

BIMBA XR - PRIVACY POLICY

Application Name: BIMba XR

Company Name: Sarvayaan

Last Updated: November 24, 2025

Jurisdiction: India

1. INTRODUCTION

This Privacy Policy ("**Policy**") describes how Sarvayaan ("**we**," "**us**," "**our**," or "**Company**") collects, processes, stores, uses, shares, and protects your personal data and sensitive personal data when you use the BIMba XR mobile application ("**Application**").

Our Commitment: Sarvayaan is committed to protecting your privacy and ensuring transparency about our data practices. We comply with:

- **Information Technology Act, 2000** and associated Rules
- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011**
- **Information Technology (Intermediaries Guidelines and Digital Ethics Code) Rules, 2021**
- **Digital Personal Data Protection Act, 2023** (once notified)
- **Consumer Protection Act, 2019**
- All applicable Indian laws and regulations

By using the BIMba XR Application, you acknowledge that you have read and understood this Privacy Policy and agree to the collection and use of your information as described.

2. DEFINITIONS

Personal Data: Information that identifies you or can be used to identify you, including:

- Name, email address, phone number
- Device identifiers and unique IDs
- IP address and location data
- Account credentials and passwords

Sensitive Personal Data: As defined under IT Rules, 2011, includes:

- Passwords
- Financial information (bank accounts, payment details)
- Biometric data (facial recognition, fingerprints, iris scans)
- Health data and medical records

- Sexual orientation
- Official identifiers (Aadhaar, PAN, passport numbers)

Processing: Any operation performed on personal data, including collection, storage, use, sharing, deletion, or retention.

Data Controller: Sarvayaan (the entity that determines purposes and means of processing).

Data Processor: Third-party service providers authorized to process data on behalf of Sarvayaan.

User Consent: Affirmative action giving permission to process personal or sensitive personal data.

3. INFORMATION WE COLLECT

3.1 Information You Provide Directly

Account Registration:

- Full name and email address
- Phone number (optional)
- User profile information (company name, designation)
- Password and authentication credentials
- Profile picture or avatar (optional)
- Address and city (optional)

Project and Workspace Data:

- 3D models and files you upload or create
- Project metadata (project name, description, location, dates)
- Annotations, notes, measurements, and comments
- Collaboration permissions and team member assignments
- Project budget and cost data (if applicable)

Communication Data:

- In-app messages and communications
- Support requests, feedback, and inquiries
- Customer service chat logs
- Survey responses and user feedback
- Inquiry history and documentation

Payment Information (if applicable):

- Billing address and phone number
- Payment method details (last 4 digits of card, card type)

- Transaction history and invoice records
- Subscription information and billing cycle
- Refund and cancellation requests
- GST/Tax identification information

Voluntary Information:

- Additional information you choose to provide
- Document uploads or attachments
- Voice or video messages (if feature is available)

3.2 Information Collected Automatically

Device Information:

- Device type, model, manufacturer (e.g., Samsung, OnePlus)
- Operating system and version
- Device identifiers (IDFA, Android Advertising ID)
- Screen resolution and device specifications
- Mobile network provider and signal strength
- Device storage capacity

Usage Information:

- Features accessed and frequency of use
- Specific actions performed within the Application
- Time spent on features or screens
- Navigation patterns and user journey
- Session duration and frequency of use
- Crash reports and error logs
- Performance metrics and analytics
- Search queries within the Application

Location Information:

- Precise GPS coordinates (when location services enabled)
- Approximate location based on IP address
- Location history associated with projects (if enabled)
- Geofencing triggers for location-based features
- City/region derived from IP or GPS

Camera and AR Data (processed locally by default):

- Images captured through AR camera (stored locally only unless saved by user)

- AR environment mapping and spatial data
- 3D point clouds and environmental data
- Device orientation and pose tracking
- Lighting conditions and environmental parameters
- Surface detection data

Biometric Data (where applicable):

- Facial recognition data (processed locally on device, not transmitted unless user explicitly enables)
- Eye-tracking data for AR interactions (local processing only)
- Voice data from voice commands or notes (encrypted end-to-end)
- Fingerprint data (if used for authentication)

Sensor and Motion Data:

- Accelerometer readings
- Gyroscope data
- Magnetometer measurements
- Ambient light sensor data
- Motion tracking for gesture recognition
- Device shake/vibration data

Communication Metadata:

- IP address and connection timestamp
- HTTP headers and request/response data
- Bandwidth and data usage
- Network type (WiFi, 4G, 5G)
- Connection duration and frequency

3.3 Information from Third Parties

Authentication Providers:

- Data from Google Account sign-in (name, email, profile picture, unique ID)
- Data from other third-party authentication services (Microsoft, Apple ID)

Third-Party Integrations:

- Data from integrated cloud storage (Google Drive, OneDrive, Dropbox)
- Data from CAD/BIM software integrations (AutoCAD, Revit, Sketchup)
- Data from collaboration tools (Microsoft Teams, Slack)
- Project data shared through third-party services

Analytics and Service Providers:

- Crash reporting data from Firebase Crashlytics
- Usage analytics from Google Analytics and Firebase
- Payment data from Google Play Billing and payment processors
- Marketing and advertising performance data

Data from Others:

- Information shared about you by other users (e.g., if invited to a project)
- Feedback or reviews you receive from team members
- Information from support tickets involving other users

4. PURPOSES OF DATA COLLECTION AND PROCESSING**4.1 Core Functionality**

- To provide, maintain, and improve the BIMba XR Application
- To deliver AR visualization and 3D model viewing capabilities
- To store and synchronize your projects across devices
- To enable collaboration between team members
- To process and render spatial data and environmental information
- To provide technical support and troubleshooting

4.2 Communication and Support

- To send account notifications and alerts
- To respond to support requests and inquiries
- To provide customer service and technical assistance
- To send updates about features, maintenance, or service changes
- To communicate changes to Terms, Privacy Policy, or features
- To send security notifications and alerts
- To verify account ownership and prevent fraud

4.3 Personalization and Optimization

- To customize your user experience based on preferences
- To remember your account settings and preferences
- To provide feature recommendations
- To optimize Application performance for your device
- To improve AR tracking accuracy and visual quality

- To customize AR visualization based on your device capabilities

4.4 Analytics and Improvement

- To analyze how users interact with the Application
- To understand usage trends and patterns in India
- To identify and fix bugs, errors, and performance issues
- To develop new features based on user demand
- To conduct A/B testing and user experience research
- To optimize Application stability, speed, and reliability
- To understand which features are most valuable to users

4.5 Security and Fraud Prevention

- To verify your identity and authenticate your account
- To detect, prevent, and investigate fraud and abuse
- To enforce our Terms and Conditions
- To protect the security and integrity of our systems
- To investigate suspicious activity or security breaches
- To comply with legal obligations and requests from authorities
- To prevent unauthorized access and data theft

4.6 Legal and Regulatory Compliance

- To comply with the Information Technology Act, 2000 and Rules 2011
- To comply with Digital Personal Data Protection Act, 2023
- To respond to court orders, subpoenas, or legal requests
- To maintain records as required by tax and accounting laws
- To fulfill regulatory requirements and licensing obligations
- To respond to requests from law enforcement or government authorities
- To protect our legal rights and defend against claims

4.7 Business Operations

- To process payments and billing
- To generate invoices and tax documentation
- To manage subscriptions and renewals
- To conduct customer satisfaction surveys
- To maintain customer records and account history
- To manage employee and team permissions

5. LEGAL BASIS FOR DATA PROCESSING

Under Indian law, we process your personal data based on:

Contractual Performance:

- Processing necessary to provide the Application and services you request
- Fulfilling subscription or payment obligations
- Delivering services as per your agreement

Consent:

- Explicit, informed consent for optional features (location, biometric, voice)
- Consent for marketing communications (can be withdrawn anytime)
- Consent for sensitive personal data processing

Legal Obligation:

- Compliance with Information Technology Act, 2000
- Compliance with tax and accounting regulations
- Response to lawful government requests
- Compliance with consumer protection laws

Legitimate Interests:

- Improving our services and user experience
- Detecting and preventing fraud
- Ensuring system security and integrity
- Business analytics and optimization
- Defending legal claims

Vital Interests:

- Protecting your health and safety
- Emergency situations requiring immediate response

Public Interest:

- Activities in public interest
- Compliance with regulatory requirements

6. DATA SHARING AND DISCLOSURE

6.1 Sharing with Service Providers

We share your data with trusted third-party service providers who assist in operating the Application. These include:

Infrastructure and Hosting:

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Analytics and Monitoring:

- Google Firebase (Analytics, Crashlytics)
- Mixpanel or similar analytics platforms
- Sentry (error tracking)

Payment and Billing:

- Google Play Billing
- Stripe or similar payment processors
- Tax and accounting service providers

Communication:

- Email service providers
- SMS gateway providers
- Push notification services

Customer Support:

- Zendesk or similar support platforms
- Customer relationship management (CRM) systems

Data Security:

- Backup and disaster recovery providers
- Cybersecurity service providers

Contractual Obligations: All service providers are:

- Contractually bound to use data only for specified purposes
- Required to maintain appropriate security and confidentiality
- Prohibited from selling or disclosing data to unauthorized parties
- Subject to our data protection requirements
- Audited for compliance with data protection standards

6.2 Collaboration and Shared Access

If you use collaborative features:

- Project data and files are shared with team members you explicitly invite
- Team members' profile information is visible to others in the project
- The scope of shared data is determined by your permission settings
- You can manage access permissions in the Application

6.3 Third-Party Integrations

If you connect the Application to third-party services:

- Your data is shared according to the integration settings
- Integration partners' privacy policies govern their use of data
- You retain control over the scope of data sharing
- You can disconnect integrations anytime

6.4 Legal Requests and Compliance

We may disclose your personal data when required by Indian law or legal process, including:

- Court orders, subpoenas, or legal investigations
- Requests from law enforcement agencies
- Requests from central or state government authorities
- Protection of our legal rights and property
- Prevention of fraud or security threats
- Compliance with statutory obligations

Transparency: When legally permitted, we will notify you of legal requests to disclose your data.

6.5 Data We Do NOT Share

- We do NOT sell your personal data to third parties for marketing
- We do NOT share sensitive personal data (biometric, financial) with unauthorized parties
- We do NOT disclose location history without your explicit consent
- We do NOT share voice or camera data with advertisers
- We do NOT monetize your personal data through data brokers
- We do NOT share data with political parties or candidates
- We do NOT enable targeted harassment or discrimination through data sharing

6.6 Aggregated and Anonymized Data

We may share aggregated, de-identified, or anonymized data that cannot reasonably identify you with:

- Research institutions and universities
- Industry analysts and consultants
- Marketing partners (anonymized only)
- Government agencies (for statistical purposes)

7. DATA SECURITY

7.1 Technical Security Measures

Encryption in Transit:

- TLS 1.2 or higher encryption for all data transmission
- HTTPS protocol for all web communications
- Secure protocols for API communications

Encryption at Rest:

- AES-256 encryption for sensitive data stored on servers
- Encrypted database fields for critical information
- Secure key management and rotation

Access Controls:

- Role-based access control (RBAC)
- Multi-factor authentication for accounts
- Strong password requirements and enforcement
- Session timeout and automatic logout

Network Security:

- Firewalls and intrusion detection systems
- Network segmentation and isolation
- DDoS protection and mitigation
- Regular penetration testing

Biometric Security:

- Biometric data processed locally on device when possible
- No transmission of raw biometric data
- Device-level encryption for stored biometric templates
- Compliance with device manufacturer security standards

7.2 Administrative Security Measures

Personnel Security:

- Employees receive data protection and privacy training
- Confidentiality and non-disclosure agreements
- Background checks for employees with data access
- Limited access based on job role necessity

Access Management:

- Authorization required for all data access
- Logging and monitoring of data access
- Regular audit of access permissions
- Immediate removal of access upon termination

Organizational Measures:

- Data protection and privacy policies
- Incident response procedures
- Data breach notification protocols
- Regular security audits and assessments

7.3 Physical Security Measures

Data Centers:

- Secure, monitored facilities with physical access controls
- Video surveillance and entry logging
- Environmental controls (fire, flood, temperature)
- Redundant power and cooling systems

Device Management:

- Secure disposal of devices containing personal data
- Asset tracking and inventory management
- Secure destruction of data before device reuse

7.4 Security Limitations

Despite our security measures, **no system is completely secure**. We cannot guarantee:

- Absolute protection against all cyberattacks
- Prevention of all unauthorized access attempts
- Protection from sophisticated hacking attempts

- Security against state-sponsored attacks

Your Responsibility:

- Maintain confidentiality of account credentials
- Do not share your password
- Secure your device with lock screen and encryption
- Use secure networks (avoid public WiFi for sensitive operations)
- Keep your device and Application updated
- Report suspicious activity immediately

8. DATA RETENTION

Your personal data is retained based on the purposes for which it was collected and applicable legal requirements:

Data Type	Retention Period	Reason
Account Information	During active use + 30 days post-deletion	Account recovery and legal obligations
Project Files	As long as account is active	Service delivery; deleted upon account deletion
Usage Analytics	24 months	Service improvement and optimization
Payment Records	7 years	Tax, GST, and accounting compliance (per Income Tax Act)
Support Tickets	3 years	Legal reference and dispute resolution
Backup Data	90 days	Disaster recovery purposes
Security Logs	12 months	Incident investigation and forensics
Marketing Data	Until opt-out	Marketing communication purposes; deleted on unsubscribe
Biometric Data	Stored locally on device	Not transmitted or retained on servers

Early Deletion: You can request deletion of your data anytime through your account settings, subject to legal retention requirements. We will process deletion requests within **30 days**.

Retention After Deletion:

- Backup copies retained for 90 days for recovery purposes
- Legal and tax records retained per statutory requirements
- Aggregated/anonymized data retained indefinitely (cannot identify you)
- Legal obligations may require extended retention

9. YOUR PRIVACY RIGHTS

Under Indian law, you have the following rights:

9.1 Right to Access

You have the right to request access to your personal data and receive:

- A copy of all personal data we hold about you
- Information about the purposes of processing
- Details of recipients and categories of recipients
- The retention period for your data
- Your other privacy rights

How to Exercise: Send a written request to privacy@sarvayaan.com with subject line "**Right of Access Request**" along with identity proof. We will respond within **30 days**.

Portable Format: You can request your data in a portable, machine-readable format (CSV, JSON) for data portability.

9.2 Right to Correction/Rectification

You have the right to request correction of inaccurate, incomplete, or outdated personal data:

- We will correct data within **15 days** of verification
- Inaccuracy will be notified to third parties with whom data was shared
- You can update your account information directly through the Application

9.3 Right to Erasure and Deletion

You have the right to request deletion of your personal data in cases where:

- Data is no longer necessary for the purposes it was collected
- You withdraw consent and no other legal basis exists
- You object to processing and no compelling interest exists
- Data has been processed unlawfully

Limitations: We may not delete data if:

- Required by law (tax records, legal obligations)
- Necessary for fulfilling contractual obligations
- Required for establishing, exercising, or defending legal claims
- Necessary for security or integrity of the system

Process: Send deletion request to privacy@sarvayaan.com with subject "**Right to Erasure Request**". We will respond within **30 days**. Data will be deleted within 30 days post-verification, except where legal retention applies.

9.4 Right to Restrict Processing

You can request us to restrict (limit) processing of your data:

- While we verify accuracy of contested data
- If processing is unlawful but you object to deletion
- If we no longer need data but you need it for legal purposes
- If you object to processing and we verify your interests

Effect: Restricted data is marked and only processed for storage, legal claims, or with your consent.

9.5 Right to Object

You have the right to object to processing of your personal data:

- **Marketing Communications:** Can opt out by clicking "Unsubscribe" in emails or adjusting notification settings
- **Behavioral Analytics:** Can disable analytics through settings
- **Targeted Advertising:** Can adjust ad preferences in Google Play settings
- **Profiling:** Can request we stop profiling for decision-making

Process: Email privacy@sarvayaan.com with "**Objection Request**" and we will comply within **7 days** (except where legal obligations require continued processing).

9.6 Right to Data Portability

You have the right to receive your personal data in a structured, commonly used, machine-readable format and transmit it to another service provider:

- Includes account information, projects, and communications
- Excludes third-party IP and system-generated data
- Format: CSV, JSON, or other standard format
- Available within **30 days** of request

9.7 Right to Withdraw Consent

If we rely on your consent for processing:

- You can withdraw consent anytime
- Withdrawal is as easy as initial consent
- Does not affect lawfulness of processing before withdrawal
- Withdraw through: account settings, email, or written request

9.8 Right to Appeal

If you believe we have not honored your rights:

- You can appeal to our Data Protection Officer
- Escalate to the National Data Protection Authority (post-notification of DPDPA)
- File a complaint with the Information Commissioner of India
- Approach consumer courts under Consumer Protection Act

9.9 Right Against Discrimination

You have the right not to be discriminated against for:

- Exercising any of the above rights
- Refusing to provide optional data
- Opting out of marketing communications

We will not:

- Refuse service based on exercise of privacy rights
- Charge different prices for exercising rights
- Provide inferior quality of service
- Limit functionality improperly

10. CHILDREN'S PRIVACY AND MINORS

10.1 Age Restrictions

BIMba XR is intended for users aged 18 years and above.

Younger Users:

- Ages 13-17: Permitted with verifiable parental/guardian consent
- Under 13: Not permitted to use the Application

10.2 Parental Consent

For users aged 13-17:

- **Verifiable Parental Consent:** Parent/guardian must provide written consent
- **Parent Responsibility:** Parent/guardian is responsible for all terms and liabilities
- **Parent Rights:** Parents can:
 - Review child's account and data
 - Request access to or deletion of child's data

- Revoke consent and terminate child's use
- Update consent preferences
- **Consent Mechanism:** Email parent/guardian with verification code and consent form; parent must respond with verification

10.3 Data Collection for Minors

For users aged 13-17, we:

- Collect only essential data necessary for functionality
- Limit tracking and analytics data
- Do NOT enable behavioral advertising or targeted ads
- Do NOT enable biometric features without explicit parental consent
- Do NOT share data with third-party advertisers
- Do NOT use profiling for decision-making
- Restrict location tracking features
- Do NOT enable voice/camera features without parental consent

10.4 Parental Safeguards

For minor users, we provide:

- Option to disable notifications
- Limited feature access based on age
- Age-appropriate content only
- Parental controls through device settings
- Safe browsing defaults
- Option to restrict in-app purchases

10.5 COPPA Compliance (Where Applicable)

BIMba XR complies with industry standards for child online privacy. Parents can:

- Request access to child's personal data
- Request correction of inaccurate data
- Request deletion of child's personal data
- Withdraw consent and request termination

10.6 Reporting Minors' Use

If you become aware of a child under 13 using BIMba XR:

- **Immediately contact:** support@sarvayaan.com
- **Include:** Child's account details and reason for concern
- **We will:** Promptly investigate and take corrective action

11. COOKIES AND TRACKING TECHNOLOGIES

11.1 Cookies Used

The Application may use cookies for:

- **Session Management:** Maintaining your login session
- **Preferences:** Remembering your settings and preferences
- **Analytics:** Understanding usage patterns
- **Security:** Detecting and preventing fraud
- **Functionality:** Enabling core features

11.2 Cookie Types

Essential Cookies:

- Required for basic functionality and security
- Cannot be disabled without losing core features
- Session tokens and authentication cookies
- CSRF protection tokens

Performance/Analytics Cookies:

- Google Analytics cookies
- Firebase analytics cookies
- Crash reporting cookies
- Performance metrics collection

Preference Cookies:

- Remember your language preference
- Remember your display settings
- Remember notification preferences

Targeting/Advertising Cookies:

- Google Ad Manager (if ads are displayed)

- Third-party advertising networks
- Behavioral targeting (if applicable)

11.3 Third-Party Tracking

Third-party services may place cookies:

- **Google Analytics:** google.com/privacy
- **Firebase:** firebase.google.com/support/privacy
- **Google Ads:** support.google.com/ads
- **Other Partners:** Specified in our partners list

11.4 Managing Cookies and Tracking

You can control cookies through:

- **Browser Settings:** Delete cookies, disable third-party cookies
- **Device Settings:** Disable ad tracking (Android: Settings > Google > Manage Google Account > Data & Privacy > "Manage your Google Activity")
- **Application Settings:** Disable analytics, adjust notification preferences
- **Do Not Track:** Enable "Do Not Track" signal in browser (if supported)
- **Opt-Out Services:** Use opt-out services like OptOutMyData.com

11.5 Local Storage

The Application may store data locally on your device:

- Project files and 3D models
- User preferences and settings
- Cached data for offline access
- Biometric templates (for authentication)

You can clear local storage through:

- Application Settings > Data
- Device Settings > Application Management
- Uninstalling and reinstalling the Application

12. INTERNATIONAL DATA TRANSFERS

Transfers Outside India:

If Sarvayaan transfers your personal data outside India:

- **Legal Framework:** Transfers comply with the Information Technology Act, 2000 and Rules 2011

- **Adequacy Determination:** Only to jurisdictions with adequate data protection levels
- **Contractual Safeguards:** Standard contractual clauses (SCCs) are in place
- **Standard Terms:** BCR (Binding Corporate Rules) where applicable
- **Your Consent:** You consent to international transfers by accepting this Policy

Participating Countries:

- European Union member states (GDPR adequate)
- United States (Privacy Shield or Standard Contractual Clauses)
- United Kingdom, Canada, Australia (adequacy or SCCs)
- Other countries with data protection agreements

Data Subject Rights: Your rights are protected even after international transfer through contractual obligations.

13. THIRD-PARTY LINKS AND SERVICES

The Application may contain links to third-party websites, applications, or services. **This Privacy Policy does NOT apply to third-party services.**

Sarvayaan is NOT responsible for:

- Privacy practices of third-party services
- Content, accuracy, or legality of third-party sites
- Data collection practices of third parties
- Security of third-party systems
- Changes to third-party privacy policies

Your Responsibility:

- Review third-party privacy policies before providing information
- Understand third-party terms and conditions
- Evaluate third-party security practices
- Report privacy concerns to the third party directly

14. CALIFORNIA PRIVACY RIGHTS (CCPA/CPRA)

If you are a California resident, you have rights under the California Consumer Privacy Act (CCPA) and California Privacy Rights Act (CPRA):

14.1 Right to Know

You can request:

- What personal information is collected about you
- How your information is used
- What categories of information are shared
- The sources of your information

14.2 Right to Delete

You can request deletion of personal information we have collected, except where exceptions apply (contractual necessity, legal obligations).

14.3 Right to Correct

You can request correction of inaccurate personal information.

14.4 Right to Opt-Out

You can opt out of:

- Sale or sharing of personal information (we do not sell data)
- Targeted advertising
- Profiling and automated decision-making

14.5 Right to Limit Use

You can request we limit use of sensitive personal information to necessary purposes only.

14.6 Non-Discrimination

We will not discriminate against you for exercising CCPA rights:

- No denial of service
- No different pricing or terms
- No retaliation for rights exercise

Process: Email privacy@sarvayaan.com with "CCPA Request" and include your California address. We will respond within 45 days.

15. PRIVACY INCIDENTS AND DATA BREACHES

15.1 Breach Response

In the event of a data breach, we will:

- **Immediately investigate** the breach
- **Contain and remediate** the unauthorized access
- **Notify affected individuals** without unreasonable delay
- **Notify authorities** as required by law (CERT-IN, police, etc.)
- **Maintain incident records** for regulatory review

15.2 Breach Notification

We will notify you of significant breaches by:

- **Email** to your registered email address
- **In-app notification** with details of the breach
- **Website notification** posted prominently
- **Within 72 hours** (as per IT Rules 2011) or as legally required

Notification Content:

- Nature and scope of the breach
- Data categories affected
- Likely consequences
- Measures taken or recommended
- Contact information for further details

15.3 Your Rights in Case of Breach

- Right to compensation for losses
- Right to claim damages under IT Act, 2000
- Right to file consumer complaint
- Right to notify Credit Information Bureau (if financial data breached)
- Right to legal action

16. MODIFICATION OF PRIVACY POLICY

Sarvayaan may update this Privacy Policy to reflect:

- Changes in our data practices
- New technologies or features
- Changes in Indian law or regulations
- Feedback from users or regulators

- Business developments

16.1 Effective Changes

Material Changes require:

- At least **30 days' advance notice** via email or in-app notification
- Clear description of what has changed
- Your acknowledgment before continued use
- Option to opt-out or delete account before changes take effect

Minor Changes (clarifications, corrections) are effective immediately with notice.

16.2 Continued Use

Your continued use of the Application after notification of changes indicates your acceptance of the updated Privacy Policy. If you do not agree, you must discontinue use.

17. DATA PROTECTION OFFICER AND CONTACT INFORMATION

For all privacy-related inquiries, requests, or concerns:

Sarvayaan - BIMba XR Privacy Team

Email: privacy@sarvayaan.com

Support Email: support@sarvayaan.com

Website: www.sarvayaan.com

Registered Address: [To be inserted - Registered office address in India]

Phone: [To be inserted - Contact number in India]

Data Protection Officer (if appointed):

Name: [To be inserted]

Email: [To be inserted]

Contact: [To be inserted]

Response Commitment: We will respond to all privacy inquiries and requests within **7-30 days** depending on complexity.

18. REGULATORY COMPLIANCE

18.1 Information Technology Act, 2000

Sarvayaan complies with:

- IT Act Section 43 (damage to computer resources)
- IT Act Section 66 (computer-related offenses)
- IT Rules 2011 (sensitive personal data protection)

- IT(Intermediaries Guidelines) Rules 2021 (content moderation)

18.2 Digital Personal Data Protection Act, 2023

Upon notification of DPDPA 2023, we comply with:

- Consent-based processing model
- Privacy by design and default
- Rights of data subjects
- Obligations of data fiduciaries
- Data Protection Board authority
- Cross-border transfer restrictions

18.3 Consumer Protection Act, 2019

You have rights under Consumer Protection Act:

- Right to information about service terms
- Right to seek redressal for defective service
- Right to compensation for loss or damage
- Access to consumer dispute redressal forums (District, State, National)

18.4 Other Applicable Laws

- **Bharatiya Nyaya Sanhita, 2023** (criminal provisions)
- **State data protection laws** (where applicable)
- **Tax laws** (GST, Income Tax Act)
- **Employment laws** (if employer data processing)
- **Telecom regulations** (NTC, TRAI guidelines)

19. YOUR CHOICES AND CONTROL

You have control over:

Data/Feature	Your Control
Notifications	Disable in app settings or device settings
Location Services	Enable/disable in device settings
Camera Access	Enable/disable in device settings
Microphone Access	Enable/disable in device settings
Contacts Access	Enable/disable in device settings
Biometric Features	Enable/disable in app settings

Data/Feature	Your Control
Analytics Tracking	Opt-out in app settings
Advertising Personalization	Disable in Google Play settings
Marketing Emails	Unsubscribe via link or settings
Data Retention	Request deletion anytime
Account Deletion	Delete account through settings
Data Download	Download your data via settings

20. SUPERVISORY AUTHORITIES AND GRIEVANCE REDRESSAL

20.1 Indian Authorities

If you believe your privacy rights have been violated:

Information Commissioner of India (ICoI)

- Under Right to Information Act, 2005
- File complaint for information access issues
- Website: rti.gov.in

Consumer Protection Authority

- District Consumer Commission (up to ₹1 Crore)
- State Consumer Commission (₹1-10 Crore)
- National Consumer Commission (above ₹10 Crore)
- File complaint for defective service or unfair trade practices

Data Protection Authority (when DPDPA 2023 is notified)

- National Data Protection Authority (NDPA)
- File complaint for data protection violations
- Seek remedies and compensation

Law Enforcement

- Local police (for cybercrimes)
- CBI Cyber Cell (for serious cybercrimes)
- CERT-IN (Indian Computer Emergency Response Team)

20.2 Grievance Redressal Process

Step 1 - Internal Complaint

- Email: grievances@sarvayaan.com
- Include: Details of complaint, impact, requested remedy
- Timeline: We respond within **7 business days**

Step 2 - Escalation

- If unsatisfied, escalate to: support@sarvayaan.com
- Timeline: Response within **15 business days**

Step 3 - External Remedies

- Consumer Commission complaint
- National Data Protection Authority (post-notification)
- Police/law enforcement for criminal violations

21. DEFINITIONS AND INTERPRETATIONS

Application: The BIMba XR mobile software available on Google Play and other platforms.

Sarvayaan: The company registered in India that owns and operates BIMba XR.

Processing: Any operation on personal data (collection, storage, use, sharing, deletion, etc.).

Personal Data: Information identifying a person (name, email, IP address, device ID, etc.).

Sensitive Personal Data: Data categories requiring higher protection (passwords, biometric data, financial information, health data).

Data Controller: The entity determining how and why data is processed (Sarvayaan).

Data Processor: Third-party services processing data on behalf of the controller.

Consent: Affirmative, informed permission to process data.

Processing Lawfully: Data processing is compliant with applicable law and this Privacy Policy.

Data Subject: The person to whom personal data relates (you).

Third Party: Entity other than you or Sarvayaan.

22. ACKNOWLEDGMENT AND CONSENT

By downloading and using BIMba XR, you:

- Acknowledge that you have read this entire Privacy Policy
- Understand how your data is collected and used
- Consent to the processing of your personal data as described
- Agree that you have the legal capacity to provide consent
- Accept that your information may be transferred internationally with safeguards
- Understand the security measures we implement
- Accept the limitations of our liability

Parental Consent (for minors 13-17): Parents/guardians acknowledge they have read this Policy and consent to their child's use and data processing.

23. CONTACT US

For any questions about this Privacy Policy:

Sarvayaan - BIMba XR Team

Primary Contact:

Email: privacy@sarvayaan.com

Phone: [To be inserted]

Website: www.sarvayaan.com

Escalation:

Email: grievances@sarvayaan.com

Address: [To be inserted - Registered office in India]

Business Hours: Monday-Friday, 9:00 AM - 6:00 PM IST

Response Time: 7-30 days depending on complexity

Document Version: 1.0

Effective Date: November 24, 2025

Last Updated: November 24, 2025

Jurisdiction: India

Status: Ready for Google Play Deployment in India

This Privacy Policy has been prepared in compliance with the Information Technology Act, 2000, Information Technology Rules 2011, Digital Personal Data Protection Act 2023 (upon notification), Consumer Protection Act 2019, and all applicable Indian laws and regulations.

Customization Required Before Deployment:

- *Insert registered company address in India*
- *Insert contact phone number (India-based)*

- *Insert Data Protection Officer details (if appointed)*
- *Insert grievance contact person details*
- *Review and update jurisdiction-specific clauses as needed*