on their independence or integrity.

Third parties must comply with all applicable laws, statutes, regulations, and codes relating to anti-bribery and anti-corruption, including, but not limited to the Bribery Act 2010 ('**Anti-Bribery Requirements**'). In particular, third parties must not engage in any activity, practice or conduct that does constitute, or may be determined to constitute an offence under sections 1, 2 or 6 of the Bribery Act 2010.

Third parties must maintain, implement and (where appropriate) enforce their own policies and procedures that ensures compliance with the **Anti-Bribery Requirements**. In the event that a third party receives any request or demand for undue financial or other advantage of any kind, in the course of doing business with ARAG, it must promptly report this to ARAG.

A third party must promptly report to ARAG if it is subjected to any bribery or corruption investigation, or if it makes any corporate self-report to any authority worldwide in relation to bribery or corruption.

Third parties must ensure that no benefits in any form whatsoever have been or will be demanded, promised or accepted by the third party and no other criminal acts have been or will be committed that may be regarded as illicit activity, or active or passive bribery.

Third parties must:

- Take proactive steps to detect and prevent fraud.
- Have in place and keep up to date policies and procedures to prevent and detect fraud.
- Notify ARAG as soon as practicable if fraud or suspected fraud is detected, to the extent directly or indirectly relevant to the third party's relationship with ARAG.
- Allow ARAG to investigate any such instance of fraud or suspected fraud and proactively cooperate with such investigation.
- Provide further information on request from ARAG in relation to any such instance of fraud or suspected fraud and steps taken to address the same.

Third parties must exercise a zero-tolerance policy on corruption, bribery and fraud. A third party's violation of any of these obligations shall entitle ARAG to exclude the third party from tender processes (including subsequent tender processes for at least three years) and terminate any existing contract between ARAG and such third party with immediate effect, with such violation deemed to be a material breach of such contract entitling ARAG to terminate.

4. Adherence to the UN Global Compact

We adhere to the **UN Global Compact** initiative. This commits us to the protection of human rights, the prevention of forced labour and child labour, the protection of the environment and the combating of corruption. Accordingly, as a requirement for cooperation, ARAG expects its third parties to commit to uphold the principles of the **UN Global Compact**. Violation will be deemed to be a material breach entitling ARAG to terminate with immediate effect.

- **Principle 1:** Businesses should support and respect the protection of internationally proclaimed human rights;
- **Principle 2:** Make sure that they are not complicit in human rights abuses;
- **Principle 3:** Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining;
- **Principle 4:** The elimination of all forms of forced and compulsory labour;
- **Principle 5:** The effective abolition of child labour;
- **Principle 6:** The elimination of discrimination in respect of employment and occupation;
- **Principle 7:** Businesses should support a precautionary approach to environmental challenges;
- **Principle 8:** Undertake initiatives to promote greater environmental responsibility;
- **Principle 9:** Encourage the development and diffusion of environmentally friendly technologies; and
- **Principle 10:** Businesses should work against corruption in all its forms, including without limitation extortion and bribery.

Please see: www.unglobalcompact.org/what-is-gc/mission/principles for more information.

5. Compliance

Third parties shall not engage in any activity, practice or conduct which would constitute a UK or foreign tax evasion offence under section 45(1) and 46(1) of the Criminal Finances Act 2017.

Third parties must have and maintain policies and prevention procedures to prevent the facilitation of tax evasion that apply to all employees, workers and agents.

Third Parties must promptly report to ARAG any incident that constitutes, or may constitute, a request or demand to facilitate tax evasion.

Third Parties must comply with the Modern Slavery Act 2015, and all applicable laws, regulations codes of practice and guidance and must take all reasonable steps to avoid slavery or human trafficking in its business or supply chain.

Third parties must prepare and maintain (at no lesser standard than required under applicable law and expected under good industry practice) full and proper accounts and records which accurately present and reflect in all material respects all transactions and matters relating to the third party's dealings with ARAG.

6. Information Security

Third parties must treat information security (confidentiality, integrity and availability) as a critical business issue. ARAG expects all third parties to adopt and implement all appropriate security governance and administrative, physical, procedural and technical controls (as a minimum, in accordance with applicable law and good industry practice) to ensure such security and to detect, respond to and remedy any information security incident, including, without limitation:

- Providing properly configured malware protection on all electronic devices and mobile phones;
- Restricting unauthorised copying of information on any portable storage devices;
- Implementing secure log-on procedures on any devices used;
- Using encryption on information whenever appropriate;
- Testing and applying appropriate security patches to its systems, applications and software;
- Implementing physical security measures on sites and locations, such as building access controls, visitor management processes and premise surveillance;
- Protecting equipment from power failures;
- Implementing appropriate penetration testing to its systems;
- Performing regular security audits; and
- Enforcing a clear desk policy for papers and clear screen policy on devices.

Third parties must impose the same, or substantially similar security requirements and assurance processes to their own suppliers, having regard to the nature of the goods or services they provide.

Third parties must ensure that any information security incidents are responded to in a quick, effective and orderly manner. Third parties must promptly report to ARAG all potential and actual information security incidents that affect or may affect ARAG's data. ARAG expects any such report to identify all relevant information about the information security incident and the third party must provide ARAG with any further information that it reasonably requests.

ARAG requires all third parties to co-operate and work with it to agree an exit strategy that removes access rights and returns and/or destroys any ARAG data before the engagement with ARAG terminates.

Third parties must comply at all times with all applicable data protection and privacy laws.

7. Business Continuity and Disaster Recovery

Third parties must implement and maintain effective and up-to-date **Business Continuity and Disaster Recovery** plans (“**BCDR Plans**”) to ensure that they are able to manage events that adversely impact their ability to perform any services or obligations they owe to ARAG.

Third parties shall ensure that their **BCDR Plans** include provisions that adequately address the following scenarios, in accordance with good industry practice:

- Loss of access to workplace, building or site;
- Loss of people;
- Loss of suppliers;
- Loss of systems (e.g. IT networks, applications, infrastructure, data centres and telephony); and
- Loss of data (accidentally or deliberate corruption, theft, or encryption e.g. ransomware).

Third parties must regularly test (no less than once a year) that their **BCDR Plans** manage all appropriate and potential scenarios and that their strategies are in accordance with good industry practice. Third parties should conduct further tests of their **BCDR Plans** whenever there is a significant change to their operations.

In the event that a BCDR test reveals any material risks to the performance of services or obligations to ARAG, the third party must:

- Notify ARAG in writing;
- Provide ARAG with an action plan of how it will rectify the issue;
- Complete the action plan within a reasonable timeframe;
- Notify ARAG when the action plan has completed; and
- Provide a declaration that the issue(s) are rectified, at ARAG’s request.

8. Confidentiality

Third parties must keep confidential (and ensure that their professional and other advisers keep confidential) all confidential information that ARAG discloses to them, or that they otherwise obtain, develop or create in the course of their dealings with ARAG (“**ARAG’s Confidential Information**”).

Third parties must restrict disclosure of **ARAG’s Confidential Information** to their employees, workers or agents on a strictly need-to-know basis for the purpose of discharging their obligations to ARAG and shall impose the same or substantially similar confidentiality obligations such recipients.

Third parties must only use **ARAG’s Confidential Information** in connection with performance of their obligations to ARAG and must take all reasonable steps necessary to secure **ARAG’s Confidential Information** against theft, loss or unauthorised disclosure.

Third parties must impose the same or substantially similar confidentiality obligations in respect of **ARAG’s Confidential Information** to their own suppliers.

For the avoidance of doubt, the above confidentiality obligations do not apply if such information was already in the public domain, and/or is required to be disclosed by an applicable law or regulation in a jurisdiction of substantially similar repute as the United Kingdom.

In the event that there is a legitimate need to disclose **ARAG’s Confidential Information** to a third party to obtain professional advice (i.e. legal or financial), the disclosure of **ARAG’s Confidential Information** must:

- i) be minimised as much as is reasonably practicable; and
- ii) not be disclosed unless there is in place a substantially similar written agreement of confidentiality with the recipient party.

9. Sanctions

Third parties must:

- Conduct business in accordance with international economic and financial sanctions legislation, export controls, trade embargoes and any other restrictive measures from time to time imposed, administered or enforced by a regulator or other competent authority;
- Not by act or omission expose themselves or ARAG to any sanction, prohibition or restriction contrary to **Sanctions Targets** and/or any additional regulations, or breach or cause ARAG to breach any international economic, export control or financial sanctions rules set by a regulator, by ARAG or by any other competent authority; and
- Conduct on an ongoing basis appropriate screening and maintain systems and controls, procedures and training designed to prevent any violation of the preceding provisions of this section.

Sanctions Targets for the purpose of this section means those persons (whether regimes, entities and/or individuals) designated as being subject to financial sanctions in the United Kingdom, the European Union, the United States of America or any other territory local to either Party, including the HM Treasury's consolidated list, the OFSI consolidated list, the UN Security Council consolidated list, the Bundesanzeiger, the EU Financial Sanctions List, the Dow Jones list or by the Office of Foreign Assets Control (including both SDN and non SDN lists).