

PRIVACY POLICY

Effective Date: 1st May 2026

Upsurge Labs LLP, a limited liability partnership registered under the laws of India, having its registered office at 13, 80 Feet Rd, 3rd Floor Above Aurum Fitness, Koramangala, Bangalore - 560034 (hereinafter referred to as “Zelta”, “Company”, “we”, “us”, or “our”), values your privacy and is committed to protecting your personal, sensitive, and health-related information.

This Privacy Policy describes how we collect, process, store, use, disclose, retain, and protect information when you access or use the Zelta platform, website, telemedicine services, consultations, subscription services, communications systems, and related services (collectively, the “Platform” or “Services”).

This Privacy Policy is intended to comply with applicable Indian laws governing digital personal data protection, electronic records, telemedicine, healthcare confidentiality, consumer protection, and related regulatory requirements.

By accessing, registering with, or using the Platform, you acknowledge that you have read, understood, and agreed to this Privacy Policy.

1. INTRODUCTION

Zelta operates as a technology-enabled healthcare facilitation and telemedicine platform designed to support healthcare delivery, patient-management workflows, specialist consultations, treatment coordination, prescription fulfilment support, and subscription-based healthcare services.

The Platform facilitates preliminary health assessments, onboarding workflows, telemedicine consultations with licensed medical practitioners (“Specialists”), treatment-management support, prescription fulfilment coordination through licensed pharmacy partners, logistics coordination, and related healthcare-support services.

The Company understands that certain information processed through the Platform may constitute sensitive health-related personal information. Accordingly, the Company is committed to processing such information responsibly, securely, and only for lawful and operationally necessary purposes connected with the Services.

By using the Platform, you expressly consent to the collection, processing, storage, sharing, retention, and disclosure of your information in accordance with this Privacy Policy.

2. INFORMATION WE COLLECT

In order to provide the Services, the Platform may collect, receive, process, or store different categories of information from Users.

2.1. Personal Information

The Company may collect personal information including:

- full name;
- date of birth;
- age;
- gender;
- email address;
- mobile number;
- residential address;
- emergency contact details;
- account credentials;
- government identification details where required under applicable law;
- and other information voluntarily provided by the User.

Such information may be collected during:

- registration;
- onboarding;
- consultations;
- support interactions;
- payment processing;
- and continued use of the Platform.

2.2. Health & Medical Information

The Platform may collect health-related information including:

- height;
- weight;
- BMI;
- medical history;
- symptoms;
- diagnoses;
- medications;
- allergies;
- treatment objectives;
- lifestyle information;
- laboratory reports;
- prescriptions;
- consultation records;
- treatment history;
- adverse event information;
- and other medically relevant information voluntarily provided by the User.

Certain information may be collected:

- through assessment forms;
- during consultations;
- through telemedicine interactions;
- through follow-up care;
- or through communications with Specialists or support personnel.

The User acknowledges that certain healthcare decisions and treatment recommendations may depend upon the completeness and accuracy of the information provided.

2.3. Payment & Subscription Information

The Company may collect information relating to:

- subscription plans;
- payment transactions;
- recurring billing authorisations;
- invoices;
- refunds;
- and billing history.

Payment processing services may be provided by authorised third-party payment processors.

The Company does not intentionally store complete debit card, credit card, banking, or payment authentication credentials unless permitted under applicable law and industry standards.

2.4. Technical & Device Information

The Platform may automatically collect technical information including:

- IP address;
- browser type;
- operating system;
- device identifiers;
- session activity;
- access timestamps;
- cookies;
- analytics information;
- website interaction behaviour;
- and related technical usage information.

Such information may be used for:

- security;
- analytics;

- fraud prevention;
- service improvement;
- debugging;
- and operational monitoring purposes.

2.5. Communications & Support Information

The Company may collect and maintain records relating to:

- emails;
- WhatsApp communications;
- telephonic conversations;
- support interactions;
- onboarding calls;
- grievance communications;
- consultation scheduling;
- and related operational communications.

Certain communications may be documented, retained, monitored, or reviewed for:

- patient safety;
- audit;
- quality control;
- grievance handling;
- medico-legal;
- compliance;
- and operational purposes.

3. HOW WE USE YOUR INFORMATION

The Company may use the information collected through the Platform for lawful and operationally necessary purposes connected with the Services.

Such purposes may include:

- facilitating telemedicine consultations;
- coordinating healthcare services;
- supporting Specialists in treatment workflows;
- facilitating prescription fulfilment;
- coordinating pharmacy and logistics operations;
- processing subscriptions and payments;
- maintaining medical and operational records;
- improving Platform functionality and user experience;
- customer support and grievance handling;
- fraud prevention and security monitoring;
- regulatory compliance;
- audit and quality-control purposes;

- and lawful operational purposes connected to the Services.

The Company may also use information to:

- maintain continuity of care;
- improve treatment-management workflows;
- monitor service quality;
- manage operational risks;
- and ensure Platform safety and compliance.

The Company does not sell personal health-related information to unrelated third parties for independent commercial exploitation.

4. TELEMEDICINE & HEALTH DATA

The Platform facilitates healthcare interactions through telemedicine technologies and digital communication systems.

By participating in consultations through the Platform, the User expressly consents to:

- telemedicine consultations;
- remote healthcare delivery;
- electronic collection of medical information;
- digital storage of records;
- electronic prescriptions;
- and healthcare coordination through electronic systems.

The User acknowledges that telemedicine consultations may involve:

- audio communications;
- video consultations;
- electronic records;
- digital assessments;
- asynchronous communications;
- and remote treatment-management systems.

The User further acknowledges that telemedicine consultations have inherent limitations when compared to physical in-person consultations, including:

- inability to conduct physical examinations;
- reliance on self-reported information;
- technology disruptions;
- and limitations associated with remote healthcare delivery.

Consultation records, prescriptions, onboarding interactions, support communications, and related healthcare interactions may be electronically documented, retained, monitored, and reviewed for:

- patient safety;
- quality control;
- audit;
- medico-legal;
- grievance resolution;
- training;
- regulatory compliance;
- and operational continuity purposes.

5. DATA SHARING & DISCLOSURE

The Company may share information strictly where reasonably necessary for lawful healthcare delivery, operational support, compliance, or related purposes connected with the Services.

5.1. Specialists

Information may be shared with licensed Specialists for:

- consultations;
- treatment recommendations;
- prescriptions;
- dosage management;
- follow-up care;
- and patient treatment purposes.

5.2. Pharmacy Partners

Information may be shared with licensed pharmacy partners for:

- prescription verification;
- medication dispensing;
- pharmaceutical compliance;
- logistics coordination;
- and treatment fulfilment purposes.

5.3. Logistics & Delivery Providers

The Company may share relevant operational information with logistics and delivery providers for:

- shipment handling;
- cold-chain coordination;
- address verification;
- delivery fulfilment;
- and related logistics operations.

5.4. Payment Processors

Information relating to subscriptions and payments may be shared with authorised payment processors for:

- payment processing;
- recurring billing;
- fraud prevention;
- transaction verification;
- and related financial operations.

5.5. Service Providers & Vendors

The Platform may utilise authorised third-party service providers including:

- cloud-hosting providers;
- analytics vendors;
- CRM systems;
- communication systems;
- customer-support tools;
- telemedicine infrastructure providers;
- and operational vendors.

Such vendors shall receive access only to the extent reasonably necessary for providing operational support or Services.

5.6. Regulatory & Legal Authorities

The Company may disclose information where required:

- under applicable law;
- pursuant to regulatory directives;
- in response to lawful governmental requests;
- pursuant to court orders;
- for fraud prevention;
- for dispute resolution;
- or for legal compliance purposes.

6. COMMUNICATION CONSENT

By accessing or using the Platform, the User expressly consents to receiving communications through:

- email;
- SMS;
- WhatsApp;
- telephonic calls;

- push notifications;
- and in-platform communication systems.

Such communications may include:

- consultation reminders;
- prescription updates;
- treatment communications;
- subscription notifications;
- support communications;
- billing alerts;
- delivery updates;
- operational notices;
- and regulatory communications.

The User acknowledges that certain communications may be necessary for providing healthcare support, treatment continuity, operational coordination, compliance, and patient safety.

Users may opt out of promotional communications where applicable. However, service-related and operational communications may continue where reasonably necessary for providing the Services.

7. COOKIES & ANALYTICS

The Platform may use cookies, analytics systems, tracking technologies, and related tools for:

- improving Platform functionality;
- understanding user behaviour;
- maintaining security;
- monitoring operational performance;
- fraud prevention;
- analytics;
- and improving user experience.

Third-party analytics providers may collect certain technical and behavioural information in accordance with their respective privacy practices.

Users may modify browser settings to manage or disable cookies; however, certain Platform functionalities may become unavailable or impaired if cookies are disabled.

8. DATA RETENTION

The Company retains personal and health-related information only for as long as reasonably necessary:

- to provide the Services;
- to maintain healthcare records;
- for operational continuity;
- for legal and regulatory compliance;
- for audit purposes;
- for dispute resolution;
- for fraud prevention;
- and for enforcement of legal rights.

Certain medical and operational records may be retained for extended durations where required under applicable law, healthcare documentation standards, telemedicine obligations, or regulatory requirements.

Upon expiry of applicable retention periods, the Company may securely delete, anonymise, archive, or de-identify information in accordance with applicable practices and operational requirements.

9. DATA SECURITY

The Company implements commercially reasonable administrative, technical, organisational, and operational safeguards designed to protect information against:

- unauthorised access;
- misuse;
- disclosure;
- alteration;
- destruction;
- accidental loss;
- and unlawful processing.

Such safeguards may include:

- restricted access controls;
- password protection;
- encryption measures;
- secure hosting infrastructure;
- audit mechanisms;
- vendor oversight;
- and operational monitoring systems.

While reasonable safeguards are implemented, no digital system, internet transmission, or electronic storage mechanism can be guaranteed completely secure.

Users are responsible for maintaining confidentiality of:

- account credentials;
- devices;

- passwords;
- and access mechanisms used to access the Platform.

10. USER RIGHTS

Subject to applicable law, Users may have the right to:

- access certain personal information;
- request correction of inaccurate information;
- withdraw consent where legally permissible;
- request deletion of information where applicable;
- and raise grievances regarding data processing.

Requests may be submitted through the contact details provided below.

The Company may request verification of identity before processing certain requests in order to:

- protect account security;
- prevent unauthorised access;
- and comply with applicable legal obligations.

Certain information may continue to be retained where:

- legally required;
- operationally necessary;
- or necessary for compliance, dispute resolution, fraud prevention, audit, or healthcare documentation purposes.

11. CHILDREN'S PRIVACY

The Platform is not intended for individuals below eighteen (18) years of age unless accessed through:

- a parent;
- legal guardian;
- or authorised representative,

in accordance with applicable law.

The Company does not knowingly collect personal information from minors without appropriate authorisation where required.

12. CROSS-BORDER PROCESSING & VENDORS

Certain authorised vendors, service providers, technology systems, cloud infrastructure providers, analytics providers, or communication systems used by the Platform may involve storage or processing of information across different jurisdictions.

By using the Platform, the User expressly consents to such processing where reasonably necessary for:

- operational continuity;
- healthcare coordination;
- Platform functionality;
- customer support;
- analytics;
- security;
- and Service delivery.

The Company shall endeavour to ensure that authorised vendors process information in accordance with reasonable contractual, operational, and security safeguards.

13. THIRD-PARTY LINKS & SERVICES

The Platform may contain links to third-party websites, applications, tools, services, or platforms.

The Company does not control and is not responsible for:

- privacy practices;
- content;
- operational standards;
- or security measures

of third-party platforms not operated or controlled by the Company.

Users are encouraged to independently review applicable third-party privacy practices before interacting with such platforms.

14. POLICY MODIFICATIONS

The Company reserves the right to modify, update, revise, or amend this Privacy Policy from time to time.

Updated versions shall become effective upon publication on the Platform unless otherwise required under applicable law.

Continued access to or use of the Platform following publication of revised versions constitutes acknowledgment and acceptance of the updated Privacy Policy.

15. GRIEVANCE OFFICER & CONTACT DETAILS

For privacy-related concerns, data requests, consent withdrawal requests, or grievances, Users may contact:

Email: info@zelta.in

Support: +91 9980308701

The Company shall endeavour to address grievances and requests within reasonable timelines in accordance with applicable law.

16. CONSENT ACKNOWLEDGMENT

By accessing or using the Platform, the User acknowledges and agrees that:

- (a) the User has read and understood this Privacy Policy;
- (b) the User voluntarily consents to the collection, processing, storage, retention, sharing, and disclosure of information in accordance with this Privacy Policy;
- (c) certain information processed through the Platform may constitute sensitive health-related personal information;
- (d) telemedicine consultations and related healthcare interactions may involve electronic communications and digital recordkeeping;
- (e) information may be shared with Specialists, pharmacy partners, logistics providers, payment processors, authorised vendors, and regulatory authorities strictly where necessary for Service delivery, compliance, healthcare coordination, operational support, and related lawful purposes;
- (f) communications may occur through email, SMS, WhatsApp, telephonic calls, and related communication systems;
- (g) consultation records and operational interactions may be electronically documented, monitored, retained, and reviewed for patient-safety, audit, medico-legal, quality-control, training, grievance-resolution, and regulatory purposes; and
- (h) the User voluntarily consents to the processing of information for lawful healthcare, operational, compliance, security, and related purposes connected to the Services.