PRIVACY POLICY

Effective Date: January 27, 2026
Last Updated: January 27, 2026

---

1. INTRODUCTION

RelyceAI ("**we**," "**us**," "**our**," or the "**Company**") is committed to protecting your privacy and complying with all applicable Indian data protection laws. This Privacy Policy explains how we collect, use, store, and protect your personal data when you use our chatbot services, website, and applications (collectively, the "**Services**").

This Privacy Policy is an important document. We strongly recommend you read it carefully. By using our Services, you acknowledge that you have read and understood this Privacy Policy and consent to the data practices described herein.

---

2. WHAT PERSONAL DATA WE COLLECT

2.1 Data You Provide Directly ("Input Data")

When you use our Services, you may voluntarily provide:

Account Information: Name, email address, username, password - for account creation and authentication

Usage Data: Queries you submit, interactions with the chatbot - for providing chatbot responses and service functionality

Communication Data: Messages, feedback, support inquiries - for customer support and service improvement

Profile Data: Language preference, timezone, interests - for personalization of user experience

Device Information: Device type, operating system, IP address, browser type - for security, fraud detection, service optimization

Important: We do **NOT** request or collect: - Passwords for other services - Banking or financial account details - Biometric information (fingerprints, facial recognition) - Health records or medical data - Government ID numbers (Aadhaar, PAN, etc.) - Sexual orientation or other sensitive identity data

---

2.2 Data Collected Automatically

We automatically collect certain information through:

Cookies and Similar Technologies: - Session cookies (temporary, deleted when you close browser) - Functionality cookies (remember your preferences) - Analytics cookies (track usage patterns) - Security cookies (prevent fraud and abuse)

Server Logs: - IP address and geolocation - Timestamp of access - Pages or features accessed - Duration of use - Referring URL - Error logs and system diagnostics

Analytics Tools: - Google Analytics (if enabled) - tracks general usage patterns - Custom analytics - measures chatbot performance - User engagement metrics

You can control cookie settings through your browser. Disabling cookies may limit some features.

2.3 Conversation Data

Critical Commitment: Your conversation data with our chatbot is: - **Stored temporarily** only to provide immediate service functionality - **Not used** to train, improve, or develop our AI models - **Not shared** with third parties for AI training purposes - **Automatically deleted** after a reasonable retention period (typically 30-90 days) - **Deletable upon request** with 30 days for complete removal

---

3. HOW WE USE YOUR PERSONAL DATA

3.1 Service Delivery

- Providing chatbot responses and functionality
- Creating and maintaining your account
- Authenticating your identity
- Personalizing your experience
- Delivering requested features

3.2 Service Improvement and Maintenance

- Analyzing chatbot performance and response quality
- Identifying and fixing technical issues
- Optimizing user interface and functionality
- Conducting security testing and updates
- **NOT** for training new AI models

3.3 Security and Fraud Prevention

- Detecting abuse, fraud, or unauthorized access
- Preventing spam and phishing

- Protecting intellectual property rights
- Enforcing our Terms of Use
- Responding to security incidents

3.4 Legal and Regulatory Compliance

- Complying with court orders and legal processes
- Responding to government agency requests
- Enforcing our Terms of Use and other agreements
- Protecting against legal liability
- Maintaining audit trails and records

3.5 Customer Support

- Responding to your inquiries and complaints
- Providing technical assistance
- Following up on support tickets
- Improving support processes

3.6 Communication

- Sending account notifications (login alerts, password resets)
- Service announcements
- Security alerts
- Policy updates
- **With consent only**: Marketing communications or promotional offers

3.7 Data We Do NOT Use

- Training our AI models (this is a core commitment)
- Developing competing products or services
- Selling data to third parties for profit
- Creating user profiles for tracking across internet
- Behavioral advertising or targeting based on sensitive data
- Creating deceptive deepfakes or misleading content

---

4. LEGAL BASIS FOR DATA PROCESSING

Under the Digital Personal Data Protection Act, 2023, our processing is based on:

Service delivery & account management: Your explicit consent and contractual necessity

Security and fraud prevention: Your consent and our legitimate interest in protecting the platform

Legal compliance: Legal obligation under Indian law

Customer support: Your consent and contractual obligation

Service improvement (non-training): Your consent and legitimate interest

Communication with you: Your consent

You may withdraw consent at any time, though this may limit our ability to provide Services.

---

5. DATA SHARING AND DISCLOSURE

5.1 We Do NOT Share Your Data With Third Parties For:

- AI model training or development
- Selling to data brokers or marketing companies
- Behavioral advertising or profiling
- Commercial purposes without your explicit consent
- Building competing AI systems

5.2 We MAY Share Your Data With:

Service Providers: - Cloud storage providers (data hosting) - Email service providers (for communications) - Analytics platforms (usage tracking) - Payment processors (if applicable) - Support ticketing systems

These vendors are contractually bound to: - Use data only as directed by us - Implement reasonable security safeguards - Not disclose data to third parties - Delete data when no longer needed - Not use data for their own purposes

Legal Authorities: - Government agencies, courts, or law enforcement - Only in response to valid legal process (court order, warrant, subpoena) - Only the data specifically required by law - We will notify you of disclosure unless prohibited by law

Business Transfers: - In case of merger, acquisition, or sale of assets - Data recipients will be bound by this Privacy Policy or a substantially similar one - You will be notified of material changes

5.3 Data Processors We Use

Details of third-party processors: - Cloud hosting provider (Data storage and infrastructure) - Analytics provider (Usage analytics and performance) - Support platform (Customer support management)

(Details to be updated upon finalization of service architecture)

---

6. DATA RETENTION AND DELETION

6.1 Retention Periods

Conversation Data: 30-90 days - Service functionality; automatically deleted

Account Data: Duration of account + 180 days - Legal obligations, dispute resolution

Server Logs: 90 days - Security, fraud detection, debugging

Analytics Data: 12-24 months (aggregated) - Service improvement

Support Records: 2 years - Legal compliance, dispute resolution

Payment Records (if applicable): 7 years - Tax and legal compliance

6.2 Data Deletion Rights

You have the right to request deletion of your data:

- **Request Method**: Email support@relyceai.com with subject "Data Deletion Request"
- **Response Time**: We will acknowledge within 15 days and complete deletion within 30 days
- **Exceptions**: We may retain data longer if:
  - Required by law (tax records, legal holds)
  - Necessary for account security or dispute resolution
  - Needed for ongoing investigations

6.3 Automatic Deletion

- Conversation data is automatically purged from active systems after 90 days
- Your account can be deleted, which removes associated personal data
- Automated deletion processes ensure timely removal

---

7. DATA SECURITY AND PROTECTION

7.1 Security Measures

We implement industry-standard safeguards:

- **Encryption**: TLS/SSL encryption for data in transit; AES-256 for data at rest
- **Access Controls**: Role-based access; least privilege principles; authentication requirements
- **Infrastructure Security**: Firewalls, intrusion detection, regular security audits
- **Employee Training**: Data protection training for all staff handling data
- **Incident Response**: Documented procedures for breach detection and response
- **Regular Testing**: Penetration testing, vulnerability assessments, security reviews

- **Compliance Standard**: Aligned with ISO/IEC 27001 information security practices

7.2 Limitations of Security

No security system is impenetrable. While we implement robust safeguards: - We cannot guarantee absolute protection against sophisticated attacks - You are responsible for maintaining your account password confidentiality - Transmission of data over the internet carries inherent risks - We are not liable for security breaches caused by user negligence

---

8. YOUR DATA PROTECTION RIGHTS

Under the Digital Personal Data Protection Act, 2023, and Section 43A of the Information Technology Act, 2000, you have the following rights:

8.1 Right to Know (Access)

- **What**: Access to all personal data we hold about you
- **How**: Email support@relyceai.com with "Data Access Request"
- **Response Time**: 30 days
- **Format**: Digital format (machine-readable if feasible)
- **Cost**: Free

8.2 Right to Correct (Rectification)

- **What**: Correct inaccurate or incomplete data
- **How**: Update your profile or email support@relyceai.com
- **Response Time**: 15 days
- **Examples**: Update incorrect email, phone, or preferences

8.3 Right to Erasure (Deletion)

- **What**: Request deletion of your personal data
- **How**: Email support@relyceai.com with "Deletion Request"
- **Response Time**: 30 days for complete deletion
- **Exceptions**: Data required by law or for legitimate purposes (security, legal holds)

8.4 Right to Withdraw Consent

- **What**: Withdraw consent for specific data processing at any time
- **How**: Email support@relyceai.com with "Withdraw Consent Request"
- **Effect**: We will stop using data for that purpose (may limit Services)
- **No Penalty**: Withdrawal does not affect past processing

8.5 Right to Data Portability

- **What**: Receive your data in structured, standard format
- **How**: Email support@relyceai.com with "Data Portability Request"
- **Format**: CSV, JSON, or similar machine-readable format
- **Response Time**: 30 days

8.6 Right to Grievance

- **What**: Lodge complaints about data handling
- **How**:
  - Email: support@relyceai.com
  - Data Protection Board of India: complaints@dataprotectionboard.gov.in (when operational)
  - District Consumer Commission under Consumer Protection Act, 2019

Exercise Your Rights

To exercise any right, email: **support@relyceai.com**

Include: - Full name and account identifier - Specific request (access, correction, deletion, etc.) - Reason for request (if applicable) - Contact information for response

---

9. CHILDREN'S DATA PROTECTION

9.1 Age Restrictions

- Our Services are not directed to children under 18 years old
- We do not knowingly collect data from children under 13
- Children aged 13-17 may use Services only with parental consent

9.2 Parental Consent for Children 13-17

- Parents/guardians must:
  - Provide explicit written consent
  - Verify their identity
  - Accept responsibility for the child's use
- We will not process children's data without verified parental consent
- Children cannot consent on their own; parental consent is mandatory

9.3 Parental Rights for Children's Data

Parents/guardians of children 13-17 may: - Request access to the child's data - Require correction of data - Request deletion of data - Withdraw consent for processing - Receive notification of changes to privacy practices

9.4 Data Minimization for Children

- We collect minimal data from children
- No targeting, profiling, or behavioral tracking
- No cookies or tracking pixels
- No marketing communications without parental consent
- No sharing with third parties except as necessary for service

9.5 Reporting Child Safety Violations

- If you suspect a child's data is being misused, contact: support@relyceai.com
- Include details of violation and evidence
- We will investigate and respond within 15 days

---

10. INTERNATIONAL DATA TRANSFERS

10.1 Data Localization

- Your data is primarily stored in India (Tamil Nadu or other Indian locations)
- We comply with data localization requirements under the Digital Personal Data Protection Act, 2023

10.2 Cross-Border Transfers (if applicable)

- Where data must be transferred outside India:
  - Only to jurisdictions with adequate data protection laws
  - Only with your explicit consent
  - Only with contractual safeguards (Standard Contractual Clauses or adequacy decisions)
  - You will be notified in advance

10.3 Your Rights for International Transfers

- You may withdraw consent for cross-border transfers
- We will maintain data within India upon your request
- This may limit functionality in certain cases

---

11. COOKIES AND TRACKING TECHNOLOGIES

11.1 Types of Cookies We Use

Session Cookies: Maintain login and service state - Browser session - Automatically cleared

Preference Cookies: Remember your language, timezone - 12 months - Browser settings

Security Cookies: CSRF protection, fraud prevention - Session - Browser settings

Analytics Cookies: Track usage for improvement - 24 months - Opt-out available

Third-Party Cookies (if any): Google Analytics (if enabled) - Varies - Google privacy controls

11.2 Your Cookie Choices

- Most browsers allow you to refuse cookies
- You can delete cookies at any time

- Disabling cookies may limit chatbot functionality
- You can use private/incognito browsing to avoid persistent cookies

11.3 Managing Cookies

- **Chrome**: Settings > Privacy and security > Cookies and site data
- **Firefox**: Settings > Privacy & Security > Cookies and Site Data
- **Safari**: Preferences > Privacy > Manage Website Data
- **Edge**: Settings > Privacy, Search, and Services > Clear browsing data

---

12. AUTOMATED DECISION-MAKING AND PROFILING

12.1 No Automated Individual Decision-Making

- We do **NOT** make decisions that significantly affect your rights based solely on automated processing
- Examples of decisions we don't make:
  - Denying access based on automated analysis
  - Determining creditworthiness or eligibility
  - Creating psychological profiles or risk assessments
  - Making recommendations that fundamentally limit your opportunities

12.2 No Profiling for Targeting

- We do **NOT** create detailed profiles for:
  - Behavioral targeting
  - Manipulation or nudging
  - Predictive decisions about you
  - Building psychological models
  - Selling to advertisers

12.3 Transparency Requirements

- Any automated processing is transparent
- You can request information about automated processing
- You have the right to human review of decisions

---

13. DATA BREACH NOTIFICATION

13.1 Our Commitment

- We monitor for breaches continuously
- We respond to breaches immediately
- We notify affected individuals and authorities as required by law

13.2 Breach Response Timeline

Breach detection: Immediate investigation

Internal assessment: 72 hours

Notification to you: Within 72 hours of confirmation (if required)

Notification to authorities: As required by law

Public announcement: If required by law or affecting many individuals

13.3 What We'll Tell You

In breach notifications, we'll provide: - Description of the breach and data involved - Likely consequences for your data - Steps we're taking to secure data and prevent recurrence - Your rights and recommended actions - Contact for more information

13.4 Your Breach Rights

- You have the right to know if your data is breached
- You may file complaints with Data Protection Board
- You may seek compensation for losses under IT Act Section 43A
- You may file complaints with Consumer Commissions

---

14. COMPLIANCE WITH APPLICABLE LAWS

14.1 Laws Governing This Policy

This Privacy Policy complies with: - **Digital Personal Data Protection Act, 2023** (DPDP Act) - **Information Technology Act, 2000** (Sections 43A, 72A) - **IT (Reasonable Security Practices) Rules, 2011** - **IT (Intermediary Guidelines) Rules, 2021** - **Consumer Protection Act, 2019** - **Consumer Protection (E-Commerce) Rules, 2020** - **Indian Contract Act, 1872** - **Any other applicable Indian federal and state laws**

14.2 Regulatory Authorities

- **Data Protection Board of India**: Handles DPDP Act complaints (when operational)
- **District Consumer Commissions**: Handle consumer protection complaints
- **State and National Consumer Commissions**: Appellate authority
- **Central Cyber Crime Portal**: Report data security incidents

---

15. AI-GENERATED CONTENT AND DATA TRANSPARENCY

15.1 No Data Used for Training

- Conversations with our chatbot are **NOT** used to train our AI models
- Responses you receive are generated from pre-trained models
- Your data does not improve our models

- Historical conversations are not used for model fine-tuning

15.2 AI-Generated Output

- Responses are AI-generated based on your input
- Output may contain errors or inaccuracies
- Output is not guaranteed to be unique
- Other users may receive similar responses

15.3 Transparency and Labeling

- Our chatbot is clearly identified as AI
- You always know you're interacting with AI, not a human
- We do not:
  - Claim AI output was human-generated
  - Impersonate human experts
  - Create deceptive deepfakes using your data
  - Use your data to create misleading content

---

16. THIRD-PARTY LINKS AND SERVICES

16.1 Third-Party Websites

- Our Services may contain links to third-party websites
- We are **not responsible** for their privacy practices
- Third-party privacy policies govern their data collection
- We do not endorse or warrant third-party sites

16.2 Third-Party Integrations (if any)

- If we integrate with third-party services, it will be clearly disclosed
- Integration is optional; you can choose not to connect
- Third-party services have separate privacy policies
- We are not responsible for third-party data handling

---

17. CALIFORNIA AND EU RESIDENTS (If Applicable)

17.1 California Residents (CCPA/CPRA)

- California residents have additional rights under CCPA/CPRA
- These rights are in addition to Indian law rights
- Contact support@relyceai.com to exercise California rights

17.2 EU Residents (GDPR)

- If you're in the EU, GDPR rights apply
- Our India operations comply with GDPR to the extent you're a data subject
- Contact support@relyceai.com for GDPR inquiries

18. CONTACT AND GRIEVANCE REDRESSAL

18.1 Contact Information

For any questions, requests, or concerns about this Privacy Policy:

RelyceAI Privacy Team
Email: support@relyceai.com
Website: https://relyceai.com/
Address: Chennai, Tamil Nadu, India
Response Time: Within 15 business days

18.2 Grievance Officer

We have appointed a Grievance Officer under the IT Intermediary Guidelines:

Email: grievance@relyceai.com
Response Time: Within 24 hours of receipt

18.3 How to File a Grievance

Step 1: Email grievance@relyceai.com with: - Subject: “Privacy Grievance” - Your name and account identifier - Description of the grievance - Supporting documentation

Step 2: We will acknowledge within 24 hours and assign a reference number

Step 3: Investigation and resolution within 15 days

Step 4: If unsatisfied, escalate to: - Data Protection Board of India (once operational) - District Consumer Commission - Cyber Crime Reporting Portal

18.4 Escalation to Authorities

If you’re unsatisfied with our response:

Consumer Commission (Consumer Protection Act, 2019): - District Consumer Commission (Tamil Nadu) - State Consumer Commission (Tamil Nadu) - National Consumer Commission: https://consumercomplaints.nic.in/

Data Protection Board (Digital Personal Data Protection Act, 2023): - Website: (To be operational) - Email: complaints@dataprotectionboard.gov.in

Cyber Crime Portal: - Website: https://cybercrime.gov.in/ - Report data security incidents and deepfakes

19. CHANGES TO THIS PRIVACY POLICY

19.1 Policy Updates

- We may update this Privacy Policy periodically
- Material changes will be communicated with **at least 30 days' notice** via:
  - Email notification to your registered email
  - In-product notification when you log in
  - Updated on our website with a "Last Updated" date

19.2 Your Rights When We Update

- You will be informed of material changes before they take effect
- You can review the updated policy before continuing to use Services
- Continuing to use Services after the notice period means you accept the updated policy
- You may withdraw consent if you disagree with changes

19.3 Significant Changes

Examples of material changes requiring advance notice: - New purposes for data collection or use - New third-party sharing arrangements - Changes to retention periods - Changes that reduce your rights - Changes that increase our obligations

---

20. GENERAL PROVISIONS

20.1 Entire Agreement

- This Privacy Policy, together with our Terms of Use, forms the complete agreement
- No other statements, promises, or commitments apply
- Conflicting provisions: Terms of Use > Privacy Policy

20.2 Severability

- If any provision is invalid or unenforceable, it is severed
- Remaining provisions continue in full force

20.3 Survival

- Provisions regarding your rights, data security, and grievance procedures survive any termination

20.4 Our Authority

- RelyceAI is the Data Fiduciary (Controller) responsible for your personal data
- We determine the purpose and means of data processing
- We are accountable for compliance with this Privacy Policy

End of Privacy Policy