Tradewize Worker

PRIVACY AND SECURITY POLICY

Last Updated: 03/26/2025 (US) - 10:30 AM EDT

TABLE OF CONTENTS

1. Introduction
2. Permissions Overview
3. Detailed Permissions Analysis
4. Data Collection & Usage
5. User Rights & Controls
6. Security Measures
7. Compliance Information
8. Data Safety Section
9. Children’s Privacy
10. International Data Transfers
11. Changes to This Policy
12. Contact Information
13. Technical Implementation Details
14. User Consent Mechanisms
15. Data Processing Locations

1. INTRODUCTION

Trade Wize Mobile App ("we," "our," or "us") is committed to protecting your privacy. This document provides detailed information about the permissions our Android application requires, how we use them, and how we protect your data. We encourage you to read this document carefully to understand our practices regarding your personal information and how we will treat it.

By using our app, you agree to the collection and use of information in accordance with this policy. We take your privacy seriously and are committed to protecting your personal data.

This Privacy Policy applies to all users of the Trade Wize Mobile App, regardless of how you access or use our services. By downloading, installing, or using our app, you acknowledge that you have read, understood, and agree to be bound by all the terms of this Privacy Policy.

2. PERMISSIONS OVERVIEW

Our application requires the following permissions to function properly:

A. Essential Permissions (Required for core functionality):
- Internet Access
- Location Services
- Notifications

B. Optional Permissions (Enhance app functionality but not required):
- Bluetooth
- Media Access
- Camera and Audio

We request permissions at the time we need them, and you can always change your permission settings in your device settings. We will never request permissions that are not necessary for the app’s functionality.

For Android 13 (API level 33) and above, we use the new granular permission model for media access, requesting specific permissions for photos, videos, and audio separately. For older Android versions, we use the broader storage permission.

3. DETAILED PERMISSIONS ANALYSIS

3.1 Internet Access

Permission: android.permission.INTERNET
Purpose:
- Connect to our servers for real-time trading data
- Download market information and updates
- Synchronize user data across devices
- Enable push notifications
- Access trading APIs and services
- Download app updates and patches

Data Collected:
- Trading activity data
- Market information
- User preferences
- App usage statistics
- Error reports and diagnostics

Retention Period: Data is retained only for the duration of your session and as required by law
User Control: This permission cannot be revoked as it is essential for the app to function
Technical Implementation: We use HTTPS for all network communications and implement certificate pinning for additional security

3.2 Location Services

Permissions:
- android.permission.ACCESS_FINE_LOCATION
- android.permission.ACCESS_COARSE_LOCATION

Purpose:
- Provide location-based trading alerts
- Enable regional market analysis
- Optimize app performance based on your location
- Comply with regional trading regulations
- Detect and prevent fraudulent activities
- Provide location-specific market information

Data Collected:
- Approximate location (city/region level)
- Trading location data
- Market access verification
- Location history for security purposes

Retention Period: Location data is retained only while the app is actively used
User Control: You can revoke this permission at any time through your device settings, though some features may be limited
Technical Implementation: We use the Android Location API with a minimum accuracy threshold of 100 meters for coarse location

3.3 Bluetooth

Permissions:
- android.permission.BLUETOOTH_SCAN
- android.permission.BLUETOOTH_CONNECT

Purpose:
- Connect to trading peripherals
- Enable secure data transfer

- Support for wearable device integration
- Connect to external trading hardware
- Enable proximity-based features
Data Collected:
- Device identifiers
- Connection status
- Performance metrics
- Bluetooth device names and types
Retention Period: Connection data is retained only during active sessions
User Control: You can revoke this permission at any time through your device settings
Technical Implementation: We use the Bluetooth Low Energy (BLE) protocol for energy-efficient connections

3.4 Notifications
Permissions:
- android.permission.POST_NOTIFICATIONS
- android.permission.SCHEDULE_EXACT_ALARM
Purpose:
- Send trading alerts
- Provide market updates
- Notify about account activities
- Remind about scheduled trades
- Alert about security events
- Notify about system maintenance
Data Collected:
- Notification preferences
- Interaction with notifications
- Alert settings
- Notification delivery status
Retention Period: Notification settings are retained until changed by the user
User Control: You can manage notification preferences in the app settings or revoke this permission through your device settings
Technical Implementation: We use Firebase Cloud Messaging (FCM) for reliable notification delivery

3.5 Media Access
Permissions:
- android.permission.READ_EXTERNAL_STORAGE
- android.permission.READ_MEDIA_AUDIO
- android.permission.READ_MEDIA_IMAGES
- android.permission.READ_MEDIA_VIDEO
Purpose:
- Save trading charts and reports
- Export trading data
- Share trading information
- Backup trading history
- Import trading documents
- Save screenshots of trading activities
Data Collected:
- Trading documents
- Chart images
- Trading reports
- Exported data files
Retention Period: User-generated content is retained until deleted by the user
User Control: You can revoke these permissions at any time through your device settings
Technical Implementation: We use the Android Storage Access Framework for modern Android versions

3.6 Camera and Audio
Permissions:
- android.permission.CAMERA
- android.permission.RECORD_AUDIO
Purpose:
- Document trading activities
- Record trading notes
- Enable video trading consultations
- Support for augmented reality trading features
- Scan QR codes for quick actions
- Record voice commands
Data Collected:
- Trading documentation
- Voice notes
- Video consultations
- Scanned QR codes
Retention Period: Media content is retained until deleted by the user
User Control: You can revoke these permissions at any time through your device settings
Technical Implementation: We use the Android CameraX API for consistent camera behavior across devices

4. DATA COLLECTION & USAGE

4.1 How We Collect Data
- Directly from you when you use our app
- Automatically through app functionality
- From third-party services with your consent
- Through cookies and similar tracking technologies
- From your device’s sensors and hardware
- From your interactions with our app
- From error reports and crash logs
- From analytics services

4.2 How We Use Your Data
- To provide and maintain our trading services
- To notify you about changes to our services
- To provide customer support
- To gather analysis or valuable information to improve our services
- To monitor the usage of our services
- To detect, prevent and address technical issues
- To personalize your experience
- To comply with legal obligations
- To prevent fraud and enhance security
- To optimize app performance
- To conduct research and development
- To communicate with you about our services

4.3 Data Sharing
We do not sell your personal information. We may share your data with:
- Service providers who assist in our operations
- Regulatory authorities when required by law
- Business partners with your explicit consent
- Analytics providers to improve our services
- Payment processors for financial transactions

- Cloud storage providers
- Security service providers

4.4 Third-Party Services
Our app may contain links to third-party websites or services that are not owned or controlled by us. We have no control over, and assume no responsibility for, the content, privacy policies, or practices of any third-party websites or services.

We use the following third-party services:
- Firebase Analytics for app usage statistics
- Google Maps for location services
- Stripe for payment processing
- AWS for cloud storage and computing
- Sentry for error tracking and monitoring

Each of these services has its own privacy policy, which we encourage you to review.

5. USER RIGHTS & CONTROLS

5.1 Your Rights
You have the right to:
- Access your personal data
- Correct inaccurate data
- Request deletion of your data
- Object to data processing
- Data portability
- Withdraw consent
- Restrict processing
- Lodge a complaint with a supervisory authority
- Receive information about data breaches
- Obtain a copy of your data in a structured format

5.2 How to Exercise Your Rights
- Through the app settings
- By contacting our support team
- Through your account dashboard
- By emailing us at privacy@tradewize.com
- By submitting a formal request through our website
- By calling our support hotline

5.3 Permission Controls
You can manage app permissions through:
- Android device settings
- App settings within Trade Wize
- Account preferences
- Our privacy dashboard on the website

5.4 Data Portability
You can request a copy of your data in a structured, commonly used, and machine-readable format. We support the following formats:
- JSON
- CSV
- PDF

5.5 Data Deletion

You can request the deletion of your data through:
- The app’s account settings
- Our website’s privacy dashboard
- By contacting our support team

We will process deletion requests within 30 days, unless legal requirements prevent immediate deletion.

6. SECURITY MEASURES

6.1 Data Protection
- End-to-end encryption for sensitive data
- Secure data storage
- Regular security audits
- Access controls and authentication
- Data minimization principles
- Regular security training for employees
- Multi-factor authentication
- Biometric authentication options
- Secure key storage
- Regular penetration testing

6.2 Technical Safeguards
- SSL/TLS encryption
- Secure API endpoints
- Regular security updates
- Vulnerability testing
- Firewall protection
- Intrusion detection systems
- DDoS protection
- Rate limiting
- Input validation
- Output encoding

6.3 Data Breach Procedures
In the event of a data breach, we will:
- Notify affected users within 72 hours
- Take immediate steps to contain the breach
- Investigate the cause
- Implement measures to prevent future breaches
- Comply with all legal reporting requirements
- Provide guidance to affected users
- Work with law enforcement if necessary
- Document the incident and our response

6.4 Secure Development Practices
- Secure coding guidelines
- Code review processes
- Automated security testing
- Dependency vulnerability scanning
- Regular dependency updates
- Security-focused CI/CD pipeline

7. COMPLIANCE INFORMATION

7.1 Regulatory Compliance

Our app complies with:
- Google Play Store policies
- GDPR requirements
- CCPA requirements
- Regional financial regulations
- COPPA (Children's Online Privacy Protection Act)
- PIPEDA (Personal Information Protection and Electronic Documents Act)
- LGPD (Lei Geral de Proteção de Dados)
- PDPA (Personal Data Protection Act)
- FISMA (Federal Information Security Management Act)
- SOX (Sarbanes-Oxley Act)

7.2 Certification
- Google Play Store verified
- Security certifications
- Financial regulatory compliance
- ISO 27001 certification
- SOC 2 Type II compliance
- PCI DSS compliance
- FedRAMP authorization
- CSA STAR certification

7.3 Compliance Documentation
We maintain detailed documentation of our compliance efforts, including:
- Data processing records
- Security assessment reports
- Privacy impact assessments
- Vendor risk assessments
- Compliance audit reports

8. DATA SAFETY SECTION

8.1 Data Types Collected
- Personal Information (name, email, phone number)
- Financial Information (trading history, account balances)
- Device Information (device ID, IP address, operating system)
- Usage Data (app interactions, features used)
- Location Data (approximate location)
- Media Content (photos, videos, audio recordings)
- Authentication Data (login history, security questions)
- Transaction Data (trades, transfers, payments)
- Communication Data (support tickets, messages)
- Preference Data (settings, customization options)

8.2 Data Encryption
- All data in transit is encrypted using TLS 1.2 or higher
- Sensitive data at rest is encrypted using AES-256
- Encryption keys are managed securely
- Key rotation policies are implemented
- Hardware security modules (HSM) for key storage
- End-to-end encryption for sensitive communications

8.3 Data Retention
- Personal data is retained only as long as necessary
- Data is automatically deleted after the retention period

- Users can request immediate deletion of their data
- Retention periods vary by data type:
  * Account data: 7 years (for regulatory compliance)
  * Trading history: 7 years
  * Location data: 90 days
  * Usage analytics: 2 years
  * Communication data: 3 years

8.4 Data Sharing with Third Parties
- We share data only with trusted third parties
- All third parties must sign data processing agreements
- We regularly audit third-party data handling
- We maintain a list of all data processors
- We conduct vendor risk assessments
- We require third parties to implement appropriate security measures

8.5 Data Minimization
We follow the principle of data minimization by:
- Only collecting data necessary for specific purposes
- Automatically deleting data when no longer needed
- Using anonymization and pseudonymization where appropriate
- Implementing data retention policies
- Regularly reviewing our data collection practices

9. CHILDREN'S PRIVACY

Our app is not intended for use by children under the age of 13. We do not knowingly collect personal information from children under 13. If you are a parent or guardian and you are aware that your child has provided us with personal information, please contact us so that we can take necessary actions.

We implement age verification mechanisms to prevent children from creating accounts. If we discover that a child under 13 has provided us with personal information, we will:
- Immediately delete the account
- Delete all associated data
- Notify the parent or guardian
- Provide information about how to prevent future collection

10. INTERNATIONAL DATA TRANSFERS

Your information may be transferred to, and maintained on, computers located outside of your state, province, country, or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction. If you are located outside the United States and choose to provide information to us, please note that we transfer the information to the United States and process it there. Your consent to this Privacy Policy followed by your submission of such information represents your agreement to that transfer.

We ensure appropriate safeguards are in place for international data transfers, including:
- Standard contractual clauses approved by the European Commission
- Binding corporate rules
- Adequacy decisions by relevant authorities
- Data processing agreements with third parties

11. CHANGES TO THIS POLICY

We may update our Privacy Policy from time to time. We will notify you of any changes by posting the

new Privacy Policy on this page and updating the "Last Updated" date at the top of this Privacy Policy. You are advised to review this Privacy Policy periodically for any changes. Changes to this Privacy Policy are effective when they are posted on this page.

For significant changes, we will:
- Provide a more prominent notice
- Send you an email notification
- Require you to acknowledge the changes
- Provide a summary of the key changes

12. CONTACT INFORMATION

For questions about this Privacy Policy or our practices, please contact us at:
- Email: feroz.ahmed@prediction3d.com

13. TECHNICAL IMPLEMENTATION DETAILS

13.1 App Architecture
- Native Android application using Kotlin
- MVVM architecture pattern
- Repository pattern for data management
- Dependency injection using Hilt
- Reactive programming with Kotlin Coroutines and Flow
- Offline-first approach with local caching

13.2 Data Storage
- Local storage using Room database
- Encrypted SharedPreferences for sensitive data
- File storage for documents and media
- Cloud storage with AWS S3
- Secure key storage using Android Keystore

13.3 Network Communication
- RESTful API using Retrofit
- GraphQL for complex data queries
- WebSocket for real-time updates
- Certificate pinning for enhanced security
- Automatic retry mechanisms with exponential backoff

13.4 Authentication
- OAuth 2.0 and OpenID Connect
- JWT token-based authentication
- Biometric authentication integration
- Multi-factor authentication options
- Session management with automatic timeout

13.5 Analytics and Monitoring
- Firebase Analytics for usage statistics
- Crashlytics for crash reporting
- Performance monitoring
- User behavior analytics
- Error tracking with Sentry

14. USER CONSENT MECHANISMS

14.1 Consent Collection
We collect user consent through:
- In-app consent dialogs
- Checkbox confirmations during registration
- Explicit permission requests
- Settings toggles for optional features
- Granular consent options for different data uses

14.2 Consent Management
Users can manage their consent through:
- Account settings
- Privacy dashboard
- Permission settings
- Email preferences
- Cookie preferences

14.3 Consent Withdrawal
Users can withdraw consent by:
- Changing app settings
- Contacting our support team
- Using the privacy dashboard
- Submitting a formal request

14.4 Consent Records
We maintain records of:
- When consent was given
- What was consented to
- How consent was obtained
- When consent was withdrawn
- Consent version history

15. DATA PROCESSING LOCATIONS

15.1 Primary Data Centers
Our primary data processing locations are:
- United States (AWS us-east-1, us-west-2)
- European Union (AWS eu-central-1, eu-west-1)
- Asia Pacific (AWS ap-southeast-1, ap-northeast-1)

15.2 Data Processing Agreements
We have data processing agreements with:
- Amazon Web Services
- Google Cloud Platform
- Microsoft Azure
- Firebase
- Other service providers

15.3 Data Residency Options
For users in specific regions, we offer data residency options:
- EU data residency for European users
- US data residency for American users
- Asia data residency for Asian users

This document is subject to updates. We will notify users of any material changes through the app or via email.