

PRIVACY POLICY

Last Updated: 22 September 2026

This Privacy Policy describes how RIPL Media, operating under the brand name RiplCap (“**RiplCap**”, “**we**”, “**us**” or “**our**”), collects, uses, stores, shares and otherwise processes information in connection with the RiplCap website, web application, platform, products, managed services and related services (collectively, the “**Services**”).

RiplCap provides technology and managed operational solutions for participants in private markets, including investment managers, alternative investment funds, schemes, family offices, investors and portfolio companies.

By accessing or using the Services, you acknowledge the practices described in this Privacy Policy.

1. Scope

This Privacy Policy applies to personal data and other information processed by RiplCap through the Services.

Depending upon the circumstances, RiplCap may process personal data:

- (a) for its own purposes in connection with operating the Services, managing accounts, communications, security, billing and business operations; or
- (b) on behalf of an organisation using RiplCap, where such organisation determines the purposes for which information is collected and processed.

Where RiplCap processes information on behalf of a customer, the customer's own privacy notices, policies and instructions may also apply.

2. Information We Collect

We may collect the following categories of information:

Account and identification information: name, designation, organisation, business email address, telephone number, username, authentication information and account details.

Professional and organisational information: employer, fund, scheme, portfolio company, investor or other organisational affiliation, role, authority and professional contact details.

Investor and LP information: identification details, contact details, commitment and contribution information, capital call information, distribution information, investment holdings and other information uploaded or maintained by an authorised customer.

KYC and AML information: identification and verification information, KYC documents, beneficial ownership information and information required for KYC, AML, sanctions, PEP or related screening workflows.

Portfolio and investment information: investment amounts, securities, ownership, valuations, financial information, investment performance, transaction details, investor rights, funding rounds, exits and other portfolio information.

Documents and files: agreements, term sheets, investment documents, financial statements, MIS reports, valuation reports, KYC documents, board or shareholder documents, correspondence and other materials uploaded to the Services.

Usage and technical information: IP address, device and browser information, login information, timestamps, pages or features accessed, activity logs, audit logs and security-related information.

Communications: information contained in emails, support requests, demonstrations, feedback, enquiries and other communications with RipplCap.

Website information: information collected through cookies and similar technologies, where used.

We may also receive information from customers, their authorised users, portfolio companies, investors, service providers and other persons authorised to provide information through the Services.

3. How We Use Information

We may process information to:

- (a) provide, operate and maintain the Services;
- (b) create and administer accounts and user permissions;
- (c) facilitate fund, scheme, portfolio company and investor workflows;
- (d) support portfolio monitoring and investor relations;
- (e) facilitate onboarding, KYC and AML-related workflows;
- (f) conduct or facilitate AML, sanctions, PEP and related screening through RipplCap or authorised third-party service providers;
- (g) facilitate reporting and document-management workflows;
- (h) generate, extract, organise, classify or analyse information contained in documents;
- (i) assist with preparation of term sheets, investment documents, reports and other outputs;
- (j) provide managed operational services, including follow-ups, information collection and document-completeness workflows;
- (k) provide technical support and respond to requests;
- (l) maintain audit trails, records and platform security;
- (m) prevent fraud, misuse, unauthorised access and security incidents;
- (n) improve and develop the Services;
- (o) communicate product, operational and service-related information;
- (p) comply with applicable law, regulatory requirements, legal processes and lawful requests; and
- (q) establish, exercise or defend legal rights.

Where required by applicable law, RipplCap will process personal data on an appropriate lawful basis and obtain consent where required.

4. Customer-Provided Data

Customers may upload or provide information concerning their investors, LPs, portfolio companies, directors, employees, representatives, service providers and other persons.

The customer is responsible for ensuring that it has the necessary authority, permissions, notices and, where applicable, consents required to provide such information to RipplCap and instruct RipplCap to process it.

RipIcap will process customer-provided information in accordance with the applicable customer agreement, authorised instructions and applicable law.

5. KYC and AML Information

Certain Services may enable customers to collect, review or process information for KYC and AML-related purposes.

AML, sanctions, PEP, adverse-media or similar screening may be performed through specialist third-party providers. Information necessary for such screening may therefore be securely transmitted to such providers.

A screening result, match or alert does not by itself constitute a determination that a person has engaged in unlawful or improper conduct. Customers remain responsible for reviewing screening results and making their own compliance determinations.

6. Artificial Intelligence and Automated Processing

Certain RipIcap features may use artificial intelligence, machine learning, optical extraction or other automated technologies to extract, classify, summarise, analyse or generate information.

Such technologies may be used, for example, to extract information from financial or legal documents, identify data fields, generate draft documents or assist with reporting workflows.

Automated outputs may contain errors or omissions and should be reviewed by appropriately qualified persons before being relied upon.

Where third-party technology providers are used, information may be processed by such providers subject to contractual, confidentiality and security arrangements.

7. Sharing of Information

We may share information with:

Service providers: cloud hosting providers, infrastructure providers, communications providers, analytics providers, security providers, AI technology providers and other vendors supporting the Services.

KYC and AML providers: specialist providers used for identity verification, sanctions, PEP, AML or related screening.

Professional advisers: lawyers, accountants, auditors, consultants and other advisers where reasonably necessary.

Customer-authorised recipients: investors, portfolio companies, investment managers, schemes or other persons where the customer directs or authorises such sharing through the Services.

Government and regulatory authorities: where disclosure is required by applicable law, court order or lawful governmental or regulatory request.

Corporate transactions: in connection with a merger, acquisition, financing, restructuring, sale of business or similar transaction, subject to appropriate safeguards.

We do not sell personal data as a business model.

8. Connected Organisations and Data Visibility

Where the Services enable investment managers, funds, portfolio companies, investors or other organisations to connect, information will only be made available in accordance with applicable permissions, customer instructions and platform access controls.

The fact that multiple organisations use RiplCap does not, by itself, permit one organisation to access another organisation's confidential information.

9. Data Security

RiplCap implements reasonable technical and organisational safeguards designed to protect information against unauthorised access, alteration, disclosure, loss or destruction.

These measures may include, as appropriate, access controls, role-based permissions, authentication controls, encryption, audit logging, backups and monitoring.

No electronic system or transmission method is completely secure. Accordingly, absolute security cannot be guaranteed.

10. Data Retention

We retain information for so long as reasonably necessary to provide the Services, fulfil contractual obligations, comply with applicable law, resolve disputes, maintain security and audit records and enforce agreements.

Retention periods may vary depending on the nature of the information, customer instructions and applicable legal requirements.

Following termination of a customer relationship, information may be deleted, anonymised or retained for a limited period in accordance with applicable agreements, backup cycles and legal requirements.

11. International Processing and Transfers

RiplCap or its service providers may process information using infrastructure located in India or other jurisdictions.

Where personal data is transferred or processed across jurisdictions, RiplCap will take measures required under applicable law.

12. Your Rights

Subject to applicable law and the capacity in which RiplCap processes the relevant information, individuals may have rights in relation to their personal data, including rights to access information, request correction or updating, request erasure, withdraw consent where processing is based on consent, raise grievances and exercise other rights available under applicable law.

Where RiplCap processes personal data solely on behalf of a customer, a request may need to be directed to the relevant customer.

Requests may be submitted to dewansh.vashishth@riplcap.com.

13. Cookies

RiplCap may use cookies and similar technologies that are necessary for authentication, security, preferences, functionality, analytics and operation of the Services.

Where required by applicable law, users will be provided appropriate choices regarding non-essential cookies.

14. Communications

We may send users service-related communications concerning accounts, security, product functionality, transactions and other operational matters.

Subject to applicable law, we may also send information about RiplCap products, services and developments. Recipients may opt out of marketing communications using the unsubscribe mechanism provided or by contacting us.

15. Children's Data

The Services are intended for businesses and professionals and are not directed towards children.

Users must not knowingly provide children's personal data through the Services unless they are legally authorised to do so and all requirements under applicable law have been satisfied.

16. Third-Party Services

The Services may integrate with or contain links to third-party platforms or services. RiplCap is not responsible for the independent privacy practices of third parties, and users should review the applicable third-party privacy policies.

17. Changes to this Privacy Policy

We may update this Privacy Policy from time to time to reflect changes in the Services, applicable law or our processing practices.

The updated version will be made available through the Services together with the revised “Last Updated” date. Where required by applicable law, additional notice or consent will be obtained.

18. Governing Data Protection Framework

RiplCap processes personal data in accordance with applicable Indian law, including provisions of the Information Technology Act, 2000 and applicable rules thereunder, and the Digital Personal Data Protection Act, 2023 and Digital Personal Data Protection Rules, 2025 to the extent such provisions are in force and applicable from time to time.

19. Grievances and Contact

For privacy-related questions, requests or grievances, please contact:

RiplCap

Brand of RIPL Media (Sole)

Address: Suncity, Sector 54, Gurgaon

Email: dewansh.vashishth@riplcap.com

Grievance Contact: Dewansh Vashishth