

Welcome to **Maxora Keystone Vendor**. Your privacy is paramount to us. This policy outlines our practices for collecting, using, and protecting the personal and business information you provide while using our mobile application.-----1. Data Collection

We collect information necessary to provide and secure our vendor services:A. Vendor and Business Information

When you register, we collect:

- **Account Details:** Your name, username, email address, and profile picture.
- **Business Profile:** Your business name, category, physical address (City, State), and operating hours.
- **Referral Data:** Any referral codes used during your sign-up.

B. Verification Data (KYC)

For legal compliance and business verification, we collect:

- Selected identity verification documents.
- Business license or tax registration documentation.
- Photographs of the business premises.

C. Financial and Transaction Data

As a payment-handling vendor portal, we process:

- **Transaction History:** Records of invoices, receipts, and payment methods.
- **Maxora Wallet Data:** Your wallet balance and transaction activity.
- **Payout Details:** Necessary information for processing withdrawals to your bank account.

D. Device and Usage Data

- **Location:** We request access to your GPS location to accurately set your business on the map.
- **Media Access:** Camera and photo library access for uploading KYC documents and business images.
- **Notifications:** Device tokens are used to send essential real-time updates (orders, payments, policy changes).

-----2. Use of Your Information

We utilize the collected data for the following core functions:

- **Service Delivery:** Managing your profile and facilitating all business transactions within the app.
- **Identity Verification:** Conducting the mandatory KYC process to ensure legitimacy.
- **Financial Processing:** Managing withdrawals, top-ups, and generating digital customer receipts.
- **Communication:** Sending important updates through Socket.IO and local alerts.
- **Security & Integrity:** Preventing fraud and protecting the overall health of the Maxora ecosystem.

-----3. Data Sharing and Third Parties

We commit to *not selling* your data. We only share information with trusted partners required for the application's functionality:

- **Google Services:** For authentication (Sign-In) and mapping features (Maps).
- **Payment Processors:** Services like **Razorpay** for secure financial transaction processing.
- **Cloud Infrastructure:** Your data is securely hosted on our proprietary servers (softsoveapi.cloud).

-----4. App Permissions

The application will explicitly request the following device permissions:

- **Location:** To accurately display your business location on the customer-facing map.
- **Camera:** For taking photos for KYC and business profile uploads.
- **Photo Library:** To upload existing business images.
- **Microphone:** For potential use in video-based verification or business content (if introduced).

-----5. Data Security

We employ industry-standard security measures to safeguard your information:

- **Data Encryption:** SSL/TLS is used to encrypt data transferred to our APIs.
- **Secure Sessions:** Token-based authentication secures all vendor sessions.
- **Data Protection:** We utilize standard non-exempt encryption for data protection at rest.

-----6. Data Retention and Deletion

We retain your data as long as your vendor account is active, or as legally required for financial auditing and tax purposes. You have the right to request account deletion via the app settings or by contacting our support team.-----7. Policy Updates

This Privacy Policy may be updated periodically. We will notify you of any significant changes by posting the revised policy on this page and updating the "Effective Date" at the top.-----8.
Contact Information

For any questions regarding this Privacy Policy, please reach out to us:

- **Email:** care@maxorakeystone.com
- **Support Portal:** Located within the "Vendor Support" section of the application.