

PRIVACY POLICY

RiseUp Creators Platform
Sharde Media and Productions Pvt. Ltd.

Legal Entity & Registration Details

Company Name: Sharde Media and Productions Pvt. Ltd. CIN: U90009BR2023PTC062405 GSTIN: 10ABKCS5322D1ZU Registered Office: Jagriti Nagar, Ashiyana, Patna Aerodome Phulwari, Patna — 800014, Bihar, India Website: www.riseupcreators.com | Email: privacy@riseupcreators.com

Effective Date: [Insert Date] | Version: 2.1 | Last Reviewed: May 2026

Amendment Notice

This document incorporates amendments resolving all compliance gaps identified in the Cyber Law Audit of May 2026, including: Data Fiduciary identity (§2), AI training consent (§13A), children's data (§14), breach notification (§12A), legitimate uses (§5B), retention schedule (§11), processor accountability (§9), rights operationalisation (§8), dispute resolution (§20), SPDI compliance (§3B), and AI content liability (§13B).

1. Introduction

RiseUp Creators is a digital platform operated by **Sharde Media and Productions Pvt. Ltd.** ("Company", "RiseUp", "we", "our", "us"), a company incorporated under the Companies Act, 2013, bearing CIN **U90009BR2023PTC062405** and GSTIN **10ABKCS5322D1ZU**, having its Registered Office at Jagriti Nagar, Ashiyana, Patna Aerodome Phulwari, Patna — 800014, Bihar, India.

RiseUp enables creators, artists, musicians, performers, educators, and event organizers to monetize content, distribute digital media, sell event tickets, engage with audiences, and manage creator communities.

We are committed to protecting the privacy and personal data of our users in compliance with:

- The Digital Personal Data Protection Act, 2023 ("DPDP Act") and applicable Rules notified thereunder;
- The Information Technology Act, 2000 and IT (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("SPDI Rules");
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021;
- Applicable RBI payment, GST, and intermediary compliance obligations;
- The Consumer Protection Act, 2019;
- The Copyright Act, 1957 (as applicable to content licensing);
- GDPR-aligned principles where cross-border data flows involve EEA data subjects.

2. Data Fiduciary — Identity & Contact

AMENDED — Issue #2 Resolved: Data Fiduciary identity now fully established

For all purposes under the DPDP Act and applicable Indian law, the Data Fiduciary is:

Data Fiduciary

Sharde Media and Productions Pvt. Ltd. CIN: U90009BR2023PTC062405 GSTIN: 10ABKCS5322D1ZU Registered Office: Jagriti Nagar, Ashiyana, Patna Aerodome Phulwari, Patna — 800014, Bihar — 800014 Operating as: RiseUp Creators Website: www.riseupcreators.com Privacy Email: privacy@riseupcreators.com

3. Definitions

In this Privacy Policy, unless the context otherwise requires:

- "Data Principal" means the individual to whom the personal data relates, as defined under the DPDP Act.
- "Personal Data" means any data about an individual who is identifiable by or in relation to such data.
- "Sensitive Personal Data or Information (SPDI)" has the meaning assigned under the IT (SPDI) Rules, 2011, and includes passwords, financial information, health data, biometric data, and government-issued identification.
- "Processing" includes collection, storage, organisation, sharing, use, disclosure, transmission, deletion, or any operation on personal data.
- "Consent Manager" means a person registered under the DPDP framework enabling Data Principals to manage, review, or withdraw consent.
- "Creator" means any artist, musician, influencer, educator, event organizer, or rights-holder using the Platform.
- "User" means any individual accessing or using the Platform, including fans, customers, ticket purchasers, and creators.
- "Data Processor" means any person who processes personal data on behalf of the Company pursuant to a contract.
- "Minor" means any individual below the age of eighteen (18) years.
- "Verifiable Parental Consent" means consent given by a parent or lawful guardian through a mechanism that the Company can reasonably verify as authentic.
- "AI-Generated Content" means any content generated wholly or partially using artificial intelligence, including generative audio, video, text, visual, or synthetic media tools.

4. Categories of Personal Data Collected

We collect only such information as is necessary and proportionate to the purposes described in this Policy.

A. Account & Identity Information

- Name, username, email address, mobile number, date of birth
- Profile photograph
- Government-issued identification (Aadhaar number collected as SPDI — see §12 for safeguards)
- GSTIN / business details for creator/vendor accounts

B. Financial & Transaction Data (SPDI)

AMENDED — Issue #12 Resolved: SPDI classification and handling explicitly stated

The following data categories are classified as Sensitive Personal Data or Information (SPDI) under the IT (SPDI) Rules, 2011 and are subject to the enhanced safeguards set out in Section 12:

- UPI IDs and bank account details
- Payment gateway transaction references
- Ticket purchase history and subscription records
- GST invoices, PAN, and tax documentation

Note: Card payment details are processed exclusively by RBI-compliant, PCI-DSS-certified third-party payment processors and are never stored on RiseUp servers. Tokenisation of card data is implemented per RBI guidelines.

C. Creator & Content Information

- Uploaded music, videos, artwork, ticket listings, livestreams
- Content metadata and digital rights ownership declarations
- Royalty, monetisation, and licensing information

D. Device & Technical Information

- IP address, browser type, device identifiers, operating system

- App usage analytics, login timestamps, session data
- Cookies and tracking technologies (see Schedule A)

E. Communication Data

- Support tickets, chat records, feedback, grievance submissions

F. AI-Generated Content Metadata

- AI disclosure labels, AI tool identifiers, watermarking and provenance metadata
- Synthetic media declarations made by uploading creators

5. Lawful Basis for Processing

AMENDED — Issue #6 Resolved: Legitimate uses mapped to specific DPDP Act provisions

A. Consent (DPDP Act §6)

Where processing is based on consent, such consent shall be free, informed, specific, unconditional, and unambiguous, obtained through our granular purpose-specific consent interface at onboarding and at each data collection trigger point. Consent is not bundled with acceptance of Terms of Service.

Consent-based processing purposes:

- Personalised content recommendations
- Optional analytics and product improvement tracking
- Marketing and promotional communications
- AI model training using engagement signals (explicit opt-in only — see §13A)

B. Certain Legitimate Uses (DPDP Act §7) — Specific Sub-provisions

Processing under 'certain legitimate uses' is not a catch-all. Each purpose is mapped to a specific sub-provision of DPDP Act §7:

- §7(a) — State and its instrumentalities: Compliance with court orders, government directions, and statutory obligations.
- §7(b) — Legal proceedings: Processing necessary for legal claims, dispute resolution, and enforcement of contractual rights.
- §7(c) — Medical emergency or public health: Not applicable to RiseUp's core operations.
- §7(d) — Employment: Processing of employee/contractor data for HR purposes.
- §7(f) — Breakdown of public order: Cybersecurity incident response and fraud prevention in coordination with CERT-In.

Processing that does not fall within a specific sub-provision of §7 will require consent under §6.

C. Legal Compliance

- GST compliance, tax invoicing, and regulatory reporting
- PMLA / KYC obligations for financial processing
- CERT-In cybersecurity reporting obligations
- Intermediary due diligence under IT Rules 2021

6. Purpose of Data Processing

We process personal data strictly for the following specified purposes:

- Platform operations: account creation, ticketing, content delivery, creator payouts
- Music & content distribution: royalty processing, metadata management, licensing verification, copyright enforcement
- Safety & compliance: fraud detection, identity verification, AI content moderation, prevention of unlawful activity
- Analytics & product improvement: platform optimisation, audience analytics (where consented)

- Legal & financial compliance: GST invoicing, financial audits, regulatory reporting, dispute resolution
- Grievance redressal: processing complaints, responding to Data Principal rights requests

7. Consent Management & Withdrawal

Where processing is based on consent under DPDP Act §6:

- Consent shall be obtained through a granular, purpose-specific popup interface at onboarding (Step 1: account creation; Step 2: financial data; Step 3: content upload; Step 4: marketing communications) and at each subsequent data collection trigger point.
- Each purpose is presented as a separate toggle. Required processing is clearly labeled and locked. Optional processing defaults as stated in the consent interface.
- Consent is timestamped, versioned (Policy version ID), and stored in a consent audit log per user.
- Users may withdraw consent at any time through: Account Settings → Privacy; in-app consent manager; email to privacy@riseupcreators.com; or through a registered Consent Manager under the DPDP framework.
- Withdrawal of consent shall not affect the lawfulness of processing based on consent prior to its withdrawal.
- Upon withdrawal of consent for certain purposes, related features (e.g., personalised recommendations, marketing emails) will be disabled within 48 hours.

8. Data Principal Rights

AMENDED — Issue #10 Resolved: Rights operationalised with timelines, process, and grounds for refusal

Under the DPDP Act, Data Principals may exercise the following rights. All requests must be submitted to privacy@riseupcreators.com or through in-platform privacy controls, accompanied by reasonable identity verification.

A. Right to Access Information

Process: Submit a written request identifying the categories of data sought. Response: Acknowledgement within 48 hours; summary of personal data processed delivered within 15 days. Format: Digital summary via email or downloadable report in Account Settings → Privacy → My Data.

B. Right to Correction & Erasure

Process: Submit a correction or erasure request specifying the data and the correction sought, or grounds for erasure. Response: Correction or erasure completed within 15 days, or grounds for refusal communicated. Grounds for refusal: Data required for compliance with a legal obligation; data subject to an ongoing legal proceeding; data whose erasure would prejudice the rights of another Data Principal.

C. Right to Withdraw Consent

Process: Via Account Settings → Privacy, in-app toggle, or written request to privacy@riseupcreators.com. Effect: Processing for the withdrawn purpose ceases within 48 hours. Prior processing is unaffected.

D. Right to Grievance Redressal

Process: File a complaint with the Grievance Officer (see §16). Response timeline: Acknowledgement within 24 hours; resolution within 15 days; escalation pathway to Data Protection Board of India if unresolved.

E. Right to Nominate

A Data Principal may nominate another individual to exercise their rights under this Policy in the event of death or incapacity. Nominations must be submitted in writing to privacy@riseupcreators.com.

F. Right to Data Portability

Data Principals may request a copy of their personal data in a structured, commonly used, machine-readable format (JSON or CSV). Response: Within 15 days of a verified request.

9. Data Sharing & Third-Party Processor Accountability

AMENDED — Issue #9 Resolved: Processor categories, safeguards, and contractual obligations specified

We may share personal data with the following categories of third parties. All Data Processors are bound by written Data Processing Agreements (DPAs) that impose obligations equivalent to or stricter than those under this Policy and the DPDP Act.

Processor Category	Examples	Processing Purpose	Safeguard
Payment processors	Razorpay, PayU, Cashfree	Payout, subscription billing	RBI-compliant; PCI-DSS; DPA
Cloud infrastructure	AWS, GCP, Azure	Hosting, storage, CDN	ISO 27001; DPA; encryption
Analytics vendors	Mixpanel, Firebase	Usage analytics (de-identified)	DPA; no re-identification
Email / SMS providers	SendGrid, MSG91	Transactional communications	DPA; data minimisation
Music distribution	DistroKid, TuneCore	Royalty & metadata processing	DPA; copyright obligations
Rights societies	PPL India, IPRS	Licensing & royalty accounting	Statutory framework; DPA
Customer support tools	Freshdesk, Zendesk	Grievance & ticket management	DPA; data isolation

Processor Accountability Obligations

All Data Processors engaged by the Company are contractually required to:

- Process personal data only on documented instructions from the Company;
- Implement technical and organisational security measures equivalent to those described in §12;
- Not engage sub-processors without prior written consent from the Company;
- Notify the Company of any personal data breach within 6 hours of becoming aware;
- Delete or return all personal data upon termination of the processing agreement;
- Submit to audits and inspections by the Company or its nominated auditor.

We do not sell personal data to any third party for commercial or advertising purposes.

Legal & Regulatory Disclosures

We may disclose personal data to law enforcement, courts, or government authorities where required by law, court order, or government direction. We will notify the Data Principal of any such disclosure to the extent permitted by applicable law.

10. International Data Transfers

Your personal data may be processed outside India by our cloud infrastructure and analytics vendors. Such transfers are subject to:

- Applicable Central Government notifications under DPDP Act §16 restricting transfers to certain countries;
- Contractual safeguards including Standard Contractual Clauses (SCCs) or equivalent data transfer agreements;
- The Company's vendor security assessment programme.

Current countries of processing include: United States (AWS, GCP), Ireland (GCP EU region), Singapore (AWS AP). This list is updated as vendor arrangements change. Contact privacy@riseupcreators.com for the current transfer impact assessment.

11. Data Retention Schedule

AMENDED — Issue #8 Resolved: Specific retention periods specified per data category with legal basis

We retain personal data only for as long as necessary to fulfil the purposes for which it was collected, or as required by law. The following schedule sets out specific retention periods:

Data Category	Retention Period	Legal Basis
Account & identity data	Duration of account + 3 years post-closure	DPDP Act; IT Act
Financial & transaction records	7 years from transaction date	Income Tax Act, 1961; GST Act
KYC / Government ID documents	5 years post-account closure	PMLA, 2002
Payment gateway references	5 years	RBI guidelines
Royalty & licensing records	10 years	Copyright Act, 1957
Device & technical logs	90 days (rolling)	IT (SPDI) Rules 2011
Support & grievance records	3 years post-resolution	IT Act; DPDP Act
Marketing consent records	Duration of consent + 5 years	DPDP Act §6
AI content interaction metadata	2 years (de-identified)	Contractual / DPDP Act
Breach notification records	5 years	CERT-In Directions 2022

Upon expiry of the applicable retention period, personal data is securely deleted or anonymised such that the individual is no longer identifiable. Creators may request early deletion of optional data categories through Account Settings → Privacy → Delete My Data, subject to mandatory legal retention obligations.

12. Security Practices & SPDI Compliance

AMENDED — Issue #12 Resolved: SPDI Rules 2011 operationalised

A. General Security Safeguards

RiseUp implements the following reasonable security practices and procedures as required under IT Act §43A and SPDI Rules 2011, Rule 8:

- Encryption of data in transit (TLS 1.3) and at rest (AES-256);
- Role-based access controls with principle of least privilege;
- Multi-factor authentication for all administrative access;
- Secure cloud infrastructure with ISO 27001-certified providers;
- Regular security audits and penetration testing (minimum annually);
- Vendor security assessments prior to onboarding;
- Employee data protection training (minimum annually).

B. SPDI-Specific Safeguards (IT SPDI Rules 2011)

For Sensitive Personal Data or Information (including financial data, government ID, passwords):

- Written consent is obtained separately from general account consent before collection of SPDI;
- SPDI is collected only for a lawful purpose connected with a function of the Company;
- SPDI is not retained longer than is required for the purpose for which it was collected (see §11);
- SPDI is not transferred to third parties without prior permission of the Data Principal, except where required by law or court order;
- The Company has a documented Information Security Programme (ISP) reviewed annually;
- SPDI access logs are maintained and reviewed quarterly.

12A. Data Breach Notification Procedure

AMENDED — Issue #5 Resolved: Data breach procedure with statutory timelines

Breach Notification Commitment

The Company will notify the Data Protection Board of India and affected Data Principals of any personal data breach in accordance with the timelines set out below. This obligation is absolute and is not conditional on confirmation of harm.

Detection & Internal Escalation

- Any employee or contractor who becomes aware of a potential personal data breach must report it immediately to the Data Protection Officer / Grievance Officer at grievance@riseupcreators.com.
- The Grievance Officer shall convene an internal breach response team within 2 hours of receiving a report.

CERT-In Reporting (IT Act & CERT-In Directions 2022)

- Certain cybersecurity incidents (including unauthorised access, data breaches, ransomware) must be reported to CERT-In within 6 hours of the Company becoming aware.
- The Grievance Officer is designated as the CERT-In compliance point of contact.

DPDP Act — Data Protection Board Notification

- The Company shall notify the Data Protection Board of India of any personal data breach in the manner and within the period prescribed under the DPDP Act and applicable Rules.
- The notification shall include: nature of the breach; categories and approximate number of Data Principals affected; categories and approximate quantity of personal data affected; name and contact of the Grievance Officer; description of likely consequences; measures taken or proposed to address the breach.

Data Principal Notification

- Affected Data Principals shall be notified of a breach without undue delay where the breach is likely to result in high risk to their rights and freedoms.
- Notification shall be made by email to the registered email address, and by in-platform notice within the Account dashboard.
- Notification to Data Principals shall include: description of the breach in plain language; contact details of the Grievance Officer; recommended steps the Data Principal can take to protect themselves.

Breach Response Record

The Company shall maintain a record of all personal data breaches, including those not meeting the notification threshold, for a period of 5 years. This record shall be made available to the Data Protection Board on request.

13. AI Transparency & Synthetic Media Policy

In compliance with emerging Indian IT advisories and platform integrity standards:

- Users uploading AI-generated content must clearly disclose such content as required by applicable law and platform policy.
- RiseUp may label, watermark, restrict, or moderate synthetic media.
- Misleading deepfakes, impersonation content, or deceptive AI-generated media may be removed.
- We use automated moderation tools, including AI systems, for trust and safety enforcement.
- Users remain responsible for ensuring AI-generated content complies with applicable law and third-party rights.

13A. AI Systems, Model Training & Automated Processing

AMENDED — Issue #3 Resolved: AI training requires explicit opt-in consent; original creative works excluded

AI Training — Default Position

RiseUp does NOT use your original creative content (music, videos, artwork, text) for AI model training. The AI training toggle defaults to OFF at onboarding. Opt-in is entirely voluntary and can be withdrawn at any time from Settings → Content → AI Preferences.

RiseUp Creators may use the following limited categories of data for AI system development and improvement, subject to the conditions set out below:

- Platform interaction data and engagement metrics (de-identified);
- Usage patterns and session analytics;
- Content moderation signals (not the content itself);
- Recommendation system training data (de-identified, aggregated).

Conditions for AI Processing

- All AI training processing shall be carried out: (a) on a de-identified, aggregated, or pseudonymised basis where reasonably feasible; (b) subject to reasonable technical and organisational safeguards; (c) in accordance with applicable law.
- The following data shall NEVER be used for AI model training: (a) private communications; (b) payment credentials or financial data; (c) government-issued identification documents; (d) passwords; (e) health or biometric data; (f) original creative content (music, video, artwork, text) unless the Creator has entered into a separate written AI licensing agreement with the Company.
- Where the DPDP Act or applicable rules require explicit consent for AI-based processing, such consent shall be obtained through the opt-in mechanism described in §7. Consent is not bundled with account creation or Terms of Service acceptance.
- Data Principals who have opted in may withdraw consent at any time. Withdrawal applies to future processing only; de-identified data already incorporated into trained models cannot be removed.

Automated Decision-Making

RiseUp deploys automated systems for: spam detection; copyright enforcement; content moderation; fraud prevention; recommendation engines; safety monitoring; AI-generated content labelling. No automated processing shall produce decisions that have a significant legal or similar effect on a Data Principal without a meaningful human review mechanism available upon request.

13B. AI-Generated Content — Creator Rights & Platform Liability

AMENDED — Issue #13 Resolved: Due process and appeal rights added; liability framework balanced

Creator Disclosure Obligations

- Creators uploading or distributing AI-generated or synthetically altered content must disclose the use of AI tools as required by applicable law and platform policy.
- Creators must apply AI-content labels where required by Indian IT advisories or platform policy.
- Creators must not use AI tools to create deceptive impersonation or deepfake content of real individuals without their consent.

Platform Enforcement — Due Process

RiseUp reserves the right to label, restrict, demonetise, remove, or investigate AI-generated content that may mislead users, infringe third-party rights, violate applicable law, or create risks to public safety or platform integrity. However, the following due process protections apply:

- Before demonetisation or removal of content on AI grounds, the Creator shall receive a written notice specifying: (a) the content affected; (b) the grounds for action; (c) the evidence or signals relied upon; (d) the proposed enforcement action.
- The Creator shall have 7 days from receipt of notice to respond, provide additional context, or contest the decision.
- The Company shall review the Creator's response and communicate a final decision within 15 days.
- Creators may appeal final decisions to the Grievance Officer under §16. If unresolved, escalation to the Data Protection Board or courts is available as set out in §20.
- Emergency removal (without prior notice) is permitted only where content poses an imminent risk of harm to an identifiable individual, public safety, or is otherwise required by law. In such cases, the

Creator shall be notified within 24 hours of removal and the due process protections in sub-paragraphs (a)–(d) above shall apply from that point.

14. Children's Privacy

AMENDED — Issue #4 Resolved: Age verification, parental consent, and prohibition on child-directed tracking added

Children's Data — Absolute Protections

RiseUp does not knowingly engage in behavioural tracking, targeted advertising, profiling, or personalisation directed at any user below the age of 18. These protections are absolute and cannot be waived by parental consent.

A. Age Verification at Onboarding

All users must confirm their date of birth at account registration. The Platform implements the following age-gating mechanism:

- Users who declare an age of 18 or above proceed to standard onboarding.
- Users who declare an age of 13 to 17 are presented with a Parental Consent Popup requiring: (a) the name and email address of a parent or legal guardian; (b) active confirmation by the parent/guardian via a verification email sent to the parent's email address; (c) the parent/guardian's agreement to this Policy on behalf of the minor. Account creation is blocked until parental consent is verified.
- Users who declare an age below 13 are not permitted to register on the Platform under any circumstances.

B. Verifiable Parental Consent Process

The parental consent verification process operates as follows:

1. The minor provides their date of birth and their parent/guardian's email address at registration.
2. A verification email is sent to the parent/guardian's email containing: a clear description of the Platform; the specific data to be collected and its purpose; a link to this Privacy Policy; an active consent button; and a link to refuse consent.
3. The parent/guardian must actively click the consent button. Silence or non-response does not constitute consent.
4. Upon successful parental consent, the minor's account is created with restrictions described in sub-section C.
5. Parental consent is re-verified annually for minor accounts.

C. Restrictions on Minor Accounts

Accounts held by users below the age of 18 are subject to the following mandatory restrictions, which cannot be altered by the minor or their parent/guardian:

- No behavioural tracking or profiling for any purpose;
- No targeted or personalised advertising;
- No use of the minor's data for AI model training of any kind;
- No sharing of the minor's personal data with third-party advertising or marketing platforms;
- Creator monetisation features (payouts, ticket sales, subscription revenue) are disabled for users below 18;
- No tracking of listening history for external analytics sharing.

D. Discovery of Minor Accounts

If the Company discovers that a user has provided a false date of birth and is in fact below the age of 18, the account shall be immediately suspended and the data collected shall be deleted, subject to any mandatory legal retention obligations. The parent/guardian of the identified minor shall be notified.

15. Cookies & Tracking Technologies

We use essential, analytics, marketing, and functional cookies as detailed in Schedule A. Detailed management options are available in our Cookie Policy and through in-platform cookie settings.

16. Grievance Officer

AMENDED — Issue #10 Resolved: Grievance mechanism fully operationalised with timelines

Grievance Officer Details

Name: Sudhanshu Shekhar Designation: Grievance Officer, RiseUp Creators Email: grievance@riseupcreators.com Address: Sharde Media and Productions Pvt. Ltd., Jagriti Nagar, Ashiyana, Patna Aerodome Phulwari, Patna — 800014, Bihar, India Availability: Monday to Friday, 10:00 AM to 6:00 PM IST (except public holidays)

Grievance Process

6. Submission: File a grievance by email to grievance@riseupcreators.com, clearly stating: your full name; registered email address; description of the grievance; relevant data or transactions; desired resolution.
7. Acknowledgement: The Grievance Officer shall acknowledge receipt of the grievance within 24 hours.
8. Investigation: The Grievance Officer shall investigate the grievance and may request additional information from the complainant.
9. Resolution: The Grievance Officer shall communicate a resolution or reasoned decision within 15 days of acknowledgement.
10. Extension: In complex matters, the resolution period may be extended by up to a further 15 days with written notice to the complainant.
11. Escalation: If the complainant is not satisfied with the resolution, they may escalate to the Data Protection Board of India as constituted under the DPDP Act.

17. Intermediary Status & Safe Harbour

RiseUp operates as an intermediary platform for creator-generated content and claims protection under applicable intermediary safe harbour provisions under the IT Act and IT Rules 2021, subject to compliance with all due diligence obligations thereunder.

RiseUp does not claim ownership of user personal data or creator intellectual property solely by virtue of hosting. Users remain responsible for the legality of uploaded content. Nothing in this Policy limits the Company's right to take down content pursuant to court orders, government directions, or takedown notices from rights-holders.

18. Updates to This Privacy Policy

We may revise this Privacy Policy to reflect legal developments, platform changes, security updates, or regulatory requirements. Material changes will be communicated through website notices, app notifications, and email communications at least 15 days before taking effect. Continued use of the Platform after the effective date of the revised Policy constitutes acceptance.

19. Contact Us

For privacy-related questions, requests, or complaints:

- Email: privacy@riseupcreators.com
- Grievance Officer: grievance@riseupcreators.com

- Postal: Sharde Media and Productions Pvt. Ltd., Jagriti Nagar, Ashiyana, Patna Aerodome Phulwari, Patna — 800014, Bihar, India

20. Dispute Resolution & Governing Law

AMENDED — Issue #11 Resolved: Statutory consumer and regulatory rights carved out from arbitration

Statutory Rights Preserved

Nothing in this Section limits or restricts a Data Principal's right to: (a) file a complaint with the Data Protection Board of India under the DPDP Act; (b) approach a Consumer Disputes Redressal Commission under the Consumer Protection Act, 2019; (c) approach any court or tribunal of competent jurisdiction in respect of a right that cannot lawfully be subjected to mandatory arbitration.

This Privacy Policy shall be governed by and construed in accordance with the laws of India. Subject to the statutory rights preserved above, disputes shall be resolved as follows:

A. Amicable Resolution

The parties shall first attempt to resolve any dispute through good-faith negotiations. If not resolved within 30 days, the following applies.

B. Grievance Officer — First Escalation

Prior to initiating any formal proceedings (other than regulatory complaints under the DPDP Act or Consumer Protection Act), the Data Principal must first exhaust the Grievance Officer process set out in §16. This requirement does not apply where the Grievance Officer is the subject of the complaint or where immediate legal relief is required.

C. Mediation

If the dispute remains unresolved after the Grievance Officer process, it shall be referred to mediation before an independent neutral mediator mutually appointed by the parties. Mediation shall be conducted in New Delhi, India, in the English language, within 45 days of appointment.

D. Arbitration

If mediation fails, the dispute shall be finally resolved by arbitration under the Arbitration and Conciliation Act, 1996. The arbitration shall be conducted by a sole arbitrator mutually appointed (or, failing agreement, appointed per the Act); seated in New Delhi, India; conducted in English; under Indian law. The arbitral award shall be final and binding.

For the avoidance of doubt, disputes concerning alleged violations of the DPDP Act, Consumer Protection Act, or any other consumer-protection or data-protection statute may be raised before the relevant statutory authority regardless of the arbitration clause above.

E. Jurisdiction

Subject to the arbitration provisions, the courts of New Delhi shall have exclusive jurisdiction over disputes arising from this Privacy Policy.

Schedule A — Cookie & Tracking Technology Categories

Category	Purpose	Required	Opt-out Available
Essential cookies	Login, session security, payment flow	Yes — cannot be disabled	No
Analytics cookies	Usage statistics and platform optimisation	Optional	Yes — Cookie Settings
Marketing cookies	Advertising and remarketing (never for minors)	Optional	Yes — Cookie Settings

Functional cookies	Personalisation and user preferences	Optional	Yes — Cookie Settings
--------------------	--------------------------------------	----------	-----------------------

Schedule B — User Consent Statement

By using RiseUp Creators, you acknowledge that:

- You have read and understood this Privacy Policy;
- You consent to processing as described herein where consent is the lawful basis, as confirmed through the granular consent interface at onboarding;
- You understand your rights as a Data Principal under the DPDP Act and other applicable laws;
- Where you are a parent or guardian completing registration on behalf of a minor, you confirm that you have the authority to give consent on behalf of the minor and that you accept this Policy on their behalf.

Schedule C — Compliance Amendment Log

Issue #	Section	Amendment	Date
#2	§2	Data Fiduciary fully identified with CIN, GSTIN, registered address	May 2026
#3	§13A	AI training requires explicit opt-in; original works excluded; withdrawal rights added	May 2026
#4	§14	Age verification popup; parental consent process; minor account restrictions added	May 2026
#5	§12A	Data breach notification section added with CERT-In and DPDP Act timelines	May 2026
#6	§5B	Legitimate uses mapped to specific DPDP Act §7 sub-provisions	May 2026
#8	§11	Data retention schedule with specific periods and legal bases added	May 2026
#9	§9	Processor accountability table; DPA obligations; data sale prohibition clarified	May 2026
#10	§8, §16	Rights operationalised with timelines; grievance process detailed; portability added	May 2026
#11	§20	Statutory consumer and regulatory rights explicitly carved out from arbitration	May 2026
#12	§3B, §12B	SPDI classification explicit; IT SPDI Rules 2011 safeguards operationalised	May 2026
#13	§13B	Creator due process (notice, response period, appeal) added to AI content enforcement	May 2026

— End of Privacy Policy —

Sharde Media and Productions Pvt. Ltd. | CIN: U90009BR2023PTC062405 | privacy@riseupcreators.com

