



Resolve.ai

**Report on the current state of readiness for compliance with
General Data Protection Regulation (GDPR)**

PREPARED BY



Report Date: 27th April 2026

Rezolve.ai
EU GDPR Compliance Report

27th April 2026

To,
Saurabh Kumar
Rezolve.ai
11501 Dublin Blvd
Suite 200, Dublin
CA 94568, USA

Data Privacy Compliance Letter

Scope

Riskpro India was engaged to perform a compliance Reaudit against GDPR requirements applicable to the company's processes engaged in handling personal data. The purpose of this report is to provide a high-level overview of the existing compliance status of the company's operational and support processes as well as identify areas that need improvement.

Review Methodology

- Discussions and interviews with the management
- Inspection of documents, policies, and a quick glance through for the level of content
- Walkthrough of platform, processes, and systems

Summary Findings:

- Rezolve.ai has established a comprehensive Management Framework, including Privacy by design and Privacy by default principles, to carry out its business with its customers.
- Rezolve.ai has the necessary technical and organizational measures/ information security controls in place appropriate to the size and operations of the company. The implemented controls should be effectively applied for GDPR Compliance.
- Detailed records of processing and data inventory are in place. Documented all the relevant Policies and Procedures, including the Data Privacy Policy and Framework.
- A Privacy Officer is appointed to assume the role of Data Privacy Officer to handle the Privacy Program as well as all queries concerning Privacy.

Rezolve.ai
EU GDPR Compliance Report

- Privacy Incident Management is in place to enable Rezolve.ai to assess and respond to Privacy Incidents on priority, to mitigate potential harm to affected individuals, and to comply with applicable laws and regulations.


Scope Limitation

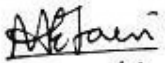
Our GDPR compliance review engagement was limited to evaluating the existence of key processes, privacy framework, and necessary artefacts for the following website and related processes.

- Rezolve.ai (<https://www.rezolve.ai/>)

Riskpro India is not liable for any incomplete or inaccurate information provided to us or for any financial or non-financial loss as a result of our engagement and this report.

Conclusion on GDPR Compliance

	Based on our review, we believe that the company's application and processes engaged in handling personal data are "GDPR Compliant"
---	--



Manoj K. Jain Director

Disclaimer: This report is intended only for information purposes and should not be considered an absolute audit report. This Report does not constitute legal advice, regulatory advice, or a certification of compliance with any data protection law. Compliance obligations remain the sole responsibility of the Client. It is merely an independent review and reporting of our findings to provide assurance to end clients about the GDPR readiness of our clients. Any mechanisms relating to international data transfers are subject to evolving regulatory requirements and require ongoing, independent legal validation; accordingly, such validation is outside the scope of this engagement. The findings and recommendations in this Report are based on information, documents, representations, and explanations provided by the Client and its personnel, and no independent verification beyond the agreed scope has been undertaken.

Rezolve.ai
EU GDPR Compliance Report

Annexure: Compliance status against EU GDPR requirements

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
1	Accountability and Governance:			
1.1.1	Decision-makers and key people in the company are aware of the Data Privacy requirements and its accountability requirement.	Compliant	<p>1. Rezolve.ai team POC informed that key people and decision-makers in the company are aware of the data privacy requirement through defined governance structures, policy ownership, and management reviews under the ISMS framework.</p> <p>2. Rezolve.ai Team takes the training for the Senior Management and Staff to make them aware of the privacy and accountability requirements. Training completion and compliance are centrally tracked through Vanta</p> <p>Rezolve.ai Team has agreed to take the regular data privacy training for the employees and senior management.</p> <p>Evidence Verified: - MRM Decks</p>	NA
1.1.2	The company has implemented adequate privacy reporting to the Board and Senior Management of the Quarterly meetings_discussions etc. that are held.	Compliant	<p>1. Rezolve.ai POC informed that Privacy and data protection risks are reported to senior management as part of periodic risk reviews and governance discussions.</p> <p>Evidence Verified: - MRM Decks</p>	NA
1.1.3	The requirement to appoint Data Protection Officer (DPO) is identified. DPO has been appointed (as required).	Does Not Apply	<p>1. Rezolve.ai does not have an obligation to appoint a Data Protection Officer as:</p> <ul style="list-style-type: none"> - Rezolve.ai is not a public authority - Core business activities of Rezolve.ai do not require large-scale, regular, and systematic monitoring of individuals, such as online behaviour tracking, etc. - Core business activities of Rezolve.ai do not require large-scale processing 	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			<p>of special categories of data or data relating to criminal convictions and offences.</p> <p>However, Rezolve.ai has identified a staff member with the roles and responsibilities of a DPO to discharge Rezolve.ai's obligations under the GDPR.</p>	
1.1.4	If a DPO appointment is not mandated by the regulation, a privacy officer is identified or appointed to assume the role of Data Privacy.	Compliant	<p>1. Rezolve.ai has identified and appointed Mr Saurabh Kumar as a Privacy Officer to assume the role of Data Privacy.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Roles & Responsibilities, Version 8 - Privacy Notice at 	NA
1.1.5	Data Protection Officer (DPO) is registered with Supervisory Authority (SA).	Does Not Apply	<p>1. Rezolve.ai does not have an obligation to appoint a Data Protection Officer.</p> <p>However, as the business expands in the future, if Rezolve.ai processes a large amount of data of EU individuals, then it needs to register the DPO with the Supervisory Authority.</p> <p>Hence, this control is not applicable.</p>	NA
1.1.6	Privacy Roles and Responsibilities are defined and documented.	Compliant	<p>1. Privacy roles and responsibilities are defined and documented within Rezolve.ai's policies and governance framework.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Data Protection Policy and Framework, Version 8 - Roles and Responsibilities, Version 8 	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
1.1.7	The organization's DPO business contact information is made available to the public.	Compliant	<p>1. Rezolve.ai has a process to connect with the Privacy Officer and to ask queries and complaints related to personal data protection in its privacy notice.</p> <p>Evidence Verified: - Email Screenshot</p>	NA
1.1.8	The Privacy Office tracks and analyses the impact of new laws, changes in laws, relevant enforcement actions and new regulatory expectations.	Compliant	<p>1. Rezolve.ai tracks and analyses the impact of new laws, changes in laws, relevant enforcement actions, and new regulatory expectations by subscribing to newsletters/blogs, tracking/monitoring websites of Governing Agencies and Regulatory Bodies or attending privacy conferences.</p> <p>Evidence Verified: - One trust - https://www.onetrust.com/resources/digital-privacy-experience-newsletter/ - ICO - https://ico.org.uk/about-the-ico/media-centre/e-newsletter/</p>	NA
1.1.9	The company has developed a procedure for Risk Assessment	Compliant	<p>1. Rezolve.ai has defined and documented Risk Assessment Procedures. It includes the requirement to conduct a privacy risk assessment in the Review of Risk Profile section.</p> <p>2. Rezolve.ai has defined and documented a Risk Register.</p> <p>Evidence Verified: - Risk Management Policy, Version 9 - Risk Register including privacy risks</p>	NA
1.1.10	Company's risk assessment covers privacy related risks.	Compliant	<p>1. Rezolve.ai has defined and documented Risk Assessment Procedures. It includes the requirement to conduct a privacy risk assessment in the Review of risk profile section.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	<p>2. Rezolve.ai has defined and documented a Risk Register.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Risk Management Policy, Version 9 - Risk Register including privacy risks 	
1.1.11	Privacy Risk Assessment is done at least half yearly _ annually	Compliant	<p>1. Rezolve.ai has defined and documented Risk Assessment Procedures. It includes the requirement to conduct a privacy risk assessment at least once annually and reviewed through management governance forums.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Risk Management Policy, Version 9 	NA
1.1.12	The company has developed procedures for Internal Audit and privacy self-assessment.	Compliant	<p>1. Rezolve.ai has defined and documented the data protection (privacy) policy that includes the requirements of conducting privacy audits annually. Controls are reviewed quarterly.</p> <p>2. Rezolve.ai has a GDPR Assessment Checklist to conduct the assessment at regular intervals.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Data Protection Policy and Framework, Version 8 - Rezolve.ai GDPR Assessment Report, 25Feb2026 	NA
1.1.13	Internal Audits of the privacy self-assessments are conducted at least annually.	Compliant	<p>1. Rezolve.ai has defined and documented the data protection (privacy) policy that includes the requirements of conducting privacy audits regularly, as stated in the Self-Assessment paragraph (7th Section) of the policy.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Data Protection Policy and Framework, Version 8 	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
1.1.14	The company provides security and privacy awareness training to the employees at the time of induction and refresher training at a regular interval.	Compliant	<p>1. Data Privacy Awareness Training Rezolve.ai maintains mandatory data protection and privacy training for all employees. Training covers GDPR principles, secure handling of personal data, incident reporting, and employee responsibilities under our data protection policies. Completion is required at onboarding and annually thereafter, as stated in the Training paragraph (7th Section) of the Data Protection Policy.</p> <p>2. Information Security Training All employees undergo mandatory information security awareness training, including secure access practices, phishing awareness, data classification, and incident escalation procedures. Refresher training is conducted regularly to reinforce compliance.</p> <p>3. Attendance Records Training completion and compliance are centrally tracked through Vanta. Participation is mandatory for all employees, and auditor access to training records can be provided through controlled Vanta access to support audit requirements.</p> <p>Rezolve.ai agrees to maintain documented evidence as an Attendance List of the trainees and furnish the same evidence upon request.</p> <p>Evidence Verified: - Evidence verified over the call - Data Protection policy Version 08</p>	NA
1.1.15	Employees and contractors acknowledge the Code of Conduct.	Compliant	<p>1. All employees and contractors of Rezolve.ai acknowledge the Code of Conduct.</p> <p>2. Rezolve.ai Code of Conduct include Privacy Clauses in its Data Privacy section.</p> <p>3. Rezolve.ai POC has informed that this is the updated code of conduct, which each new joiner will be signing.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	<p>Evidence Verified: - Code of Conduct V8</p>	
1.1.16	All new employees have to read and sign the Confidentiality Agreement upon joining.	Compliant	<p>1. Rezolve.ai POC informed that all new employees sign confidentiality agreements/NDA upon joining.</p> <p>Evidence Verified: - NDA</p>	NA
1.1.17	The company (not based in European Union) has appointed in writing a representative in the European Union.	Does Not Apply	<p>1. Rezolve.ai currently does not operate in the European Union, requiring an EU representative.</p> <p>Hence, this control is not applicable.</p>	NA
1.1.18	Company (working as a joint controller) documents the respective roles and relationships of the joint controllers.	Does Not Apply	<p>1. Rezolve.ai does not work as a joint controller.</p> <p>Hence, this is not applicable.</p>	NA
1.1.19	Company (working as a joint controller) makes available the details of the arrangement to the individuals.	Does Not Apply	<p>1. Rezolve.ai does not work as a joint controller.</p> <p>Hence, this is not applicable.</p>	NA
1.1.20	Company has Information security related policies and procedures that describes information security processes, practices and organization.	Compliant	<p>1. Rezolve.ai team has defined and documented the Information Security Policy, and it defines information security processes, practices, and organization.</p> <p>Evidence Verified: - ISMS Manual, Version 8.0</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
1.1.21	Information Security Policy & Procedures are reviewed and approved by the Management at least annually.	Compliant	<p>1. Rezolve.ai team has defined and documented the Information Security Policy, which defines information security processes, practices, and organization.</p> <p>2. The IT policy is reviewed at least once a year.</p> <p>Evidence Verified: - ISMS Manual, Version 8.0</p>	NA
2	Data Privacy Framework:			
2.1.1	The company has established and documented purposes for processing personal data.	Compliant	<p>1. Rezolve.ai has established and documented the purposes for processing personal data within its Data Inventory. Considering the organization's employee strength (up to 200 employees), maintaining a Data Inventory has been adopted as an appropriate and proportionate approach to record and manage personal data processing activities, in line with applicable data protection requirements.</p> <p>2. Rezolve.ai publishes a Privacy Notice on the website.</p> <p>Evidence Verified: - Rezolve.ai Data Inventory, Version 1 - Website privacy policy https://www.rezolve.ai/legal/privacy-policy-20260323-v2-2</p>	NA
2.1.2	<p>The Company limits the collection of personal information to the minimum necessary to provide the service. Input templates are defined which are used for data collection.</p> <p>Client organizations are responsible for providing only</p>	Compliant	<p>1. Rezolve.ai has its respective sources for data collection and collects the data according to the team's needs and use as per the service provided.</p> <p>2. Rezolve.ai has established and documented the purposes for processing personal data within its Data Inventory. Considering the organization's employee strength (up to 200 employees), maintaining a Data Inventory has been adopted as an appropriate and proportionate approach to record and manage personal data processing activities, in line with applicable data protection requirements.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	the information that is necessary.		Evidence Verified: - Rezolve.ai Data Inventory, Version 1	
2.1.3	The company has developed and implemented procedures and/or mechanisms to verify that the personal data processed is complete, accurate, not misleading, and updated.	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai HR team collects data of job seekers from the Naukri portal, LinkedIn or through referral, where data is directly provided by job seekers. 2. The employees directly provide the data to the HR and Finance Team; therefore, the data is considered to be accurate. 3. Rezolve.ai marketing Team collects the data of Prospective Business Leads through subscription-based third-party lead generation platforms - ZoomInfo, Google Ads, LinkedIn and Clay. 4. Rezolve.ai also collects lead information through its website interfaces, including Book Demo, Get Quote, Contact Us, and Book a Discovery Call forms. Since this data is directly provided by leads or prospects, it is considered accurate. 5. Rezolve.ai's engineering team collects data of tenants at the time of registration. These details are provided by customers themselves; hence, it is considered to be true. 6. Rezolve.ai collects queries directly from customers and end-users about the Privacy Policy. 	NA
2.1.4	The company undertakes periodic reviews to determine whether it is necessary to retain the personal data in its possession.	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai has documented the Retention and Disposal Policy. 2. Rezolve.ai periodically reviews personal data retention in line with documented retention schedules to ensure data is not retained longer than necessary. Evidence Verified: - Data Retention Policy, Version 8 - Data Retention Schedule	NA
2.1.5	The company has developed and implemented mechanisms	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai HR team POC confirmed that they process data of Indian employees. 	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	to notify any other individual or entity, with whom personal data has been shared if the personal data is not complete, inaccurate, is misleading, and not updated.		Rezolve.ai Team agrees to notify any other individual or entity, with whom EU individual personal data has been shared, if the personal data is not complete, inaccurate, misleading, or not updated. Also, the Rezolve.ai Team agrees to maintain documented evidence and furnish the same evidence upon request	
2.1.6	The company ensures that the personal data of individuals collected from a third-party source is accurate and complete.	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai POC from the HR Team informed that the Company processes the data of Indian employees. 2. Rezolve.ai POC from the HR Team informed that they collect the CVs of candidates from Naukri.com and LinkedIn. The CVs, which contain personal data, are directly provided by the candidates, and hence, the data is accurate. 3. Rezolve.ai POC from the marketing team informed that they collect leads/prospects data from subscription based third party platform like ZoomInfo, Google Ads, LinkedIn and Clay. Hence, it is considered to be accurate. 4. Rezolve.ai collects leads/prospects data from website forms like contact us, get a quote, book a discovery call and book a demo. This data is directly provided by leads/prospects. Hence, it is considered to be accurate. 	NA
3	Policies and Procedures			
3.1.1	The company has developed and implemented policies and procedures for data retention and data disposal.	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai has developed and implemented documented policies and procedures governing data retention and secure disposal of personal data in line with legal, contractual, and business requirements. <p>Evidence Verified: - Data Retention Policy, Version 8</p>	NA
3.1.2	The company has developed and implemented policies and	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai has defined and documented the Data Breach Policy and supporting documents. 	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	procedures for managing Data Breaches.		<p>Evidence Verified: - Data Breach Policy and Procedures, Version 8</p>	
3.1.3	The company has developed procedure and supporting templates for Data Protection Impact Assessment (DPIA)	Compliant	<p>1. Rezolve.ai has defined and documented the Data Protection Impact Assessment (DPIA) Policy. 2. Rezolve.ai does not currently conduct DPIAs as its existing processing activities do not involve high-risk personal data processing.</p> <p>However, the organization has documented procedure and will conduct DPIAs whenever future processing activities require such assessment.</p> <p>Evidence Verified: - Data Protection Impact Assessment policy, Version 8</p>	NA
3.1.4	<p>The company has developed and implemented procedures for security and data privacy assessments for Third Parties.</p> <p>Annual third-party due diligence _assessments are performed for critical vendors.</p>	Compliant	<p>1. Rezolve.ai has documented the Vendor Privacy Assessment Policy. 2. Rezolve.ai performs security and privacy due diligence through existing security and compliance frameworks. They do not maintain a formal vendor Due diligence report.</p> <p>Evidence Verified: - Third Party Vendor-Privacy Assessment, Version 8</p>	NA
3.1.5	Cross Border Transfer Policies Procedures are in place	Compliant	<p>1. Rezolve.ai has implemented policies and procedures governing cross-border transfers of personal data, including the use of appropriate safeguards where applicable.</p> <p>Evidence Verified: - Cross-border processing or transfers of personal data, Version 8</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	<ul style="list-style-type: none"> - TIA_India_Rezolve.ai - TIA_USA_Rezolve.ai 	
3.1.6	<p>The Company has code of conduct within the Employee Handbook that establishes standards and guidelines for personnel ethical behaviour. These include security and privacy clauses.</p> <p>Personnel are required to read and accept the entity's code of conduct</p>	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai maintains a Code of Conduct that includes security and privacy obligations. All personnel are required to review and acknowledge the Code of Conduct. 2. Privacy Clause included in the Data Privacy section of the Code of Conduct. 3. Rezolve.ai POC has informed that this is the updated code of conduct, which each new joiner will sign. <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Code of Conduct V8 	NA
3.1.7	<p>The data protection (privacy) policy is in place and updated within the last 12 months.</p>	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai has defined and documented the data protection (privacy) policy. <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Data Protection Policy and Framework, Version 8 	NA
3.1.8	<p>A documented and implemented privacy complaint handling process is in place, and the company has policies and practices to respond to queries and complaints related to personal data protection.</p>	Compliant	<ol style="list-style-type: none"> 1. Rezolve.ai has implemented a documented process to receive, assess, and respond to privacy-related queries and complaints, including those relating to personal data protection and data subject rights. Privacy-related communications are managed through designated contact channels and handled in accordance with defined procedures and GDPR timelines, with appropriate escalation where required. 2. A data subject can raise queries at <ul style="list-style-type: none"> - Email ID: saurabh@rezolve.ai - Phone: 001-833-5228466 - Address: 11501 Dublin Blvd STE 200, Dublin, CA 94568 3. RiskPro team has verified an email from Rezolve.ai's team to resolve the 	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			<p>queries related to data privacy. Rezolve.ai Team agrees to maintain documented evidence and furnish the same evidence upon request.</p> <p>Evidence Verified: - Grievance Handling Policy, Version 8 - Email Screenshot</p>	
4	Data Protection Implementation:			
	Data Inventory and Records of Processing:			
4.1.1	The company has identified and documented the personal data necessary for the identified purposes.	Compliant	<p>1. Rezolve.ai has identified and documented categories of personal data processed for defined business purposes. 2. A data inventory is maintained to record data types, purposes, and ownership to support GDPR accountability requirements.</p> <p>Evidence Verified: - Rezolve.ai Data Inventory, Version 1</p>	NA
4.1.2	The company has maintained a list of locations where personal data is stored, backed up including cloud infrastructure.	Compliant	<p>1. Rezolve.ai maintains an inventory of systems and locations where personal data is stored or processed, including cloud infrastructure and backup environments, to support security and data governance controls.</p> <p>Evidence Verified: - Rezolve.ai Data Inventory, Version 1</p>	NA
4.1.3	The company has identified the requirement of maintaining record of processing activities document.	Compliant	<p>1. Rezolve.ai has established and documented the purposes for processing personal data within its Data Inventory. Considering the organization's employee strength (up to 200 employees), maintaining a Data Inventory has been adopted as an appropriate and proportionate approach to record</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	and manage personal data processing activities, in line with applicable data protection requirements. Evidence Verified: - Rezolve.ai Data Inventory, Version 1	
4.1.4	The company maintains data inventory/record of processing activities document.	Compliant	1. Rezolve.ai maintains a data inventory document. Evidence Verified: - Rezolve.ai Data Inventory, Version 1	NA
	Data Protection Compliant Products and Services:			
4.2.1	On the applications and websites that shouldn't be accessible to children, Age-Gating is implemented on the sign-up page.	Does Not Apply	1. Rezolve.ai does not provide any products or services on any of the applications or websites that should not be accessible to children. Hence, age gating need not be implemented on the signup page.	NA
4.2.2	The company has developed and implemented procedures and/or mechanisms for verifying the age of a child.	Does Not Apply	1. Rezolve.ai does not provide any products or services on any of the applications and websites to children. Hence, this control does not apply.	NA
	Privacy by Design:			
4.3.1	The entity has implemented privacy by design and default whereby least privileges are set and controls relating to privacy setting are provided to the end users.	Compliant	1. Rezolve.ai applies privacy by design and default principles through role-based access controls, least-privilege configurations, and secure development practices. Privacy considerations are embedded throughout the system development lifecycle. 2. Rezolve.ai has defined and documented the Access Control Policy. Evidence Verified:	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			- Access Control Policy, Version 8 - Privacy by Design & Default v1, Version 1	
	Privacy Notice:			
4.4.1	The Company reviews Privacy Notice annually.	Compliant	<p>1. Rezolve.ai published Privacy Notices on their website. 2. Rezolve.ai reviews its Privacy Notice periodically annually and updates it as required to reflect changes in processing activities or regulatory expectations. 3. Rezolve.ai last updated its Privacy Policy on 23 March 2026.</p> <p>Evidence Verified: - Privacy Notice https://www.rezolve.ai/legal/privacy-policy-20260323-v2-2</p>	NA
4.4.2	The Privacy notice is published at all the collection points including company's website with information about choice available to data subjects and contains all the details mentioned in the act.	Compliant	<p>1. Rezolve.ai publishes its Privacy Notice on its website and ensures it includes required disclosures, data subject rights, and choices available to individuals in accordance with GDPR. 2. Rezolve.ai reviews and updates the privacy notice as per GDPR requirements 3. Data Collection points are as follows - Get Quote: https://www.rezolve.ai/get-quote - View Demo: https://www.rezolve.ai/discover-rezolve/personalized-demo - Book a discovery call: https://www.rezolve.ai/get-a-demo - Contact Us: https://www.rezolve.ai/contact-us</p> <p>Evidence Verified: - Rezolve.ai Privacy Notice https://www.rezolve.ai/legal/privacy-policy-20260323-v2-2</p>	NA
4.4.3	The company displays the cookie policy on their website	Compliant	1. Rezolve.ai displays a Cookie Policy on its website describing the use of cookies and similar technologies.	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			Evidence Verified: - Rezolve.ai Cookie Policy https://www.rezolve.ai/cookie-policy	
4.4.4	The company displays the cookie banner on the website. The cookie banner provides information about the cookies set on the website. The cookie banner requests consent from website visitors for setting non-essential cookies. (i.e. analytics, marketing). The consent is recorded.	Compliant	1. Rezolve.ai team showed over the call that cookie consent is captured and stored by HubSpot, not maintained internally by Rezolve.ai. 2. Rezolve.ai uses HubSpot to display a cookie banner that informs users about cookie usage and captures consent for non-essential cookies. 3. Consent preferences are managed at the browser level and not stored internally. While this ensures transparency and user control, detailed, auditable consent records are not maintained. Evidence Verified: - Email screenshot - Cookie Banner	NA
	Data Protection Impact Assessment (DPIA):			
4.5.1	Data Protection Impact Assessment (DPIA) is conducted for new projects and changes to existing programs, systems, or processes that handle personal data as specified by Authority.	Compliant	1. Rezolve.ai does not currently conduct DPIAs as its existing processing activities do not involve high-risk personal data processing. However, the organization has documented Policy and Procedures in place and will conduct DPIAs whenever future processing activities require such assessment 2. Rezolve.ai has defined and documented the Data Protection Impact Assessment (DPIA) Policy. Evidence Verified: - Data Protection Impact Assessment Policy, Version 8	NA
4.5.2	Data protection issues risks identified during PIAs_DPIAs are tracked and addressed.	Compliant	1. - Rezolve.ai does not currently conduct DPIAs as its existing processing activities do not involve high-risk personal data processing. However, the organization has documented Policy and Procedures in place and will	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	<p>conduct DPIAs whenever future processing activities require such assessment</p> <p>2. Rezolve.ai has defined and documented the Data Protection Impact Assessment (DPIA) Policy.</p> <p>Evidence Verified: - Data Protection Impact Assessment, Version 8</p>	
4.5.3	The company consults the supervisory authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the company to mitigate the risk.	Compliant	<p>1. Rezolve.ai does not currently conduct DPIAs as its existing processing activities do not involve high-risk personal data processing. However, the organization has documented Policy and Procedures in place and will conduct DPIAs whenever future processing activities require such assessment</p> <p>2. Rezolve.ai has defined and documented the Data Protection Impact Assessment (DPIA) Policy.</p> <p>Evidence Verified: - Data Protection Impact Assessment, Version 8</p>	NA
	Data Breach:			
4.6.1	The company has developed an Incident Response Plan.	Compliant	<p>1. Rezolve.ai maintains a documented Incident Response Plan covering detection, assessment, containment, and response to security and data breach incidents.</p> <p>Evidence Verified: - Incident Management Policy, Version 8 - Incident Response Plan</p>	NA
4.6.2	Incidents of breach are notified to the Supervisory Authority (SA) and or the Controller	Compliant	<p>1. Rezolve.ai has defined and documented the Data Breach Policy along with supporting documents to establish a structured process for managing personal data breach incidents.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			<p>2. Rezolve.ai has documented that personal data breach incidents will be reported to the Supervisory Authority and or the Controller, as applicable and required.</p> <p>Evidence Verified: - Data Breach Policy and Procedures, Version 8</p>	
5	Lawful Basis:			
	Grounds of Processing the Data (Lawful Basis):			
5.1.1	The company has identified and documented grounds for processing personal data for specific, stated purposes	Compliant	<p>1. Rezolve.ai HR team and Finance Team have the performance of a contract and legal obligation as a ground for processing the personal data of employees.</p> <p>2. Rezolve.ai HR team has consent as a ground for processing the personal data of Job seekers.</p> <p>3. Rezolve.ai Marketing Team has consent as a ground for processing the personal data for connecting the leads/prospects or the customers through the Contact Us form, get a quote, book a discovery call and book a demo tab on the website.</p> <p>4. Rezolve.ai Team has the performance of a contract as a ground for processing the personal data of vendors and customers/clients.</p> <p>5. Rezolve.ai HR Team has a performance of contract as a ground for processing of fingerprint impression data of the employees.</p> <p>6. Rezolve.ai Team has the performance of the contract as a ground for processing the personal data of the Client.</p> <p>7. Rezolve.ai Team has consent as a ground for processing the personal data for collecting queries from customers and end-users about the Privacy Policy.</p> <p>Rezolve.ai has maintained the Data Inventory. In case there are any</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	<p>changes in the process, Integrity Rezolve.ai needs to make changes in the Data Inventory_ROPA</p> <p>Evidence Verified: -Rezolve.ai Data Inventory, Version 1</p>	
5.1.2	The company has identified and documented grounds for processing for sensitive personal data for specific, stated purposes	Does Not Apply	<p>1. Rezolve.ai does not collect sensitive data.</p> <p>Hence, this control is not applied.</p>	NA
5.1.3	The company conducts Legitimate Interest Assessment before processing personal data if the grounds of processing is legitimate interest.	Compliant	<p>1. Rezolve.ai conducts a Legitimate Interest Assessment before processing personal data for purposes whose ground for processing is identified as legitimate interest.</p> <p>Evidence Verified: - LIA_Marketing Team_March 2026</p>	NA
5.1.4	The company has developed and implemented procedure to conduct Legitimate Interest Assessment before processing personal data on the grounds of legitimate interest.	Compliant	<p>1. Rezolve.ai addresses legitimate interest considerations through existing privacy, risk, and compliance assessment processes. These assessments are applied in a proportionate manner based on the nature and context of the processing activity.</p> <p>Evidence Verified: - LIA_Marketing Team_March 2026</p>	NA
5.1.5	LIA is approved internally, documented, and revised annually	Compliant	<p>1. Legitimate interest considerations are reviewed internally annually as part of ongoing privacy and compliance reviews and revisited when there are material changes to processing activities.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			Evidence Verified: - LIA_Marketing Team_March 2026	
5.1.6	The company ensures that the processing of personal data relating to criminal convictions and offences, or related security measures are carried out only under the control of official authority or when the processing is authorised by Union or Member State law.	Does Not Apply	1. Rezolve.ai does not process personal data relating to criminal convictions and offences. Hence, the control does not apply.	NA
Consent:				
5.2.1	Where the company relies on consent as its legal basis for processing data, the company obtains and records the consent from individuals	Compliant	1. Rezolve.ai demonstrated that it relies on consent as a legal basis for specific processing activities and obtains such consent through HubSpot forms and interfaces. Consent is captured and recorded within HubSpot. Evidence Verified: -Email Screenshot	NA
5.2.2	The company obtains and records the individual's explicit consent prior to collecting the individual's Sensitive Personal Data.	Does Not Apply	1. Rezolve.ai HR team POC confirmed that they process data of Indian employees. 2. Rezolve.ai collects fingerprint impressions of employees for access control purposes. The processing of such sensitive personal data is carried out for the purpose of employment.	NA
5.2.3	Where the company relies on consent as its legal basis for processing data, the company provides an option to the individual to withdraw the	Compliant	1. Rezolve.ai publishes its Privacy Notice on its website and reviews or updates it annually. 2. Rezolve.ai has defined that data subjects may withdraw their consent for processing of personal data at any time by submitting a request to the Privacy Officer, through the designated email channel.	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	consent for Processing their Personal Data.		Evidence Verified: - Rezolve.ai Privacy notice https://www.rezolve.ai/legal/privacy-policy-20260323-v2-2	
5.2.4	The company has developed and implemented procedures and/or mechanisms for obtaining the consent of the parent or guardian of a child in relation to the offer of information society services directly to a child.	Does Not Apply	1. Rezolve.ai does not provide any products or services on any of the applications and websites to children. Hence, this control does not apply.	NA
5.2.5	A Suppression list is maintained for opt-out cases and the company screens the communication against this list.	Compliant	1. Rezolve.ai maintains suppression mechanisms for opt-out requests and ensures marketing communications are screened accordingly. 2. Rezolve.ai uses the email tool 'Get Response', and it automatically removes people from this list. Evidence Verified: - Get Response Screenshot	NA
5.2.6	Do-not-call list of anyone who says they don't want marketing calls is maintained. The company screens the communication against the maintained do-not-call list including relevant preference services or relevant	Does Not Apply	1. Rezolve.ai used to conduct cold calling activities; currently, such activities are not being carried out.	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	national_regional_sectoral DND lists.			
6	Data Protection Rights			
	Data Subject Rights			
6.1.1	The company has developed and implemented procedures and_or mechanisms to meet its obligations to individuals to access their personal data.	Compliant	<p>1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to access their personal data.</p> <p>Evidence Verified: - Data Subject Rights Policy, Version 8</p>	NA
6.1.2	The company has developed and implemented procedures and_or mechanisms to meet its obligations to individuals to erase their personal data.	Compliant	<p>1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to erase their personal data.</p> <p>Evidence Verified: - Data Subject Rights Policy, Version 8</p>	NA
6.1.3	The company has developed and implemented mechanisms to restrict processing of personal data in certain cases.	Compliant	<p>1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to restrict the processing of personal data in certain cases.</p> <p>Evidence Verified: - Data Subject Rights Policy, Version 8</p>	NA
6.1.4	The company has developed and implemented procedures and_or mechanisms for transferring personal data to the individual in a structured, commonly used, and machine-readable format.	Compliant	<p>1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects for transferring personal data to the individual in a structured, commonly used, and machine-readable format.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			Evidence Verified: - Data Subject Rights Policy, Version 8	
6.1.5	The company has developed and implemented mechanisms to address the request object to processing of personal data in certain cases.	Compliant	1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to object to the processing of personal data in certain cases. Evidence Verified: - Data Subject Rights Policy, Version 8	NA
6.1.6	The company has developed and implemented mechanisms to review of and provide adequate information regarding decisions made solely based on automated processing of personal data.	Compliant	1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to object to providing adequate information regarding decisions made solely based on the automated processing of personal data. Evidence Verified: - Data Subject Rights Policy, Version 8	NA
6.1.7	The company has developed and implemented procedures and_or mechanisms to confirm whether the company is processing or has processed personal data of the individuals.	Compliant	1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to object to confirm whether the company is processing or has processed the personal data of the individuals. Evidence Verified: - Data Subject Rights Policy, Version 8	NA
6.1.8	The company has developed and implemented procedures and_or mechanisms to meet its obligations to individuals to	Compliant	1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to object to correct, complete, and update the Personal Data.	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	correct, complete, and update the Personal Data.		Evidence Verified: - Data Subject Rights Policy, Version 8	
6.1.9	The company complies with the requests and communicates the same to the individuals within the time periods specified by regulations.	Compliant	1. Rezolve.ai has developed policy and procedures and_or mechanisms for Data Subject Rights. Evidence Verified: - Data Subject Rights Policy, Version 8	NA
6.1.10	The company has developed and implemented mechanisms to object to processing of personal data for direct marketing purposes.	Compliant	1. Rezolve.ai has developed procedures and_or mechanisms to meet its obligations to data subjects to object to the processing of personal data for direct marketing purposes. Evidence Verified: - Data Subject Rights Policy, Version 8	NA
6.1.11	The company has developed and implemented mechanisms to object to processing of personal data for scientific or historical research purposes or statistical purposes except certain cases.	Does Not Apply	1. Rezolve.ai does not process personal data for scientific or historical research purposes or statistical purposes. Evidence Verified: - Data Subject Rights Policy, Version 8	NA
6.1.12	Support email or phone line is provided to modify, delete, or other data requests in the absence of a website or online self-service mechanism.	Compliant	1. Rezolve.ai has implemented a documented process to receive, assess, and respond to privacy-related queries and complaints, including those relating to personal data protection and data subject rights. Privacy-related communications are managed through designated contact channels and handled in accordance with defined procedures and GDPR timelines, with appropriate escalation where required. 2. A data subject can raise queries at - Email ID: saurabh@rezolve.ai	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			<p>- Phone: 001-833-5228466</p> <p>- Address: 11501 Dublin Blvd STE 200, Dublin, CA 94568</p> <p>3. RiskPro team has verified an email from Rezolve.ai's team to resolve the queries related to data privacy. Rezolve.ai Team agrees to maintain documented evidence and furnish the same evidence upon request.</p> <p>Evidence Verified:</p> <p>- Grievance Handling Policy, Version 8</p> <p>- Email Screenshot</p>	
7	Third Parties and Cross Border Transfers:			
	Engagement with third parties:			
7.1.1	A formal contract is executed between Company and Third-Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties.	Compliant	<p>1. Rezolve.ai executes formal contracts with third-party service providers prior to engagement. Contracts include confidentiality obligations and clearly define the responsibilities of each party.</p> <p>Evidence Verified:</p> <p>- Contract</p>	NA
7.1.2	The company ensures that the third-party processor obtains the company's express written consent prior to subcontracting services or making any changes concerning the addition or replacement of sub-processors.	Compliant	<p>Rezolve.ai confirms that it currently does not engage any sub-processors. Rezolve.ai relies on standard drafted contracts and does not specifically insist on subcontractor or sub-processor approval clauses at present.</p> <p>However, it has been agreed that, in case sub-processors are engaged in the future, the contracts will be modified accordingly.</p> <p>Evidence Verified:</p> <p>- Contract</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
7.1.3	New Third Party Service Providers are selected based on a Vendor Selection Process. Privacy and Security risk assessment is a key part of the vendor selection process. Company requires all key subservices to be compliant with security certifications and attestations such as ISO 27001, SOC1 or SOC2.	Compliant	<p>1. Rezolve.ai has documented the Vendor Privacy Assessment Policy.</p> <p>2. Rezolve.ai performs security and privacy due diligence through existing security and compliance frameworks. They do not maintain a formal vendor Due diligence report.</p> <p>Evidence Verified: - Third Party Vendor-Privacy Assessment, Version 8</p>	NA
7.1.4	On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.	Compliant	<p>1. Rezolve.ai has documented the Vendor Privacy Assessment Policy.</p> <p>2. Rezolve.ai performs security and privacy due diligence through existing security and compliance frameworks. They do not maintain a formal vendor Due diligence report.</p> <p>Evidence Verified: - Third Party Vendor-Privacy Assessment, Version 8</p>	NA
7.1.5	Data Protection Addendum (DPA), contracts are in place for all parties with whom data is shared. <_p> Entity obtains privacy commitments from vendors using Data Protection Agreement (DPA) with standard contract clauses. Entity discloses personal information only to appropriate third parties based	Compliant	<p>1. Rezolve.ai uses Data Processing Agreements and standard contractual clauses to obtain privacy commitments from vendors and customers. Personal data is shared only with appropriate third parties for defined and legitimate purposes.</p> <p>Evidence Verified: - Website DPA https://www.rezolve.ai/legal/dpa</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	on the purpose of the information. <_p>			
7.1.6	If the company is working as a data processor, the company only processes personal data in accordance with the instructions of the client company and treats it confidential.	Compliant	<p>1. When acting as a data processor, Rezolve.ai processes personal data strictly in accordance with documented customer instructions and applies confidentiality and security controls.</p> <p>Evidence Verified: - Client Contract</p>	NA
7.1.7	The company (when working as a data processor) has a contract with its client organizations to process any personal data on their behalf.	Compliant	<p>1. Rezolve.ai enters into contractual arrangements with customers governing the processing of personal data where it acts as a processor.</p> <p>Evidence Verified: - Client Contract</p>	NA
7.1.8	If the company is working as a data processor, the company obtains written authorization from the client company prior to subcontracting services.	Compliant	<p>1. Rezolve.ai addresses sub-processing requirements through contractual terms and obtains customer authorization where subcontracting is applicable.</p> <p>Evidence Verified: - Client Contract</p>	NA
Cross Border Transfer:				
7.2.1	All cross-border data flows and data export mechanisms outside of the country are identified and documented.	Compliant	<p>All cross-border data flows and data export mechanisms outside of the country are identified and documented as part of the data inventory.</p> <p>Rezolve.ai maintains the data inventory to ensure that all cross-border data flows and data export mechanisms outside of the country are identified and documented as part of the data inventory.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
			Evidence Verified: - Rezolve.ai Data Inventory, Version 1	
7.2.2	Customers are made aware that their information may be transferred outside their country.	Compliant	1. Rezolve.ai publishes a privacy notice on its website, and it contains the details about cross-border transfer. 2. Rezolve.ai reviews and updates the privacy notice as per GDPR requirements. Evidence Verified: - Rezolve.ai privacy notice https://www.rezolve.ai/legal/privacy-policy-20260323-v2-2	NA
7.2.3	Evidences of the transfer mechanism used for cross-border data flows for personal data (e.g. contracts, intra-group schemes approved by the Authority, standard contractual clauses, authority approvals) are maintained.	Compliant	1. Rezolve.ai relies on appropriate contractual and legal safeguards for cross-border data transfers and maintains relevant documentation where such transfers occur. 2. Rezolve.ai performs transfer impact assessment before transferring data across borders. Evidence Verified: - TIA_India_Rezolve.ai, - TIA_USA_Rezolve.ai, - DPA at https://www.rezolve.ai/legal/dpa	NA
8	Information Security Controls (Technical Measures):			
8.1.1	The access is provided to users on need-to-know basis.	Compliant	1. Rezolve.ai has defined and documented the Access Control Policy. 2. Rezolve.ai provides system and data access based on role-based access control and least privilege principles to ensure users only have access necessary for their job responsibilities.	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
		Compliant	<p>Evidence Verified: - Access Control Policy, Version 8</p>	
8.1.2	The access provided to the personal data is reviewed on periodic basis.	Compliant	<p>1. Rezolve.ai has defined and documented the Access Control Policy. 2. Access to systems processing personal data is reviewed periodically to ensure appropriateness and to remove unnecessary or outdated access rights. 3. Once every quarter, the CISO will review access and compare it to the HR list for any leavers still having access. 4. Once every quarter, access lists for each team’s resources will be sent to the Team Lead, who will review them against approved forms.</p> <p>Evidence Verified: - Access Control Policy, Version 8</p>	NA
8.1.3	Information security controls are implemented	Compliant	<p>1. Rezolve.ai POC informed that it is SOC compliant and hence, all the information security controls are implemented within the organization. 2. Rezolve.ai has implemented technical and organizational security controls, including encryption, network security, endpoint protection, authentication controls, and monitoring, to protect personal data.</p> <p>Evidence Verified: - SOC 2 Type 2 Report - Bridge Letter for SOC 2 Type II Report</p>	NA
8.1.4	On the day of joining, HR will send a mail to IT Helpdesk providing the details of the new joiners. The IT then provides necessary access as per request	Compliant	<p>1. Rezolve.ai HR sends an email to the IT team to provide the details of new joiners to provide access.</p> <p>Evidence Verified: Onboarding email screenshot</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
	Employee user accounts are removed from various application and network system as of the last date of employment based on access revocation request sent by HR department.			
8.1.5	When an employee leaves the organization, the employee's manager initiates the 'Exit Process'. HR informs respective teams _ IT team within 24 hours to deactivate_delete the user ID from the email system and all applications.	Compliant	<p>1. Employee exit procedures ensure timely deactivation and removal of system access following termination, supported by HR notifications and defined timelines.</p> <p>Evidence Verified: - Exit e-mail</p>	NA
8.1.6	Personal data is defined in the information classification policy	Compliant	<p>1. Rezolve.ai has defined and documented Data/ Information Classification in the Data Classification policy.</p> <p>2. Personal data is defined under the Information Classification Scheme.</p> <p>Evidence Verified: - Data Classification policy, Version 01</p>	NA
8.1.7	The data in transit and at rest in encrypted.	Compliant	<p>1. Rezolve.ai applies industry-standard encryption to protect data in transit and at rest, where applicable, in line with documented cryptographic standards and security practices.</p> <p>Evidence Verified: - tls-certificate-audit</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
8.1.8	The company must ensure that backup planning processes protect Personal Data from unauthorized use, access, disclosure, alteration, and destruction.	Compliant	<p>1. Rezolve.ai has defined and documented the Backup Policy.</p> <p>2. Rezolve.ai has defined Backup Frequency by Information Type</p> <ul style="list-style-type: none"> - Business Data: Daily backup for one week - Critical Applications: Source code version control in Bitbucket - Control Information (servers, network devices): As per cloud standards - Desktops and Laptops: No critical data stored - Portable Media: Not applicable (Frequency can be adjusted as per business/regulatory needs.) <p>Evidence Verified:</p> <ul style="list-style-type: none"> - Backup and Media Handling Policy, Version 8 	NA
8.1.9	Establish and test business continuity and disaster recovery plans.	Compliant	<p>1. Rezolve.ai maintains documented business continuity and disaster recovery plans and performs periodic testing to support service availability and data protection.</p> <p>Evidence Verified:</p> <ul style="list-style-type: none"> - BCP and DR Process, Version 9 - Disaster Recovery Plan, Version 8 	NA
9	Marketing Activities:			
	Marketing, Sales & Lead Generation:			
9.1.1	The product, service or ideals that are marketing are the same or similar to those that the individuals originally consented to receive marketing for.	Compliant	<p>1. Rezolve.ai ensures that marketing communications relate to its products and services and are consistent with the context in which contact details were originally obtained.</p>	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
9.1.2	The company identifies if the contact is an individual or business contact for marketing.	Compliant	1. Rezolve.ai distinguishes between individual and business contacts for marketing purposes and applies appropriate data protection considerations based on the context of the contact.	NA
9.1.3	The company identifies the marketer (self_other company) on any one-to-one marketing communication that they send. The company provides company name, address, phone number, and email address on any marketing communication.	Compliant	1. Rezolve.ai Marketing e-mail includes the company name, address, phone number, and email address. Evidence Verified: - Marketing email	NA
9.1.4	The company includes a link to privacy notice when sending marketing communication.	Compliant	1. Rezolve.ai includes or makes available a link to its Privacy Policy in marketing communications where applicable. Evidence Verified: - Sample Marketing mail Screenshot	NA
9.1.5	While using bought in list, company ensures that appropriate consent of data subjects are obtained by the data supplier. The company does not use a Bought-in lists for texts, emails or recorded calls unless they have proof of opt-in consent within last six months which specifically named them.	Compliant	1. Rezolve.ai utilises third-party data sources, including ZoomInfo and Clay, for sourcing business contact information.	NA

Rezolve.ai
EU GDPR Compliance Report

Ref	Controls Requirement	Current Status	Current Practice	Action Plan
9.1.6	When sending marketing communication (i.e. by email or text), the company offers an opt-out option to an individual (e.g. by reply or unsubscribe link).	Compliant	Rezolve.ai provides opt-out mechanisms in marketing communications and respects unsubscribe and preference requests in a timely manner. Evidence Verified: - Marketing email	NA

*** End of Report ***