Privacy Policy

Effective Date: June 1, 2026

Last Updated: June 1, 2026

1. Introduction & Scope

This Privacy Policy describes how Orbita LLC and its affiliates (collectively, "Axra," "we," "us," or "our") collect, use, disclose, and protect your personal information when you use our agentic banking and payments infrastructure services.

Axra provides multi-currency wallets, stablecoin management, international transfers, virtual accounts, and payment processing services for individuals, businesses, and platforms through various channels including web applications, WhatsApp, and Telegram bots.

Important: Axra is not a bank. Banking services are provided through our licensed partner financial institutions.

This Privacy Policy applies to all users of Axra services, regardless of geographic location, and explains:

- What personal information we collect
- How we collect and use that information
- With whom we share your information
- How we protect your information
- Your rights regarding your personal information
- How to contact us with privacy concerns

By using Axra services, you acknowledge that you have read and understood this Privacy Policy. If you do not agree with our practices, please do not use our services.

2. Who We Are

Axra services are operated by the following legal entities (collectively, the "Data Controllers"):

Orbita LLC.

- **Jurisdiction:** Wyoming, United States
- **Contact:**
  - Address: 30 N Gould St Ste R Sheridan, WY 82801

For the purposes of the EU General Data Protection Regulation (GDPR), the Canadian Personal Information Protection and Electronic Documents Act (PIPEDA), and the California Consumer Privacy Act (CCPA), the relevant entity in your jurisdiction acts as the data controller for your personal information.

3. Information We Collect

We collect several categories of personal information, which we classify by sensitivity level for security and compliance purposes:

3.1 High Sensitivity Financial Information

- Bank account numbers and IBANs
- Virtual account details
- Payment card information (tokenized)
- Transaction amounts and histories
- Wallet balances (fiat and cryptocurrency)
- Beneficiary account details
- Transfer instructions and confirmations
- Sanctions screening results

3.2 High Sensitivity Identity Information

- Full legal name
- Email address
- Phone number
- Physical address
- Date of birth
- Government-issued identification documents (passport, driver's license, national ID)
- Biometric data collected during identity verification
- Taxpayer identification numbers (where required)
- Account passwords and PINs (stored as cryptographic hashes only)
- Authentication tokens and session credentials
- Know Your Customer (KYC) verification records
- Proof of address documents

3.3 Medium Sensitivity Behavioral Information

- AI agent conversation history and chat messages
- User preferences and settings
- Service usage patterns
- AI memory data (contextual information to personalize your experience)
- Feature adoption metrics
- Customer support interactions

3.4 Low Sensitivity Linking Information

- Messaging platform identifiers (Telegram user ID, WhatsApp phone number)
- Beneficiary display names
- Device identifiers
- IP addresses
- Browser type and version
- Operating system information
- Referrer URLs
- Time zone and locale settings

3.5 Technical and Security Information

- Access logs (with personally identifiable information removed)
- Audit trail records
- Security incident data
- Fraud prevention signals
- Risk assessment scores
- Two-factor authentication settings

4. How We Collect Information

4.1 Information You Provide Directly

We collect information when you:

- Register for an Axra account
- Complete identity verification (KYC)
- Add bank accounts or payment methods
- Initiate transactions or transfers
- Communicate with our AI agents via WhatsApp, Telegram, or web chat
- Contact customer support
- Update your account settings or preferences
- Participate in surveys or promotional activities

4.2 Information Collected Automatically

When you use Axra services, we automatically collect:

- Device and browser information through standard web technologies
- Usage data and interaction patterns with our services
- IP addresses and geolocation data (country/region level)
- Session information and authentication events
- Transaction metadata (timestamps, channel used, success/failure status)

- Transaction metadata (timestamps, channel used, success/failure status)
- Performance and diagnostic data

4.3 Information from Third Parties

We receive information from:

- **Identity Verification Providers:** KYC data and verification results from Persona (integrated through Bridge.xyz)
- **Banking Partners:** Account verification, transaction status updates, and compliance alerts from licensed financial institutions
- **Payment Infrastructure Providers:** Transaction processing data from Bridge.xyz
- **Sanctions Screening Services:** Watchlist screening results from dilisense (covering OFAC, UN, EU, HMT, and 75+ additional sanctions lists)
- **Messaging Platforms:** User identifiers and message routing information from Telegram and WhatsApp
- **Credit Bureaus and Fraud Prevention Services:** Risk assessment data where permitted by law

4.4 Information from Public Sources

We may collect information from publicly available sources to:

- Verify your identity
- Conduct sanctions and adverse media screening
- Prevent fraud and financial crime
- Comply with legal obligations

5. Legal Bases for Processing

Under applicable data protection laws (including GDPR Article 6), we process your personal information based on the following legal grounds:

5.1 Performance of Contract (GDPR Art. 6(1)(b))

Processing necessary to provide Axra services you have requested, including:

- Account creation and management
- Transaction processing and settlement
- Customer support and service communications
- Service feature delivery

5.2 Legal Obligation (GDPR Art. 6(1)(c))

Processing required to comply with laws and regulations, including:

- Know Your Customer (KYC) and Customer Due Diligence (CDD) requirements
- Anti-Money Laundering (AML) and Counter-Terrorist Financing (CTF) obligations
- Sanctions screening and watchlist monitoring
- Financial record-keeping and reporting requirements
- Tax reporting obligations
- Regulatory inquiries and investigations
- Court orders and legal process

5.3 Legitimate Interests (GDPR Art. 6(1)(f))

Processing necessary for our or a third party's legitimate interests, where not overridden by your rights:

- Fraud prevention and security monitoring
- Risk assessment and management
- Service improvement and analytics
- Direct marketing (where permitted and with opt-out rights)
- Network and information security
- Business continuity and disaster recovery
- Internal audit and compliance monitoring

5.4 Consent (GDPR Art. 6(1)(a))

Where required by law or where we cannot rely on another legal basis, we obtain your explicit consent for:

- Processing sensitive personal data beyond what is legally required
- Marketing communications (where consent is required)
- Certain data sharing with third parties
- Optional service features that require additional data collection

You may withdraw consent at any time, which will not affect the lawfulness of processing based on consent before withdrawal.

5.5 Vital Interests (GDPR Art. 6(1)(d))

In rare circumstances, processing may be necessary to protect yours or another person's vital interests, such as preventing fraud or investigating suspected financial crimes that pose serious risks.

6. How We Use Your Information

We use your personal information for the following purposes:

6.1 Service Delivery and Account Management

- Create, maintain, and secure your Axra account
- Process and settle transactions, transfers, and payments

- Process and settle transactions, transfers, and payments
- Provide multi-currency wallet and virtual account services
- Manage stablecoin wallets and cryptocurrency operations
- Generate account statements and transaction histories
- Enable AI agent interactions across WhatsApp, Telegram, and web channels
- Personalize your service experience through AI memory features

6.2 Identity Verification and Compliance

- Verify your identity through KYC procedures
- Screen against sanctions lists and adverse media
- Monitor transactions for suspicious activity
- Comply with AML, CTF, and counter-proliferation financing requirements
- Respond to regulatory inquiries and legal process
- Maintain records as required by financial services regulations
- Conduct ongoing customer due diligence

6.3 Security and Fraud Prevention

- Authenticate your identity and authorize transactions
- Detect and prevent fraud, unauthorized access, and financial crimes
- Monitor for security threats and vulnerabilities
- Investigate and respond to security incidents
- Conduct risk assessments and scoring
- Implement multi-factor authentication and transaction confirmations

6.4 Communications

- Send transactional notifications (payment confirmations, account alerts)
- Provide customer support and respond to inquiries
- Send service updates and important account information
- Deliver marketing communications (with your consent or where permitted)
- Request feedback on your service experience
- Notify you of changes to our terms, policies, or services

6.5 Analytics and Service Improvement

- Analyze usage patterns to improve service features
- Develop new products and services
- Conduct research and data analysis
- Optimize AI agent performance and conversation quality
- Test and deploy service enhancements

- Measure marketing campaign effectiveness

6.6 Legal and Business Operations

- Enforce our Terms of Service and other agreements
- Resolve disputes and investigate complaints
- Maintain business records and audit trails
- Conduct internal audits and compliance reviews
- Manage business continuity and disaster recovery
- Evaluate and complete corporate transactions (mergers, acquisitions)

7. Data Sharing & Third Parties

We share your personal information with third parties only as described in this Privacy Policy. We do not sell your personal information to third parties.

7.1 Service Providers and Data Processors

We engage the following categories of service providers who process personal information on our behalf:

Financial Infrastructure and Banking Partners

- **Bridge.xyz:** Provides wallet infrastructure, virtual account services, payment processing, and KYC verification (including integration with Persona for identity verification). Processes customer profiles, bank account information, transaction data, and KYC records.
- **Licensed Banking Institutions:** Partner banks that provide underlying banking services, account custody, and payment settlement.

AI and Technology Services

- **Anthropic:** Provides AI language models for our conversational agent features. Anthropic's API is stateless and does not retain conversation data beyond the API call. We manage conversation history and AI memory data on our own infrastructure.
- **Cloud Infrastructure Providers:** Hosting, storage, and computing services for our applications and databases.

Compliance and Risk Management

- **dilisense:** Sanctions and watchlist screening service covering OFAC, UN, EU, HMT, and 75+ additional sanctions lists worldwide.
- **Identity Verification Providers:** Persona (via Bridge.xyz integration) for KYC document verification and biometric checks.
- **Fraud Prevention Services:** Third-party providers that help detect and prevent fraudulent transactions and account takeover attempts.

Communications Platforms

- **Telegram:** Messaging platform through which users access Axra services via bot interfaces. Telegram has access to message content transmitted through its platform.
- **WhatsApp:** Messaging platform through which users access Axra services via bot interfaces. WhatsApp/Meta has access to message content transmitted through its platform.
- **Email Service Providers:** Third-party services that deliver transactional and marketing emails on our behalf.

Analytics and Performance Monitoring

- **Analytics Providers:** Services that help us understand usage patterns and service performance (with personally identifiable information minimized or removed).
- **Application Performance Monitoring:** Tools that help us detect and resolve technical issues.

7.2 Legal and Regulatory Disclosures

We disclose personal information when required by law or to protect our rights:

- **Financial Regulators:** FinCEN, FINTRAC, Bank of Canada, and other financial regulatory authorities in jurisdictions where we operate.
- **Law Enforcement and Government Authorities:** When required by law, court order, subpoena, or legal process; to investigate suspected illegal activity; or to protect against fraud or threats to safety.
- **Tax Authorities:** Tax reporting information as required by applicable tax laws.
- **Legal and Professional Advisors:** Lawyers, accountants, auditors, and other professional advisors bound by confidentiality obligations.

7.3 Business Transfers

If Axra or any of its affiliates undergoes a merger, acquisition, bankruptcy, dissolution, reorganization, or similar transaction or proceeding, your personal information may be transferred to the successor entity, subject to this Privacy Policy.

7.4 With Your Consent

We may share your personal information with other third parties when you give us explicit consent to do so.

7.5 Aggregated and De-Identified Data

We may share aggregated, anonymized, or de-identified data that cannot reasonably be used to identify you with third parties for analytics, research, marketing, or other business purposes.

8. International Data Transfers

Axra operates globally with entities in the United States, Canada, Nigeria, and Rwanda. Your personal information may be transferred to, stored in, and processed in countries other than your country of

residence, including countries that may not provide the same level of data protection as your home country.

8.1 Transfers from the European Economic Area (EEA)

For users in the EEA, we implement appropriate safeguards for international transfers:

- **Adequacy Decisions:** Where available, we rely on European Commission adequacy decisions recognizing that certain countries provide adequate data protection.
- **Standard Contractual Clauses (SCCs):** We use EU Standard Contractual Clauses (also known as Model Clauses) approved by the European Commission for transfers to countries without adequacy decisions.
- **Additional Safeguards:** We conduct transfer impact assessments and implement supplementary measures (encryption, access controls, contractual protections) to ensure data protection in jurisdictions without adequate laws.

8.2 Transfers from Canada

For users in Canada, we comply with PIPEDA requirements for international transfers:

- We ensure comparable levels of protection through contractual commitments with service providers.
- We obtain consent where required for transfers to jurisdictions with materially different privacy protections.
- We inform you of the jurisdictions where your data may be processed.

8.3 Transfers from Other Jurisdictions

For users in other jurisdictions, we implement appropriate technical and organizational measures to protect personal information during international transfers, including encryption, access controls, and contractual data protection obligations.

8.4 Data Processing Locations

Your personal information may be processed in the following jurisdictions:

- **United States:** Primary data processing and storage, services provided by Bridge.xyz, Anthropic, and various cloud infrastructure providers.
- **Canada:** Canadian operations and customer support.
- **European Union:** Some service providers and data center locations.
- **Nigeria and Rwanda:** Local operations for customers in those markets.

9. Data Security

We implement comprehensive technical and organizational security measures to protect your personal information against unauthorized access, alteration, disclosure, or destruction.

9.1 Encryption and Cryptography

- **Data in Transit:** All data transmitted between your device and our services is encrypted using TLS 1.3 (Transport Layer Security) with perfect forward secrecy.
- **Data at Rest:** Sensitive database fields are encrypted using AES-256-GCM (Advanced Encryption Standard with Galois/Counter Mode), a military-grade encryption algorithm. Encrypted fields are marked with an "enc:" prefix in our databases.
- **Password and PIN Security:** Passwords and PINs are hashed using bcrypt with a cost factor of 12, ensuring that even if our databases were compromised, these credentials cannot be reversed or read. We never store plaintext passwords or PINs.

9.2 Access Controls and Authentication

- **Multi-Factor Authentication (MFA):** We require two-factor authentication using time-based one-time passwords (TOTP) for sensitive account operations.
- **Role-Based Access Control:** Internal access to personal information is restricted based on job function and the principle of least privilege.
- **Session Management:** Authentication tokens are stored in Redis with automatic expiration. Email verification tokens expire after 24 hours, password reset tokens after 1 hour, and transfer confirmation tokens after 15 minutes.
- **JWT Security:** Our JSON Web Tokens include `jti` (JWT ID) and `aud` (audience) claims to prevent token reuse and ensure tokens are only valid for their intended purpose.

9.3 Infrastructure Security

- **Secure Hosting:** Our infrastructure is hosted with security-certified cloud providers that maintain SOC 2 Type II and ISO 27001 compliance.
- **Network Security:** Firewalls, intrusion detection systems, and network segmentation protect our infrastructure from external threats.
- **Logging and Monitoring:** We maintain comprehensive audit logs for security events. Importantly, application logs contain only user UUIDs and never include personally identifiable information in plaintext.
- **Circuit Breakers:** Our Redis implementation includes circuit breaker patterns to ensure service resilience and prevent cascading failures.

9.4 Data Backup and Recovery

- **Daily Backups:** Database backups are performed daily and encrypted before storage in Cloudflare R2 object storage.
- **Disaster Recovery:** We maintain tested disaster recovery procedures to restore services and data in the event of a catastrophic failure.
- **Backup Retention:** Encrypted backups are retained according to our data retention schedule and regulatory requirements.

9.5 Application Security

- **Secure Development Practices:** Our development team follows secure coding standards and conducts regular security code reviews.
- **Dependency Scanning:** We continuously scan third-party dependencies for known vulnerabilities and apply security patches promptly.
- **Penetration Testing:** We engage independent security firms to conduct periodic penetration testing and security audits.
- **Vulnerability Disclosure:** We maintain a responsible vulnerability disclosure program for security researchers.

9.6 Privacy by Design

- **Data Minimization:** We collect only the personal information necessary for specified purposes and minimize the data accessible to each system component.
- **Pseudonymization:** Where possible, we use UUIDs and tokenized identifiers instead of directly identifying information in logs, analytics, and internal systems.
- **Audit Trails:** Our RequestContextInterceptor captures IP addresses and user agents for all API requests, storing them via AsyncLocalStorage for security auditing without logging PII.

9.7 Employee Security

- **Background Checks:** Employees with access to personal information undergo background screening appropriate to their role.
- **Security Training:** All employees receive regular privacy and security awareness training.
- **Confidentiality Agreements:** Employees and contractors sign confidentiality agreements protecting customer information.
- **Access Reviews:** We conduct regular reviews of employee access rights and revoke access immediately upon termination or role change.

Despite our security measures, no system is completely secure. If you believe your account has been compromised, contact us immediately at support@joingofree.com

10. Data Retention

We retain your personal information only as long as necessary for the purposes described in this Privacy Policy, to comply with legal obligations, resolve disputes, and enforce our agreements.

10.1 Retention Periods by Data Category

Financial Records and Transactions

- **Retention Period:** 7 years from the date of transaction
- **Legal Basis:** Required by financial services regulations, anti-money laundering laws, and tax record-keeping requirements

keeping requirements

- **Scope:** Transaction histories, account statements, payment records, transfer instructions, wallet balances

KYC and Identity Verification Records

- **Retention Period:** 5 years after account closure
- **Legal Basis:** Required by KYC, AML, and customer due diligence regulations
- **Scope:** Identity documents, verification results, sanctions screening records, risk assessments, proof of address documents

Audit Logs and Security Records

- **Retention Period:** 7 years
- **Legal Basis:** Required for financial services audit trails and security incident investigation
- **Scope:** Authentication events, access logs, security incidents, fraud investigations (with PII removed from application logs)

Chat Messages and AI Conversation History

- **Retention Period:** 90 days of account inactivity, or until account deletion
- **Legal Basis:** Legitimate interest in providing personalized service and customer support
- **Scope:** WhatsApp/Telegram chat history, AI agent conversations, AI memory data, user preferences

Active Account Data

- **Retention Period:** Duration of account relationship plus applicable retention periods above
- **Legal Basis:** Performance of contract, legal obligations
- **Scope:** Profile information, contact details, account settings, beneficiary information

Session and Authentication Tokens

- **Retention Period:** Automatic expiration (email verification: 24 hours; password reset: 1 hour; transfer confirmation: 15 minutes; active sessions: cleaned daily)
- **Legal Basis:** Necessary for security and session management
- **Scope:** JWT tokens, password reset tokens, email verification codes, 2FA sessions

Marketing and Consent Records

- **Retention Period:** 3 years after consent withdrawal or account closure
- **Legal Basis:** Required to demonstrate compliance with consent requirements
- **Scope:** Marketing preferences, consent records, opt-out requests

Backups

- **Retention Period:** Encrypted backups retained for 90 days on rolling basis
- **Legal Basis:** Business continuity and disaster recovery
- **Note:** Personal information in backups may persist for the backup retention period even after deletion

from production systems

10.2 Account Deletion and Cooling Period

When you request account deletion:

1. **30-Day Cooling Period:** Your account enters a 30-day cooling period during which you can reactivate your account by logging in. During this period, your account is inaccessible but data is preserved.
2. **After Cooling Period:**
   - Personal information not subject to legal retention requirements is permanently deleted
   - Financial transaction records are anonymized (personal identifiers removed) but preserved for 7 years to comply with financial record-keeping requirements
   - KYC records are retained for 5 years as required by regulation, then permanently deleted
   - Audit logs retain transaction UUIDs but all directly identifying information is removed
3. **Immediate Deletion Exceptions:** Certain data cannot be immediately deleted due to:
   - Pending transactions or disputes
   - Legal holds, investigations, or litigation
   - Backup retention periods (up to 90 days)
   - Regulatory record-keeping requirements

10.3 Data Minimization Reviews

We conduct annual reviews of retained personal information to:

- Ensure retention periods remain necessary and proportionate
- Delete or anonymize data that is no longer required
- Update retention schedules based on changing legal requirements
- Minimize data retained beyond legal obligations

11. Your Rights

Depending on your jurisdiction, you may have the following rights regarding your personal information:

11.1 Rights Under GDPR (European Economic Area, UK, Switzerland)

If you are in the EEA, UK, or Switzerland, you have the following rights under the GDPR:

Right of Access (Art. 15)

Request confirmation of whether we process your personal information and obtain a copy of that information.

Right to Rectification (Art. 16)

Request correction of inaccurate or incomplete personal information.

Right to Erasure / "Right to Be Forgotten" (Art. 17)

Request deletion of your personal information, subject to legal retention requirements. Financial transaction records will be anonymized rather than deleted where required by law.

Right to Restriction of Processing (Art. 18)

Request that we limit how we use your personal information in certain circumstances.

Right to Data Portability (Art. 20)

Receive your personal information in a structured, commonly used, machine-readable format and transmit it to another controller. We provide data export functionality in your account settings.

Right to Object (Art. 21)

Object to processing based on legitimate interests or for direct marketing purposes.

Right to Withdraw Consent (Art. 7)

Withdraw consent at any time where processing is based on consent, without affecting the lawfulness of processing before withdrawal.

Right to Lodge a Complaint

File a complaint with your local data protection authority:

- **EU/EEA:** Contact your national supervisory authority (list available at edpb.europa.eu)
- **UK:** Information Commissioner's Office (ico.org.uk)
- **Switzerland:** Federal Data Protection and Information Commissioner (edoeb.admin.ch)

11.2 Rights Under CCPA (California)

If you are a California resident, you have the following rights under the California Consumer Privacy Act:

Right to Know

Request information about the categories and specific pieces of personal information we have collected about you in the past 12 months, including:

- Categories of personal information collected
- Categories of sources from which information was collected
- Business or commercial purposes for collection
- Categories of third parties with whom we share personal information
- Specific pieces of personal information collected

Right to Delete

Request deletion of personal information we have collected from you, subject to legal exceptions.

Right to Opt-Out of Sale

We do not sell personal information, so this right does not apply to Axra services.

Right to Non-Discrimination

You have the right not to receive discriminatory treatment for exercising your CCPA rights.

Authorized Agent

You may designate an authorized agent to submit requests on your behalf. We will require proof of authorization.

11.3 Rights Under PIPEDA (Canada)

If you are a Canadian resident, you have the following rights under PIPEDA:

Right to Access

Request access to personal information we hold about you and information about how it has been used and disclosed.

Right to Correction

Request correction of inaccurate or incomplete personal information.

Right to Withdraw Consent

Withdraw consent for processing at any time, subject to legal and contractual restrictions.

Right to File a Complaint

File a complaint with the Office of the Privacy Commissioner of Canada (priv.gc.ca).

11.4 Rights Under Other Jurisdictions

If you reside in Nigeria, Rwanda, or other jurisdictions with data protection laws, you may have similar rights under local legislation. Contact us at support@joingofree.com for information about your rights.

11.5 Exercising Your Rights

To exercise any of these rights:

1. **Via Account Settings:** Many rights can be exercised directly through your Axra account settings, including:
    - Viewing and exporting your data (data portability)
    - Updating your profile information (rectification)
    - Adjusting marketing preferences (objection)
    - Requesting account deletion (erasure)

2. **Via Email:** Contact our Privacy Team at support@joingofree.com with:
    - Your full name and contact information
    - Description of your request
    - Proof of identity (to prevent unauthorized disclosure)
    - Your Axra account email or identifier
3. **Response Timeline:**
    - We will respond to requests within 30 days (GDPR), 45 days (CCPA), or as required by applicable law
    - We may extend this period by an additional 30 days for complex requests, with notice to you
    - We will verify your identity before processing requests to protect your personal information
4. **Free Requests:** We do not charge a fee for your first request in a 12-month period. We may charge a reasonable fee for subsequent requests that are manifestly unfounded, excessive, or repetitive.
5. **Limitations:** Certain rights may be limited where:
    - We have a legal obligation to retain data (e.g., financial transaction records)
    - Processing is necessary for compliance with legal obligations
    - Data is required for the establishment, exercise, or defense of legal claims
    - Other legal exceptions apply

12. Cookies & Tracking Technologies

We use cookies and similar tracking technologies to provide, secure, and improve our services.

12.1 Types of Technologies Used

Cookies

Small text files stored on your device that help us recognize you, remember your preferences, and understand how you use our services.

Local Storage

Browser storage mechanisms that allow us to store data locally on your device for session management and performance optimization.

Session Tokens

Authentication tokens stored in Redis with automatic expiration that maintain your logged-in state securely.

Device Fingerprinting

Collection of device and browser characteristics for fraud prevention and security purposes.

12.2 Categories of Cookies

Strictly Necessary Cookies

- **Purpose:** Essential for authentication, security, and core service functionality
- **Duration:** Session or as needed for security
- **Examples:** Session tokens, CSRF protection tokens, load balancing cookies
- **Opt-Out:** Cannot be disabled as they are essential for service operation

Functional Cookies

- **Purpose:** Remember your preferences and personalize your experience
- **Duration:** Up to 1 year
- **Examples:** Language preferences, timezone settings, AI agent conversation context
- **Opt-Out:** Can be disabled through browser settings, but may impact service functionality

Analytics Cookies

- **Purpose:** Understand how users interact with our services to improve performance and features
- **Duration:** Up to 2 years
- **Examples:** Page views, feature usage, session duration, error tracking
- **Opt-Out:** Can be disabled through cookie preferences

Marketing Cookies

- **Purpose:** Deliver relevant marketing content and measure campaign effectiveness
- **Duration:** Up to 1 year
- **Examples:** Ad campaign tracking, conversion measurement, email engagement tracking
- **Opt-Out:** Can be disabled through cookie preferences or opt-out of marketing communications

12.3 Third-Party Cookies

Some cookies are placed by third-party services we use:

- **Analytics Providers:** To measure service performance and usage patterns (with PII minimization)
- **Fraud Prevention Services:** To detect and prevent fraudulent activity
- **Communication Platforms:** When you access Axra through Telegram or WhatsApp, those platforms may set their own cookies subject to their privacy policies

12.4 Managing Cookies

You can control cookies through:

1. **Browser Settings:** Most browsers allow you to refuse cookies or delete existing cookies. Consult your browser's help documentation for instructions.

2. **Cookie Preference Center:** Adjust your cookie preferences through our web application settings (for non-essential cookies).
3. **Do Not Track:** Our services currently do not respond to Do Not Track (DNT) browser signals, as there is no industry standard for how to interpret DNT.

Important: Disabling necessary cookies will prevent you from using Axra services. Disabling other cookies may limit functionality or personalization.

12.5 Mobile Application Tracking

If you access Axra through mobile applications, we may collect:

- Device identifiers (advertising ID, device UUID)
- Operating system and version
- Application version and crash reports
- Usage analytics and feature engagement

You can limit mobile tracking through your device's privacy settings (e.g., "Limit Ad Tracking" on iOS, "Opt out of Ads Personalization" on Android).

13. Children's Privacy

Axra services are not directed to individuals under the age of 18 (or the age of majority in your jurisdiction), and we do not knowingly collect personal information from children.

13.1 Age Restrictions

To use Axra services, you must be:

- At least 18 years of age in most jurisdictions
- At least the age of majority in your jurisdiction if higher than 18
- Legally capable of entering into binding contracts

13.2 Parental Consent

We do not offer services to minors, even with parental consent, due to financial regulatory requirements and the nature of our banking and payment services.

13.3 Inadvertent Collection

If we discover that we have inadvertently collected personal information from a person under the required age:

- We will delete the information as quickly as possible
- We will close any associated accounts
- We will not use or disclose the information for any purpose

- We will not use or disclose the information for any purpose

If you believe we have inadvertently collected information from a minor, please contact us immediately at privacy@useaxra.com.

14. Changes to This Policy

We may update this Privacy Policy from time to time to reflect changes in our practices, services, legal requirements, or for other operational reasons.

14.1 Notification of Changes

When we make material changes to this Privacy Policy:

- We will update the "Last Updated" date at the top of this policy
- We will notify you by email to your registered email address
- We may display a prominent notice in our application or send a notification through WhatsApp/Telegram
- For material changes that affect your rights, we may require you to affirmatively accept the new policy

14.2 Non-Material Changes

For minor or non-material changes (e.g., clarifications, formatting, contact information updates), we will update the policy and post the revised version on our website without additional notice.

14.3 Review Responsibility

We encourage you to review this Privacy Policy periodically to stay informed about how we protect your personal information. Your continued use of Axra services after changes are posted constitutes acceptance of the updated policy.

14.4 Previous Versions

We maintain an archive of previous Privacy Policy versions. To request a copy of a prior version, contact support@joingofree.com.

15. Contact Information

If you have questions, concerns, or requests regarding this Privacy Policy or our privacy practices, please contact us:

Privacy Team

- **Email:** privacy@joingofree.com
- **Response Time:** We aim to respond to all privacy inquiries within 5 business days

Data Protection Officer (DPO)

- **Email:** dpo@joingofree.com
- **Purpose:** GDPR-related requests and data protection inquiries

Security Concerns

- **Email:** support@joingofree.com
- **Purpose:** Report security vulnerabilities or suspected data breaches

General Support

- **Email:** support@joingofree.com
- **Purpose:** General customer support inquiries

Mailing Address

Orbita LLC
30 N Gould St
Ste R Sheridan,
WY 82801

Regulatory Complaints

If you are not satisfied with our response, you have the right to file a complaint with the relevant data protection authority in your jurisdiction:

- **EU/EEA:** Your national data protection authority (list at edpb.europa.eu)
- **UK:** Information Commissioner's Office (ico.org.uk)
- **Canada:** Office of the Privacy Commissioner of Canada (priv.gc.ca)
- **USA (California):** California Attorney General (oag.ca.gov)

Axra is a product of Orbita LLC.

This Privacy Policy is effective as of June 1, 2026, and supersedes all prior versions.