



Supplier Code of Conduct

Owner: Head of Compliance and CISO

Contents

HUMAN RIGHTS 3

BUSINESS ETHICS..... 3

COMPLIANCE AND REPORTING 4

ENVIRONMENTAL SUSTAINABILITY 5

HEALTH AND SAFETY 6

INFORMATION SECURITY AND DATA PRIVACY 6

INCIDENT MANAGEMENT 8

ARTIFICIAL INTELLIGENCE (AI) 8

COMMITMENT TO IMPROVEMENT 9

Supplier Code of Conduct

At RezolveAi PLC and its subsidiaries (collectively “RezolveAi”), we value integrity, ethical business practices, and respect for human rights and the environment. We expect our suppliers, business partners, affiliated companies, and approved subcontractors to uphold these principles and conduct business responsibly. This Supplier Code of Conduct outlines RezolveAi’s expectations regarding labor practices, environmental sustainability, business ethics, information security, data privacy, artificial intelligence, and compliance with applicable laws and regulations. Each subsidiary shall adopt this Code (or an equivalent standard) and mandate compliance with its provisions in all contracts entered into with its own suppliers, vendors, subcontractors, and business partners.

This Supplier Code of Conduct applies to all suppliers, vendors, contractors, consultants, agents, subcontractors, and other third parties that provide goods or services to RezolveAi or act on RezolveAi’s behalf. Suppliers are responsible for ensuring that their personnel, affiliates, and approved subcontractors understand and comply with this Code and with all applicable contractual obligations. At a minimum, all Suppliers must comply with applicable laws and regulations in the jurisdictions where they operate and cooperate with regulators responsible for enforcing those laws. Failure to comply with this Supplier Code of Conduct may result in remedial action, suspension, disqualification as an approved supplier, termination of contract, or exclusion from future business with RezolveAi.

HUMAN RIGHTS

We are committed to supporting the protection and advancement of human rights in our business and throughout our supply chain. We expect our suppliers to have appropriate policies and practices in place that apply to their employees and supply chains.

Fair Employment: Suppliers must offer fair wages, benefits, and working conditions to their employees, in line with relevant laws and regulations on working hours, minimum wage, overtime pay, harassment, and workplace safety.

Non-Discrimination: Suppliers must avoid discrimination based on race, color, religion, gender, age, disability, sexual orientation, or any other protected characteristic in their hiring and employment practices.

Forced Labor: Suppliers must not utilize forced labor or involuntary labor, including prison labor or human trafficking, within their operations or supply chain.

Child labor: Suppliers must not hire workers below the legal minimum age for employment according to local and international laws.

BUSINESS ETHICS

RezolveAi is committed to conducting business in accordance with high standards of ethics, integrity, and accountability, and expects the same from its suppliers and business partners. Ethical conduct is fundamental to our values and plays a vital role in building trust, fostering long-term relationships, and contributing positively to society and the environment. Our commitment extends beyond compliance with laws and regulations and includes promoting fairness, honesty, respect, and accountability in all business dealings.

Supplier Code of Conduct

Integrity: Suppliers must conduct business honestly, transparently, and with integrity. They must not engage in, facilitate, or tolerate bribery, corruption, fraud, money laundering, conflicts of interest, or other unethical practices in connection with their business dealings with RezolveAi.

Suppliers must maintain accurate books, records, invoices, reports, and other business documentation related to their work for RezolveAi. Suppliers must not falsify, conceal, or misrepresent any transaction, payment, expense, certification, or compliance record.

Conflict of Interest: Suppliers must not offer, provide, solicit, or accept gifts, entertainment, meals, travel, hospitality, or anything else of value that could improperly influence—or reasonably appear to influence—a business decision involving RezolveAi. Gifts and entertainment must be reasonable, infrequent, appropriate to the business relationship, and permitted under applicable law and RezolveAi policies. Cash and cash equivalents are strictly prohibited.

Confidentiality: Suppliers must respect the confidentiality of RezolveAi's information, assets, and intellectual property, ensuring they are protected from unauthorized disclosure or misuse by maintaining appropriate processes.

Privacy: Suppliers must respect individual privacy rights and comply with applicable data protection laws and regulations when handling personal data or sensitive information. In addition, personal data provided by or on behalf of RezolveAi must only be used, accessed, and disclosed as permitted by the Supplier agreement.

Suppliers must process personal data only in accordance with RezolveAi's documented instructions and applicable data protection agreements. Suppliers may not sell, share, reuse, or disclose RezolveAi personal data unless authorized by contract, and must maintain appropriate safeguards for cross-border transfers, onward transfers, retention, deletion, and return of personal data.

Trade and sanctions: Suppliers must adhere to all applicable trade laws, export control regulations, and economic sanctions imposed by relevant authorities in the jurisdictions where they operate or conduct business.

COMPLIANCE AND REPORTING

RezolveAi encourages suppliers to implement policies, procedures, and controls that support ethical conduct and compliance with this Supplier Code of Conduct. Any breach of the obligations contained in this Code may be considered a material breach of contract. RezolveAi expects suppliers and business partners to comply with applicable laws, regulations, contractual obligations, and ethical standards across all aspects of their operations. Failure to adhere to the standards and expectations outlined in this Code may result in contract termination or other remedial action deemed appropriate by RezolveAi.

Suppliers must maintain governance, policies, and internal controls reasonably designed to support compliance with this Code, applicable law, and contractual obligations. Upon request, suppliers must provide reasonable documentation or other evidence demonstrating compliance, including policies, risk assessments, training records, certifications, audit reports, or corrective action plans.

Compliance: Suppliers must comply with this Supplier Code of Conduct and any additional contractual requirements specified by RezolveAi PLC. Suppliers must disclose proposed subcontracting arrangements and obtain RezolveAi's prior written consent where required by contract. Suppliers remain responsible for ensuring that approved subcontractors comply with standards and security requirements equivalent to those applicable to the supplier, particularly where subcontractors may

Supplier Code of Conduct

access sensitive data, support critical operations, or otherwise affect RezolveAi's risk profile.

Monitoring and Evaluation: RezolveAi retains the right to monitor and evaluate supplier compliance with this Code of Conduct through audits, assessments, and other methods.

Business Continuity: Suppliers must develop and maintain a comprehensive business continuity plan that outlines procedures for responding to disruptions such as natural disasters, cyber-attacks, supply chain interruptions, and other emergencies. This plan should include measures for ensuring the continuity of critical operations, communication channels, data protection, and recovery strategies.

Communication: Suppliers must maintain open and transparent communication with RezolveAi regarding any potential risks or disruptions that may impact on their ability to fulfill contractual obligations.

Incident Reporting: Suppliers must report immediately, and no later than twenty-four (24) hours, any business continuity incidents or disruptions to RezolveAi and collaborate on recovery efforts as needed. Supplier must provide a formal written follow-up report within seventy-two (72) hours of the initial notification, detailing the nature, scope, and initial remediation steps taken. Thereafter, supplier must provide regular written progress updates at reasonable intervals, and upon request, until the incident is fully investigated, remediated, and closed.

Reporting Violations: Suppliers must promptly report any breaches of this Code of Conduct or any concerns regarding unethical or illegal behavior to RezolveAi for investigation and resolution.

Whistleblowing: Concerns may be raised anonymously through the Rezolve Group Whistleblowing Portal at <https://rezolve.ethicspoint.com/>.

RezolveAi prohibits retaliation against any person who, in good faith, reports a concern, cooperates in an investigation, or seeks guidance regarding this Code. Suppliers must maintain reporting channels that allow workers and other relevant stakeholders to raise concerns without fear of retaliation.

ENVIRONMENTAL SUSTAINABILITY

RezolveAi endeavors to manage and leverage our resources in a way that promotes a healthy and sustainable environment. We encourage suppliers to implement policies and measures that aim to reduce the environmental impact of their operations.

Compliance: Suppliers must adhere to all applicable environmental laws, regulations and standards in the regions where they operate.

Pollution Prevention: Suppliers must take steps to prevent air, water, and land pollution, including proper waste management and disposal practices.

Conservation of Resources: Suppliers should work towards minimizing their environmental footprint by conserving natural resources, reducing waste, and promoting energy efficiency.

HEALTH AND SAFETY

Suppliers are mandated to prioritize and secure the health, safety, and welfare of their workers and visitors. This responsibility extends to protecting the public from any health and safety risks associated with the suppliers' operations. To achieve this, suppliers must strictly adhere to all relevant laws and regulations applicable to their industry and operational activities. This includes:

Regular Training: Providing ongoing and systematic training programs that equip workers with up-to-date knowledge and skills to perform their duties safely. Training should cover general safety protocols as well as job-specific hazards, including emergency procedures, the proper use of equipment, handling of hazardous materials, and any other relevant safety measure.

Clear Communication: Maintaining open lines of communication where safety information is clearly conveyed and easily accessible. This could include signage, manuals, digital platforms, and regular safety meetings.

Evaluation and Feedback: Implementing processes to regularly evaluate the effectiveness of the training programs and incorporating feedback from workers to continuously improve safety practices.

Safety Culture: Fostering a workplace culture that prioritizes safety, where workers feel responsible for not only their own safety but also the safety of their colleagues and visitors. By embedding these practices, suppliers can ensure a safer working environment, mitigate risks, and comply with legal standards, thereby promoting the well-being of all individuals associated with their operations.

INFORMATION SECURITY AND DATA PRIVACY

The security of our intellectual property, information and systems is critical to our commercial success. We therefore need our suppliers to respect and safeguard our information by complying with applicable laws and regulations, having appropriate processes and governance in place and working with us to identify and mitigate risks.

Privacy and Data Protection Suppliers must comply with local privacy and data protection laws to respect and protect the privacy and personal data of all individuals relevant to RezolveAi. Suppliers must also comply with the requirements set out in all data processing agreements.

ResolveAi must be notified immediately, and no later than twenty-four (24) hours after becoming aware, of any data incidents or suspected breaches, or anything affecting the confidentiality, integrity or availability of personal information (e.g. unlawful destruction, loss, alteration, unauthorized disclosure or access).

These notifications should be sent to **DPM@rezolve.com** and should be prior to any notification to any government regulator to enable RezolveAi to undertake any remedial work or prepare notifications as may be required by the law.

Supplier Code of Conduct

Within 72 hours of becoming aware of the incident or breach, supplier must submit a comprehensive written follow-up report to RezolveAi. A security or data incident notice must include, to the extent known at the time of notification, a description of the incident, the systems and data affected, the categories and approximate volume of data involved, the date and time the incident was discovered, containment steps taken, anticipated remediation actions, and a primary contact for coordination with RezolveAi.

Following the 72-hour report, supplier must provide regular written progress updates at reasonable intervals, and upon request, until the incident is fully investigated, remediated, and closed.

Intellectual Property Suppliers must safeguard our confidential information, trade secrets and intellectual property (including copyrights, trademarks and patents) from unauthorized access and misuse.

Information Security Suppliers must maintain and apply best practice security to safeguard our data, confidential information, trade secrets and intellectual property, along with the integrity and availability of the products or services being provided. These controls and measures will be subject to regular review as part of RezolveAi's supplier due diligence process. Suppliers must:

Safeguard the security and privacy of their systems and our data throughout their entire supply chain;

Have appropriate technical and organizational measures in place to meet our information security and privacy requirements and standards. These may include:

Appropriate access controls in place to prevent unauthorized access to physical locations, systems, and applications used to process RezolveAi information;

A suite of information security policies and procedures that have been tailored to reflect the security nuances of the supplier's environment and are regularly communicated to all internal stakeholders;

An information security risk management framework (or similar) that facilitates the identification, analysis, evaluation, treatment, and reporting of information security risks;

An information security and data privacy training programme (or similar) that applies to both new hires during induction and existing employees on at least an annual basis thereafter;

Appropriate logging and monitoring controls in place to detect any abnormal or malicious activity on any systems and applications used to process RezolveAi information;

Appropriate incident management processes and controls in place that facilitate the identification, reporting, containment, eradication, and recovery from information security incidents that may directly or indirectly impact RezolveAi;

- Appropriate business continuity and contingency processes and controls in place to ensure that any services provided to RezolveAi can continue to operate, where possible, during any

Supplier Code of Conduct

significant business disruptions within the supplier's environment;

- Appropriate compliance controls that facilitate the security and protection of any personal data processed by the supplier belonging to RezolveAi;
- Appropriate supply chain security controls which apply to the entire lifecycle of a supplier (procurement, onboarding, ongoing monitoring and review, offboarding);
- Appropriate software development controls in place to reduce security vulnerabilities within development environments, and to ensure that all code is developed and handled in a secure manner.

The required level of security controls a supplier will need to have in place will depend upon a number of factors, including:

- The type of services provided by the supplier.
- What level of access does the supplier has to RezolveAi information.
- The overall level of risk posed by the supplier; and
- The criticality score assigned to the supplier as per our internal processes.

Suppliers that access, process, store, transmit, or support RezolveAi systems or data must maintain security controls appropriate to the sensitivity of the information and the criticality of the services provided. These controls should include, as applicable, multi-factor authentication, timely vulnerability management and patching, endpoint protection, encryption, secure configuration management, privileged access controls, logging and monitoring, backup and recovery safeguards, and secure software development practices.

INCIDENT MANAGEMENT

Suppliers must take steps to reduce the risk of an information security incident. Suppliers must ensure that their own information security arrangements and those within their supply chain are appropriate to the requirements of the information assets concerned, and any contractual obligations to RezolveAi. This must include appropriate governance and risk management processes, ensuring access to data is maintained on a need-to-know, least privileged basis and that processes are in place to respond effectively to any incidents. Suppliers should inform us if they have become aware of any cyber security incident that could or has compromised our data or services.

Suppliers must cooperate fully with us in any investigation, conduct root cause analysis and follow up actions where required.

ARTIFICIAL INTELLIGENCE (AI)

Where AI forms any part of the services suppliers are delivering to RezolveAi, suppliers must be transparent about this and tell us at the earliest opportunity. AI must not be introduced into live services (any services actively used in production – APIs and integration, payments, product systems,

Supplier Code of Conduct

managed services, etc.) without the prior written consent of designated due diligence partners at RezolveAi. Should any AI related problems arise, suppliers must inform RezolveAi promptly.

Suppliers using AI in connection with RezolveAi services must implement governance controls appropriate to the use case, including oversight, testing, monitoring, documentation, security review, privacy review, and controls designed to prevent unauthorized use of RezolveAi data. Suppliers must disclose and maintain a list of all underlying model providers and AI sub-processors used to support RezolveAi services, and be able to explain the purpose, limitations, data inputs, outputs, and material risks of any AI functionality used to support RezolveAi services.

Suppliers must use AI responsibly and within the law. Suppliers should ensure their use of AI avoids any unlawful discrimination or bias and adheres to all data privacy and equality law obligations and aligns to relevant standards and guidance, including ISO 42001

Suppliers must not use RezolveAi data (including confidential information, personal data, or proprietary assets) as input data, prompt entries in public or third-party AI tools (such as ChatGPT, public LLMs, or consumer generative AI platforms), or use it to train an AI solution without our prior written consent. Any AI usage must respect RezolveAi’s Intellectual Property rights.

COMMITMENT TO IMPROVEMENT

RezolveAi encourages ongoing enhancement of supplier practices related to labor, ethics, and the environment. We value open communication and collaboration with our suppliers to tackle challenges, implement best practices, and promote responsible business conduct throughout our supply chain. By adhering to this Supplier Code of Conduct, suppliers demonstrate their dedication to shared values of integrity, responsibility, and sustainability, making a positive impact on the communities and environments where we operate.

Acknowledgement

Name: _____

Job Title: _____

Date: _____

Approval log:

Ver	Approver	Approval Date
1	ERMC	Oct 6, 2021
2	ERMC	Nov 26, 2024
3.	CISO and Compliance	Sep 2026

