

# Privacy Policy

## Privacy Policy

Purpose and Basis. In order to provide the services of the Platform to Users, AltCryptoGems needs to collect some of your personal information when you register with the Platform, log in to the Platform and/or use the services offered by the Platform. This Privacy Policy, in combination with AltCryptoGems.com's other applicable policies, set out the rules as to the use and protection of the collected information in order to prevent misuse.

## Article 2

Designation. For the convenience of wording in this agreement (the "Agreement"), the Platform is referred to as "we", "us" or "our". Users of and other visitors to the Platform are referred to as "you", "your" or "User". We and you are collectively referred to as "both parties" and as "a/one party" individually.

## Article 3

Definition and Interpretation. The following terms or expressions shall have the meanings ascribed to them below, unless any other term or condition hereunder provides otherwise:

■1■Personal Information: all information that is recorded electronically or otherwise and can be used, whether independently or in combination with any other information, to identify any particular natural person or reflect the pattern of behaviour of a particular natural person, including, but not limited to, sensitive personal information;

■2■Sensitive Personal Information: including but not limited to identity card and other proof of identity documents details, personal biometric information, bank account details, registered address, whereabouts, transaction information, etc.;

■3■Deletion of personal information: the deletion of personal information from any system involved in carrying out routine business functions so that such personal information cannot be accessed or retrieved.

## Article 4

Scope of Application. This Agreement shall apply to all Users trading on the AltCryptoGems.com Global website and on its APP (the "Platform"). Users shall comply



with the terms and conditions of this Agreement, subject to and as permitted by any and all laws relating to the protection of personal information and data in the country or region where they are based.

#### Article 5

Invocation. Any code or statutory decree or administrative regulation referred to in this Agreement shall refer to the latest amended version thereof, regardless of whether such amendment is made before or after the signing of this Agreement.

#### Article 6

Headings. The headings used in this Agreement are for convenience only and shall not be used for the purpose of interpreting the terms and conditions of this Agreement. References herein to any statement, term, condition, annex, schedule shall refer to statements, terms, conditions, annexes and schedules hereunder.

#### Article 7

Use of the term "include". The term "include" used herein shall, under any and all circumstances always have the meaning of "include but not limited to", unless this Agreement specifies otherwise.

#### Article 8

User Consent and Authorization. The Users acknowledge and understand that, at the point of logging into the Platform, the User will be deemed to have expressed to us their acceptance, consent, undertaking and confirmation of the following, regardless of whether the User has completed their registration on the Platform:

■1■that the User agrees, on a voluntary basis, to disclose personal information to us;

■2■the User will abide by all the terms and conditions of this Agreement;

■3■the User agrees and authorises the Platform to collect the User's personal information when the User registers with the Platform, logs into the Platform and/or uses the Platform services;

■4■the User agrees to all the terms and conditions of this Agreement and agrees to accept any amendment that may subsequently be made to the Privacy Policy;



■5■the User agrees that any of our branch companies, subsidiary companies, or employees will contact the User in connection with any product and service that may be of interest to the User (unless the User has indicated that he or she does not wish to receive such information).

## Article 9

Information Collected. The Users agree that the Platform may use cookies to track the User's actions in connection with their use of the Platform and may collect and record all information left by Users, including but not limited to their IP address, geographical location and other data.

Personal data which we may collect include:

- Personal Identification Information: Full name, date of birth, nationality, gender, ethnicity, signature, facial data, utility bills, photographs, phone number, precise location, home address, and/or email.

- Formal Identification Information: Government issued identity document such as Passport, Driver's License, National Identity Card, State ID Card, Tax ID number, passport number, driver's license details, national identity card details, visa information, and/or any other information deemed necessary to comply with our legal obligations under financial or anti-money laundering laws.

- Virtual Identity: AltCryptoGems.com Account/ Password, AltCryptoGems.com Nickname.

- Institutional Information: Employer Identification number (or comparable number issued by a government), proof of legal formation (e.g. Articles of Incorporation), personal identification information for all material beneficial owners.

- Financial Information: Bank account information, payment card primary account number (PAN), account assets, transaction history, trading data, and/or tax identification.

- Transaction Information: Information about the transactions you make on our Services, such as the name of the recipient, your name, the amount, and/or timestamp.

- Message Content: Feedback, Email, SMS, App Rating, Comments.

- Application Activity: Browsers and tap records, search history, installed apps, user generated content, favorites.
- Device Information: Carrier, brand, software version.



model name, manufacturer, system language, network, OAID, IMEI, GUID, MAC address.

- Employment Information: Office location, job title, and/or description of role.
- Correspondence: Survey responses, information provided to our support team or user research team.
- Audio, electronic, visual and similar information, such as call and video recordings.

We will collect your personal data in accordance with the legislative purpose of the DPA. We may also collect and store certain information automatically when you visit the Site/APP. To the extent permitted under the applicable law, we may collect certain types of information automatically, such as whenever you interact with the Sites/APP or use the Services. This information helps us address customer support issues, improve the performance of our Sites/APP and Services, provide you with a streamlined and personalized experience, and protect your account from fraud by detecting unauthorized access. Information collected automatically includes:

Online Identifiers: Geo location/tracking details, browser fingerprint, operating system, browser name and version, and/or personal IP addresses.

Usage Data: Authentication data, security questions, click-stream data, public social networking posts, and other data collected via cookies and similar technologies.

For example, we may automatically receive and record the following information on our server logs:

- (1) How you came to and use the Services;
- (2) Device type and unique device identification numbers;
- (3) Device event information (such as crashes, system activity and hardware settings, browser type, browser language, the date and time of your request and referral URL);

How your device interacts with our Sites/APP and Services, including pages accessed and links clicked;

- (4) Broad geographic location (e.g. country or city-level location); and Other technical data collected through cookies, pixel tags and other similar technologies that uniquely identify your browser.



(5) Application checklist: For advertising and safety use and approval of service applications.

We may also use identifiers to recognize you when you access our Sites/APP via an external link, such as a link appearing on a third-party site.

## Article 10

### Application and Usage of Information Permission

Android Permission	Description	Application	android.permission	Network
access	permission	Allows applications to be networked	android.permission.INTERNET	
android.permission.ACCESS_NETWORK_STATE	Get network status	permission	Allows applications to get the network status	
android.permission.CHANGE_NETWORK_STATE	Change network status	permission	Allows applications to change the network status	
android.permission.ACCESS_WIFI_STATE	Get WiFi status	permission	Allows applications to get the WiFi status	
android.permission.CHANGE_WIFI_STATE	Change WiFi status	permission	Allows applications to change the WiFi status	
android.permission.FOREGROUND_SERVICE	Frontend service start	permission	Allows market monitoring through the ticker widget	
android.permission.RECEIVE_BOOT_COMPLETED	Boot broadcast monitoring	permission	Allows monitoring of background tasks in workmanager	
android.permission.USE_FINGERPRINT	Touch ID	permission	Allows fingerprint login	
android.permission.VIBRATE	Vibration	permission	Allows phone vibration	
android.permission.WAKE_LOCK	Wake lock	permission	Allows keeping the screen in awake status for KYC	
android.permission.CAMERA	Camera access	permission	Allows taking of photos and scanning of ID cards for KYC	
android.permission.ACCESS_COARSE_LOCATION	Coarse location information	access	permission	Allows push notifications for news and events
android.permission.READ_PHONE_STATE	Read local identification code	permission	Allows device fingerprinting, statistics, and facial recognition	
android.permission.READ_EXTERNAL_STORAGE				
android.permission.WRITE_EXTERNAL_STORAGE	Read and write external storage	permission	Allows reading or writing of images, files, etc. to ensure stable app operation	
android.permission.WRITE_SETTINGS	Read and write system settings	permission	Allows device fingerprint functionality	
android.permission.REQUEST_INSTALL_PACKAGES	Unknown source installation	permission	Allows offline push notifications	
android.permission.SYSTEM_ALERT_WINDOW				
android.permission.SYSTEM_OVERLAY_WINDOW	Hoverbox	permission	Allows floating window functionality	
android.permission.ClipboardManager	Clipboard access	permission	Used for ZFA login.	



red envelopes, and deposit and withdrawal services iOS Permission Description Application NSFaceIDUsageDescription Facial or fingerprint information access permission Login with Facial ID Camera Camera access permission Allows taking of photos and scanning of ID cards for KYC LocationServices Coarse location information access permission Allows push notifications for news and events Photos Read and write external storage permission Allows reading or writing of images Push Push permission Allows offline push notifications UIPasteboard Clipboard access permission Used for 2FA login, red envelopes, and deposit and withdrawal services Article 11

Supply of Information. If Users voluntarily use the services provided by the Platform, they will be required to fill in and/or provide the following two categories of information in accordance with the requirements of AltCryptoGems.com:

■1■ Identity Information: this category of the User information, which may help the Platform verify whether the User is eligible to register on the Platform, includes, but is not limited to: the User's full name, registered address, postal address, official proof of identity documents and the document numbers, as well as all other information that may assist the Platform in verifying the User's identity (hereinafter collectively referred to as "Identity Information");

■2■ Service Information: this category of User information helps the Platform to contact the User and to provide a smooth service experience It includes, but is not limited to, the User's telephone number, fax number, valid email address, postal address, and debit card information and/or other account information (hereinafter collectively referred to as "Service Information"). Article 12

Changes in the Method of Information Collection. When a User uses the Platform, the Platform may collect additional necessary information by an email box that is exclusively owned by the Platform and released to the public via the Platform or by any other method that is deemed as in compliance with relevant laws and regulations, so as to improve the functionality of the Platform and enhance the Users' experience of using the Platform services and the security thereof, or as is required by any order of a court, any applicable law or regulation, or any other competent government agency. Article 13

Third-party Websites. If a User visits any link on this APP that leads to a third-party website or to a third-party partner's website, the User agrees to and shall comply with the separate and independent privacy policies of such third-party websites. The User understands and acknowledges that the Platform is not responsible for the content or activities of such third-party websites or partners. These sources may include:



(1) Our AltCryptoGems.com Family of Companies: Our “family of companies” is the group of companies related to us by common control or ownership (“Affiliates”). In accordance with applicable law, we may obtain information about you from our Affiliates as a normal part of conducting business, if you link your various AltCryptoGems.com accounts (e.g., AltCryptoGems.com Wallet account or AltCryptoGems.com Commerce account in order to convert cryptocurrency into fiat and make withdrawals into your bank account), so that we may offer our Affiliates’ Services to you.

(2) Public Databases, Credit Bureaus & ID Verification Partners: We obtain information about you from public databases and ID verification partners for purposes of verifying your identity in accordance with applicable law. ID verification partners like World-Check use a combination of government records and publicly available information about you to verify your identity. Such information may include your name, address, job role, public employment profile, credit history, status on any sanctions lists maintained by public authorities, and other relevant data. We obtain such information to comply with our legal obligations, such as anti-money laundering laws. In some cases, we may process additional data about you to assess risk and ensure our Services are not used fraudulently or for other illicit activities. In such instances, processing is necessary for us to continue to perform our contractual obligations with you and others.

(3) Blockchain Data: We may analyze public blockchain data to ensure parties utilizing our Services are not engaged in illegal or prohibited activity under our Terms, and to analyze transaction trends for research and development purposes.

(4) Joint Marketing Partners & Resellers: For example, unless prohibited by applicable law, joint marketing partners or resellers may share information about you with us so that we can better understand which of our Services may be of interest to you.

(5) Advertising Networks & Analytics Providers: We work with these providers to provide us with de-identified information about how you found our Sites/APP and how you interact with the Sites/APP and Services. This information may be collected prior to account creation.

#### Article 14

Installation of Cookies. When a User visits the Platform, the Platform will use Google Stats via Cookies to record the Platform’s performance and check the effectiveness of online advertising. Cookies are a small amount of data that is sent to the User’s browser and stored on the User’s computer hard drive. Only when the User uses his/her computer to access the Platform can the Cookies be sent to the User’s computer hard drive.





Function of Cookies. Cookies are frequently used to record the habits and preferences of visitors when they browse various items on the Platform. Cookies collect anonymous collective statistics which do not contain personal data. Cookies cannot be used to obtain data from the User's hard drive, the User's email address or personal data; they can enable the Platform or a service provider's system to recognize the User's web browser as well as capture and remember information. Article 16

Disabling Cookies. Most browsers are preset to accept Cookies and Users can choose to set their web browsers to reject Cookies or to notify Users upon the installation of Cookies. Users should be aware that they may be unable to start or use certain features of the Platform if they opt to disable Cookies. Article 17

Use of Information. The information collected by the Platform is used by the Platform for the following purposes or in the following manner:

■1■to provide the Users with the Platform's services via the Platform; ■2■to identify and confirm the Users' identities when Users use the Platform;

■3■to improve and upgrade the services of the Platform (the Users' information and feedback received by the Platform can help the Platform improve the services of the Platform, so that the Platform can respond to the Users' service requests and support needs in a more effective manner); ■4■to keep statistics relating to the use of the Platform and for use in data analysis carried out in cooperation with government agencies and public affairs institutions;

■5■to personalise the User experience (more specifically, the User information will help the Platform to better respond to each User's personalised needs); ■6■to facilitate transactions. The Users' personal information will not be sold, exchanged, transferred, or otherwise provided to any third party company on any ground without the Users' consent, except for where doing so is expressly for the purpose of completing the transactions the Users require; ■7■to send regular emails. More specifically, email addresses will be used by the Platform to send Users newsletters, updates, relevant product or service information, as well as announcements and updates on the Users' orders;

■8■to fulfil other purposes as specified in the User Service Agreement and to be used for all the legal means adopted for fulfilling such purposes. Article 18

Information Disclosure to Third Parties. The Platform does not sell, trade, or otherwise transfer information or allow any other party to collect or use any information from our Platform. However, this does not involve the following parties and does not include the





following information: the Platform's affiliates, trusted third parties who help the Platform operate the Platform's websites, manage the Platform's business or provide services to Users, provided that these parties agree to keep such information confidential. If the Platform discloses information to the above-mentioned parties, such information disclosure shall in accordance with any applicable laws, regulations, rules or by any order of any court or other competent authorities, or necessary for executing the strategy of the Platform and ensuring the proper functioning of the Platform, or as may be necessary for the related parties to provide services, or for the protection of the rights, property or safety of us or other persons. Any such information disclosure will not be used by any of the above-mentioned parties for marketing, advertising or any other purpose that has not been agreed on by all the parties concerned.

For Example, (a) We may use AppsFlyer to measure the advertising performance, detect and prevent fraudulent activity on your account in real time. Information shared with AppsFlyer is treated by AppsFlyer in accordance with its Privacy Policy. (b) We may use Sentry to monitor the anomalies of the Platform. Information shared with Sentry is treated by Sentry in accordance with its Privacy Policy.

Third-Party SDK Purpose Data Involved Link to Third Party Bugly Stability monitoring  
Device data Log data File data Network data System name System version Country code

Firebase Performance monitoring Cloud configuration Push notifications Crashlytics MAID  
IDFV/Android ID FID App Instance ID Crashlytics Installation UUIDs Crash traces  
Breakpad minidump formatted data (NDK crashes only).

Protection of Personal Data. The Platform adopts appropriate physical, electronic, management and technical measures to protect and safeguard the security of the Users' personal data. The Platform will, to the greatest extent possible, ensure that any personal data collected through the Platform shall be free from being subject to nuisance by any third party unrelated to us. The security measures that the Platform may take include but are not limited to:

■1■Physical measures: records of Users' personal information will be stored in an appropriately secure location.

■2■Electronic measures: computer data containing Users' personal information will be stored in computer systems and storage medias that are subject to strict login restrictions.

■3■Management measures: only staff members duly authorized by the Platform may access the Users' personal data and such staff members shall comply with the Platform's internal code concerning personal data confidentiality.



■4■ Technical measures: encryption techniques such as Secure Socket Layer Encryption may be used to transmit Users' personal data.

■5■ Other measures: the Platform's network servers are protected by a proper "firewall".  
Article 20

Reporting of Flaws. If any User becomes aware of any security flaw in the Platform, the User should contact the Platform through the service email promptly so that the Platform can take appropriate measures to address any such flaw as soon as possible. Article 21

Exemption. Despite the above-mentioned technical and security measures, the Platform cannot guarantee that the information transmitted via the Internet is absolutely safe, so the Platform does not provide any guarantees with respect to the security of the personal information that the Users provide to the Platform; and the Platform may not be held liable for any loss or damage arising from or caused by any event that may occur in connection with unauthorized access to the Users' personal information.

Article 22

Amendment of this Agreement. The Platform reserves the right to modify this Agreement at any time. The Platform will inform the Users of the amendments made to the Privacy Policy by releasing updates thereof, publishing the effective date of new versions thereof and highlighting the amendments thereto. Sometimes, but not always, the Platform may issue a notice to Users to inform them of any amendments made to the Privacy Policy. Users shall regularly review the Privacy Policy and focus on amendments thereto, if any; and if the Users do not agree to any such amendments, the Users shall promptly stop accessing this Website. Whenever an updated version of this Privacy Policy is released, the User's continued access to and use of this Website shall demonstrate the User's agreement to the updated version of the Privacy Policy.

Article 23

Communication with Us. Any User comments or feedback should be sent to the following email address: support@AltCryptoGems.com. This is the only valid and official email address through which the Platform communicates with Users. If an User uses any other means of communication to contact the Platform, the Platform shall not be obliged to reply and the Platform will not be held liable in any manner whatsoever. Article 24

Publishing of Announcements. The Platform publishes announcements and information exclusively via the use of valid and up-to-date contact information provided to this Website



or by posting announcements on the Platform. Therefore, the Platform shall not be held liable for any loss arising from any User's trust in any information that is obtained in any manner other than the above-mentioned means.

RUE

RUE

RUE

RUE

RUE

RUE

RUE

RUE

RUE

RUE

RUE

RUE



RUE



RUE