



GDPR Compliance Letter

As of April 21, 2025



www.riskpro.in

April 21, 2025

To,
The Management,
Rezolve.ai,
USA

GDPR Compliance

Scope

Riskpro India was engaged to perform the following GDPR activities.

1. Gap Assessment / compliance review against GDPR requirements followed by issuance of Gap Report.
2. GDPR Implementation Support that included data mapping, data inventory and determining lawful basis, consent formats, etc.
3. Implementation of Privacy Policies and procedures including DPIA, Breach Response Plan, Data Subject rights
4. Third party DPA, cross border transfers
5. GDPR Induction training to staff

The regulatory scope of this report is limited to General Data Protection Regulation (GDPR).

Review Methodology

The following are the procedures and review methodologies adopted to perform the assignment.

- Discussions and interviews with the management to explain the internal processes
- Review of operations activities relating to how business is carried out
- Inspection of documents, policies and procedures
- Walkthrough of processes and systems with business

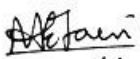
Summary Findings / Areas of Concern or Improvement

1. The company has a comprehensive Privacy Management Framework
2. The company has necessary technical and organisation measures / information security controls in place appropriate to the size and operations of the company.
3. Privacy policy on the website is GDPR compliant
4. DPA will need to be signed by each third party with which Rezolve.ai does business with. This is currently in progress.

Conclusion on GDPR Compliance



Based on our review and support during GDPR implementation, we believe that Rezolve.ai is **"GDPR Compliant"**.

A handwritten signature in black ink, appearing to read "Manoj Jain".

Manoj Jain
Director

Framework code	Title	Description	Domain	Test name	Test outcome
Article 6	Identify lawful basis	The company documents the lawful basis for PII processing.	COMPLIANCE	Publicly available privacy policy	PASS
Article 6	Identity and document purpose	The company documents the purpose for which PII is processed.	PRIVACY	Publicly available privacy policy	PASS
Article 7	Modify or withdraw consent	<p>The company provides a mechanism to modify or withdraw consent.</p> <p>Guidance: This is typically the data subject access request process.</p>	PRIVACY	Cookie consent manager	PASS
Article 7	Object to PII processing	<p>The company provides a mechanism for data subjects to object to processing.</p> <p>Guidance: This is typically the data subject access request process.</p>	PRIVACY	Publicly available privacy policy	PASS
Article 7	Consent obtained	The company determines and documents when and how consent was obtained.	PRIVACY	Company has approved its policy: Cookie Policy	Pass
Article 12, Article 13, Article 14, Article 15, Article 16, Article 17, Article 18, Article 19, Article 20, Article 21, Article 22, Article 23	Handling DSAR requests	Define and document procedures for handling Data Subject Access Requests (DSAR).	DATA_CLASSIFICATION_HAN DLING	The company has made provisions for DSAR in their website	Passed after Review

Article 12, Article 13, Article 14	PII data subject notice	The company determines and documents requirements for notice to data subjects and the timing of the notice.	PRIVACY	The company includes the necessary notifications to their subscribers in their website.	Passed after Review
Article 13	PII data subject information	The company provides data subjects clear and easily accessible information identifying the controller and describing the PII processing.	PRIVACY	Cookie Policy	PASS
Article 13	PII data subject information	The company provides data subjects clear and easily accessible information identifying the controller and describing the PII processing.	PRIVACY	Publicly available privacy policy	PASS
Article 15, Article 16	Access, correction and/or erasure	Defined process and procedure for data subjects to access and correct their PII. Guidance: This is typically the data subject access request process.	DATA_CLASSIF ICATION_HAN DLING	Publicly available privacy policy	PASS
Article 15	Copy of PII processed	Establish a process of providing a copy of PII to data subjects upon verified request.	PRIVACY	DSAR process is made available with the company	Passed after Review
Article 19	PII controllers' obligations to inform third parties	Establish a process, policies and procedures for notifying sub processors of corrections, deletions or withdrawals of PII.	PRIVACY	The company has made provisions for DSAR in their website	Passed after Review

Article 21, Article 22	Automated decision making	Identify and address obligations to data subjects resulting from decisions made from automated processing (if applicable).	PRIVACY	Data Protection Impact Assessment (DPIA)	PASS
Article 24, Article 28, Article 32	Production inventory maintained	The company maintains a formal inventory of production system assets.	ASSET_MANA GEMENT	Inventory items have descriptions	Pass
Article 24, Article 28, Article 32	Production inventory maintained	The company maintains a formal inventory of production system assets.	ASSET_MANA GEMENT	Inventory items have active owners	Pass
Article 24, Article 28, Article 32	Production inventory maintained	The company maintains a formal inventory of production system assets.	ASSET_MANA GEMENT	Inventory list tracks resources that contain user data	Pass
Article 24, Article 28, Article 32	Continuity and Disaster Recovery plans established	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	BUSINESS_CO NTINUITY_DIS ASTER_RECOV ERY	Company has an approved Business Continuity and Disaster Recovery Plan	Pass
Article 24, Article 28, Article 32	Continuity and Disaster Recovery plans tested annually	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it annually.	BUSINESS_CO NTINUITY_DIS ASTER_RECOV ERY	Company has an approved Business Continuity and Disaster Recovery Plan	Pass
Article 24, Article 28, Article 32	Password policy enforced	The company requires passwords for in-scope system components to be configured according to the company's policy.	CONFIGURATI ON_MANAGE MENT	The password policy addresses the complexity requirements	Passed after Review

Article 24, Article 28, Article 32	PII transmission controls for processor	The company encrypts PII in transit.	CRYPTOGRAP HIC_PROTECTI ONS	Company has an approved Cryptography Policy	Pass
Article 24, Article 28, Article 32	PII transmission controls for processor	The company encrypts PII in transit.	CRYPTOGRAP HIC_PROTECTI ONS	Strong SSL/TLS ciphers used	Pass
Article 24, Article 28, Article 32	PII transmission controls for processor	The company encrypts PII in transit.	CRYPTOGRAP HIC_PROTECTI ONS	SSL configuration has no known issues	Pass
Article 24, Article 28, Article 32	PII transmission controls for processor	The company encrypts PII in transit.	CRYPTOGRAP HIC_PROTECTI ONS	SSL/TLS certificate has not expired	Pass
Article 24, Article 28, Article 32	PII transmission controls for processor	The company encrypts PII in transit.	CRYPTOGRAP HIC_PROTECTI ONS	SSL/TLS enforced on company website	Pass
Article 24, Article 28, Article 32	PII transmission controls for controller	The company implements technical controls to ensure data transmitted to third parties reaches its destination.	CRYPTOGRAP HIC_PROTECTI ONS	Company has an approved Cryptography Policy	Pass
Article 24, Article 28, Article 32	PII transmission controls for controller	The company implements technical controls to ensure data transmitted to third parties reaches its destination.	CRYPTOGRAP HIC_PROTECTI ONS	Strong SSL/TLS ciphers used	Pass
Article 24, Article 28, Article 32	PII transmission controls for controller	The company implements technical controls to ensure data transmitted to third parties reaches its destination.	CRYPTOGRAP HIC_PROTECTI ONS	SSL configuration has no known issues	Pass
Article 24, Article 28, Article 32	PII transmission controls for controller	The company implements technical controls to ensure data transmitted to third parties	CRYPTOGRAP HIC_PROTECTI ONS	SSL/TLS certificate has not expired	Pass

		reaches its destination.			
Article 24, Article 28, Article 32	PII transmission controls for controller	The company implements technical controls to ensure data transmitted to third parties reaches its destination.	CRYPTOGRAPHIC PROTECTIONS	SSL/TLS enforced on company website	Pass
Article 24, Article 28, Article 32	Data encryption utilized	The company's datastores housing sensitive customer data are encrypted at rest.	CRYPTOGRAPHIC PROTECTIONS	Verifies that Cloudflare provides encryption at rest of all data stored within Cloudflare Workers KV by default.	Pass
Article 24, Article 28, Article 32	Remote access encrypted enforced	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	CRYPTOGRAPHIC PROTECTIONS	Employees access the Network over VPN	Passed after Review
Article 24, Article 28, Article 32	Data transmission encrypted	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	CRYPTOGRAPHIC PROTECTIONS	Company has an approved Cryptography Policy	Pass
Article 24, Article 25, Article 28, Article 32	Data classification policy established	The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	DATA CLASSIFICATION HANDLING	Company has an approved Data Management Policy	Passed after Review

Article 24, Article 28, Article 32	Asset disposal procedures utilized	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	DATA_CLASSIFICATION_HAN DLING	The company has a data retention and disposal policy	Passed after Review
Article 24, Article 28, Article 32	Portable media encrypted	The company encrypts portable and removable media devices when used.	DATA_CLASSIFICATION_HAN DLING	Company has an approved Cryptography Policy	Passed after Review
Article 24, Article 28, Article 32	Portable media encrypted	The company encrypts portable and removable media devices when used.	DATA_CLASSIFICATION_HAN DLING	Personnel computer hard disk encryption	Passed after Review
Article 24, Article 32	Accuracy and quality	The company has a process to ensure that PII is complete, accurate, and up-to-date.	SECURITY_PRIVACY_GOVER NANCE	Input fields in the website ensure the data is accepted only in the allowed format	Passed after Review
Article 24, Article 28, Article 32	Access revoked upon termination	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	HUMAN_RESOURCES_SECURITY	Employee termination checklist	PASS
Article 24, Article 28, Article 32	Access requests required	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	IDENTIFICATION_AUTHENTIC ATION	Company has an approved Access Control Policy	Pass

Article 24, Article 28, Article 32	Access reviews conducted	The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	IDENTIFICATION	Proof of completed access review	Passed after Review
Article 24, Article 28, Article 32	Remote access MFA enforced	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	IDENTIFICATION	MFA on Bitbucket	Passed after Review
Article 24, Article 28, Article 32	Production network access restricted	The company restricts privileged access to the production network to authorized users with a business need.	IDENTIFICATION	Privileged access is provided based on Job roles only	Passed after Review
Article 24, Article 28, Article 32	Production deployment access restricted	The company restricts access to migrate changes to production to authorized personnel.	IDENTIFICATION	Company has an approved Operations Security Policy	Passed after Review
Article 24, Article 28, Article 32	Unique network system authentication enforced	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	IDENTIFICATION	Access to production network is only enabled as per the access management policy and job roles	Passed after Review
Article 24, Article 28, Article 32	Unique account authentication enforced	The company requires authentication to systems and applications to use	IDENTIFICATION	Personnel have unique SSH keys	Pass

		unique username and password or authorized Secure Socket Shell (SSH) keys.			
Article 24, Article 28, Article 32, Article 33, Article 34	Incident response policies established	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	INCIDENT_RESPONSE	Incident report or root cause analysis	PASS
Article 24, Article 28, Article 32	MDM system utilized	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	MOBILE_DEVICE_MANAGEMENT	Malware detection on Windows workstations	Pass
Article 24, Article 28, Article 32	Network firewalls utilized	The company uses firewalls and configures them to prevent unauthorized access.	NETWORK_SECURITY	Azure Scaleset VM Public SSH denied	Pass
Article 24, Article 28, Article 32	Network segmentation implemented	The company's network is segmented to prevent unauthorized access to customer data.	NETWORK_SECURITY	Network segregation	PASS
Article 24, Article 28, Article 32	Network firewalls reviewed	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	NETWORK_SECURITY	Azure Scaleset VM Public SSH denied	Pass
Article 24, Article 28	GDPR training is implemented	The company requires employees to complete GDPR awareness training within thirty days of hire and annually thereafter.	SECURITY_AWARENESS_TRAINING	GDPR security awareness training selected	Pass

Article 24, Article 28, Article 32	Network and system hardening standards maintained	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	SECURE_ENGINEERING_ARCHITECTURE	Company has an approved Operations Security Policy	Passed after Review
Article 24, Article 28, Article 32	Intrusion detection system utilized	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	THREAT_MANAGEMENT	Personnel have computers monitored by the Vanta Agent or an MDM	Pass
Article 24, Article 28, Article 32	Anti-malware technology utilized	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	THREAT_MANAGEMENT	Personnel have computers monitored by the Vanta Agent or an MDM	Pass
Article 24, Article 28, Article 32	Service infrastructure maintained	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	VULNERABILITY_PATCH_MANAGEMENT	Records of security issues being assigned to owners	Pass

Article 24, Article 28, Article 32	Service infrastructur e maintained	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	VULNERABILIT Y_PATCH_MA NAGEMENT	Security issues assigned priorities	Pass
Article 24, Article 28, Article 32	Service infrastructur e maintained	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	VULNERABILIT Y_PATCH_MA NAGEMENT	Records of security issues being tracked	Pass
Article 24, Article 28, Article 32	Service infrastructur e maintained	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	VULNERABILIT Y_PATCH_MA NAGEMENT	P1 security issues resolved	Pass
Article 24, Article 28, Article 32	Service infrastructur e maintained	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to	VULNERABILIT Y_PATCH_MA NAGEMENT	Sample of remediated vulnerabilities	PASS

		help ensure that servers supporting the service are hardened against security threats.			
Article 24, Article 28, Article 32	Service infrastructure maintained	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	VULNERABILITY_PATCH_MANAGEMENT	Vulnerability scan	PASS
Article 25	Return, transfer or disposal of PII	The company returns, transfers, disposes PII in accordance to its policies and commitments. (SCC 8.5)	COMPLIANCE	Company has an approved Data Management Policy	Passed after Review
Article 25	Limit collection	The company limits collection of PII to the minimum that is necessary for its purposes.	COMPLIANCE	Company only collects minimum information required for processing	Passed after Review
Article 25	PII minimization	The company ensures that it only collects and processes data which it needs for its purposes.	COMPLIANCE	Company only uses minimum data that is required for processing	Passed after Review
Article 25	PII de-identification and deletion at the end of processing	The company deletes or de-identifies when no longer needed.	COMPLIANCE	Company has an approved Data Management Policy	Passed after Review
Article 25	Retention of PII	The company does not retain PII longer than necessary for its purposes.	COMPLIANCE	Company has an approved Data Management Policy	Passed after Review

Article 25	Disposal of PII	The company documents policies, procedures and mechanism for disposal of PII.	COMPLIANCE	Company has an approved Data Management Policy	Passed after Review
Article 25	Customer data deleted upon leave	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	COMPLIANCE	Storage accounts with Activity Logs have soft delete enabled (Azure)	Passed after Review
Article 27	Appoint EU representative	The company shall appoint an EU based representative.	COMPLIANCE	Company currently doesn't operate in Europe	Not Applicable after Review
Article 24, Article 28, Article 32	Network firewalls reviewed	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	NETWORK_SECURITY	Azure VM Scale Set has security groups or subnets with security groups attached	Pass
Article 28	Process as per processor agreements	The company only processes PII for the purposes expressed in contract (SCCs 8.1 and 8.2).	PRIVACY	Data Processing Agreements (DPA) with customers	PASS
Article 28	Marketing and advertising use	The company does not use the PII collected for services for marketing and advertising without consent. Consent for marketing is not required for using services.	PRIVACY	Data Processing Agreements (DPA) with customers	PASS
Article 28	Infringing instruction	The company informs the customer if processing	PRIVACY	Company only does processing for	Not Applicable after Review

		instructions are illegal. (SCC 8.1(b))		their subscribers	
Article 28	Customer obligations	The company provides their customer with information sufficient for them to demonstrate their privacy compliance. (SCC 8.9(b))	PRIVACY	Data Processing Agreements (DPA) with customers	PASS
Article 28	Disclosure of subcontractors used to process PII	The company discloses all PII sub processors to the customer.	PRIVACY	Vendors list maintained	Pass
Article 28	Assist controllers with privacy obligations	The company's Data Processing Agreements (DPA) with the customers (controllers) commit to assisting them with privacy obligations.	THIRD_PARTY_MANAGEMENT	Data Processing Agreements (DPA) with customers	PASS
Article 28, Article 46	Basis for PII transfer between jurisdictions	The company's Master Services Agreement (MSA) informs the customer of the legal basis for transfers between jurisdictions and allows customers to object to changes or terminate service.	THIRD_PARTY_MANAGEMENT	Data Processing Agreements (DPA) with customers	PASS
Article 28	Sub-processor changes	The company communicates the changes to sub-processors to the customer in writing with the opportunity to object.	THIRD_PARTY_MANAGEMENT	Data Processing Agreements (DPA) with customers	PASS
Article 28	Sub-processor changes	The company communicates the changes to sub-processors to the customer in writing with the	THIRD_PARTY_MANAGEMENT	MSA template	PASS

		opportunity to object.			
Article 28	Contracts with PII processors	The company implements a written contract with all PII processors, which includes their requirements.	THIRD_PARTY_MANAGEMENT	Company signs a contract agreement with all it's third parties	Passed after Review
Article 30	Countries and international organizations to which PII can be stored for processor	The company documents all countries where PII is stored.	ASSET_MANAGEMENT	Publicly available privacy policy	Passed after Review
Article 30	Countries and international organizations to which PII can be transferred for controller	The company specifies and documents the countries and international organizations where PII is transferred.	ASSET_MANAGEMENT	Publicly available privacy policy	PASS
Article 30	Records of transfer of PII	The company documents transfers of PII to or from third parties and ensures cooperation with the requests from data subjects.	ASSET_MANAGEMENT	Data Processing Agreements (DPA) with customers	PASS
Article 30, Article 44, Article 45, Article 46	Identify basis for PII transfer between jurisdictions	The company identifies and documents its legal basis for transferring between jurisdictions.	DATA_CLASSIFICATION_HANDLING	Publicly available privacy policy	PASS
Article 30	Records related to processing PII	The company maintains necessary privacy records.	PRIVACY	Records of all transactions are maintained by the company	Passed after Review
Article 30	Notification of PII disclosure requests	The company communicates legally binding disclosures for PII to the customer	PRIVACY	Data Processing Agreements (DPA) with customers	PASS

		before disclosure where possible. (SCC 15.1-2)			
Article 30	Records of PII disclosure to third parties	The company should record disclosure of PII to third parties including what has been disclosed and what time.	PRIVACY	Company maintains details of all PII disclosures to third parties	Passed after Review
Article 32	Pseudonymization	The company determines any need for pseudonymization and implement it as needed.	DATA_CLASSIFICATION_HANDLING	Data Protection Impact Assessment (DPIA)	PASS
Article 32	Pseudonymization	The company determines any need for pseudonymization and implement it as needed.	DATA_CLASSIFICATION_HANDLING	Pseudonymization procedure implemented	PASS
Article 33, Article 34	Incident management procedures followed	The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	INCIDENT_RESPONSE	Company has an approved Operations Security Policy	Passed after Review
Article 33, Article 34	Breach policy and procedure	The company establish policies and procedures to respond to data breaches including notification procedures.	INCIDENT_RESPONSE	Incident report or root cause analysis	PASS

Article 35	Determine needs and perform transfer impact assessment	If processing includes: - systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person; - processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10; or - systematic monitoring of a publicly accessible area on a large scale.	PRIVACY	Data Protection Impact Assessment (DPIA)	PASS
Article 35	Privacy impact assessment	The company performs a privacy impact assessment for processing or changes to processing, which represent a high risk to the rights and freedoms of data subjects.	RISK_MANAGEMENT	Data Protection Impact Assessment (DPIA)	PASS

Article 37, Article 38, Article 39	Appoint Data Protection Officer	If processing meets one of these conditions then appoint a Data Protection Officer - you are a public authority or body, - the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or - the core activities of the controller or the processor consist of processing on a large scale of special categories of data, or personal data relating to criminal convictions and offenses	SECURITY_PRIVACY_GOVERNANCE	Publicly available privacy policy & availability of designated CPO	PASS
Article 48	Legally binding PII disclosures	The company rejects any non-binding PII disclosures. (SCC 15.2)	PRIVACY	Data Processing Agreements (DPA) with customers	PASS
Article 51	Appoint EU lead supervisory authority	If the company is operating in more than one EU state then identify a lead Data Protection Authority.	COMPLIANCE	The company doesn't operate in Europe	Not Applicable after Review