Privacy Policy

Last updated: 2025/10/01

Article 1 Purpose for processing personal information

In order to provide services of the platform to Users, Finflux needs to collect some of your personal information for the following purposes. The personal information collected is not used for purposes other than the following. If the purpose of use is changed, necessary measures, such as separate notification or obtaining separate consent under any applicable laws, will be take.

1. Account Registration and Management

-Identification of users, customer verification (KYC), management of user information, delivery of various notices

-Account termination through non-face-to-face authentication, resetting phone numbers/emails, etc.

2. Provision of Goods or Services

- Confirmation of digital asset trading relationships

- Inheritance and transfer

- Matters related to the overall management of digital asset trading relationships, including setting, maintaining, and terminating services

- Prevention of unauthorized use

- Usage statistics and analysis, provision of new and customized services

- Improvement and upgrade the services of the platform, etc.

3. Event Information Guide

- Providing information for various events and promotions

4. Complaint handling

- Confirmation of the identity of complainants and the contents of complaints

- Contact and notification for fact-finding, notification of processing results

- Remedies for damages and incorrect transfers, etc.

5. AML/CTF and legal investigation

- AML/CTF misconduct investigations

- Law enforcement authorities' investigation, etc.

**We ONLY provide services to natural person that is at least 18 years of age or is deemed under the law of the country where such natural person is located as an adult having full capacities for civil rights and capable of independently bearing civil liabilities (otherwise, "Children", "Child"). We do not knowingly collect data from children. If we learn that we have inadvertently processed personal data from a child, we will immediately terminate the service and any activities related to the account and delete the data from our system.*
**The User has the right to refuse to consent to the collection of personal information by the Platform. The User may not be able to use any of the services the Platform provided if the User refuse to accept the collection of personal information by the platform.*

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 Processing and Retention Period of Personal information

1. The Platform shall process and retain personal information within the period of time required by applicable laws for personal information processing and retention or within the period of processing information agreed upon when collecting personal information from users.

2. The period of time for processing and retention of each personal information is as follows:

A. In principle, the personal information will be retained up to 5 years after the user deleted its accounts or the accounts have been deactivated due to abuse in order to satisfy any subsequent review of users' accounts by financial institutions or criminal investigations by relevant authorities. If no such review or investigations occurs within the years, Finflux will completely delete the personal data.

B. If an investigation is ongoing due to a violation of applicable laws and regulations, the personal information will be stored until the end of the relevant investigation is concluded.

C. If there is an outstanding debt or credit relationship arising out of use of the service, the personal information will be stored until the debt is settled

D. If there is an ongoing legal dispute between the user and the Company, the personal information will be stored until the dispute is officially resolved

E. In accordance with different regional and regulatory requirements, we may be required to retain certain records beyond our usual retention period after our business relationship with you has concluded.

① When personal information becomes unnecessary due to the passage of the retention period or the accomplishment of the processing purpose, the Company shall promptly destroy such personal information.

② In the case of personal information that must be retained under the law despite the expiration of the retention period for personal information, the Company will move such personal information to a separate database or store it in a different location.

③ The Company securely manages the personal information of a user who has been processed as a dormant user in accordance with the old Personal Information Protection Act. But the personal information of users whose mobile phone identity verification information does not exist among dormant users will be destroyed at the end of six months from the date when the users are converted to dormant users.

④ The personal information for which a reason for destruction has occurred due to the passage of the retention period or the accomplishment of the processing purpose, shall be destroyed upon approval of the personal information protection manager or through automatic deletion by the system.

⑤ The method of personal information destruction is as follows.

1. Personal information stored in electronic form is permanently deleted to prevent playback of the record.

2. Personal information recorded or stored on paper documents is shredded or incinerated.

Article 4 Data Controller

Finflux acts as a controller of your personal data where we determine the means and the purposes of any processing activities that it carries out. This Privacy Policy does not apply where we act as a processor or service provider to another controller.

Article 5 Scope of Application

This Agreement shall apply to all Users trading on the Finflux 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 6 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 7 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 8 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 9 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 authorizes 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 or service providers with whom we have engaged for the provision of the services, will contact the User to request for information or to inform the User in connection with of 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).

During our onboarding process, Finflux makes use of **automated decision-making**, particularly within our Know-Your-Customer (KYC) procedures. When you submit your identification documents, photo, and live video, our automated systems process this information to verify your identity and ensure compliance with global Anti-Money-Laundering (AML) regulations. While this enhances accuracy and efficiency, we recognize that errors may occasionally occur.

If an automated decision significantly affects your ability to use our products or services, you have the right to request that the decision not be applied to you. You may also contest the decision and ask our **Customer Service** team to review your case manually. Please note, however, that even if your request is granted, there may still be circumstances where we are unable to provide access to our services due to regulatory requirements.

Article 10 Information Collected

The Users agree that the Platform may use cookies to track the Users' 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. For example: We may use video (including audio) information as identity credentials for P2P merchants and as evidence for P2P order disputes. We may also use facial video (including audio) information for KYC identity verification on third-party platforms.

Personal data which we may collect include:

Category	Type	Purpose of Usage	Usage Scenario
Location information	Approximate location information	Government regulation; Used for completing hardware wallet transactions	When users log in and enter the homepage; When importing a hardware wallet; When signing transactions for DApps from a hardware

			wallet; When sending assets from a hardware wallet; When performing same-chain / cross-chain swaps with a hardware wallet; When signing transactions with a hardware wallet using WalletConnect.
	Fine location information	1. Used for completing hardware wallet transactions； 2. Used to accurately verify whether users are within the designated on-site area when scanning the QR code for offline events, ensuring correct distribution of exclusive on-site rewards.	1. When importing a hardware wallet; 2. When signing transactions for DApps from a hardware wallet; 3. When sending assets from a hardware wallet; 4. When performing same-chain / cross-chain swaps with a hardware wallet; 5. When signing transactions with a hardware wallet using WalletConnect； 6. When users use the Finflux app to scan QR codes for offline events to claim coupons.
Personal information	Name	Identity verification	When users use documents for KYC identity verification
	Date of birth		
	Gender		
	Nationality		
	Address		
	Document type and document number		
	Race and ethnicity		
	Phone number	1. Account creation 2. Identity verification 3. P2P dispute flow 4. Mobile Top-Up business	1. When users sign up for the first time 2. When users logs in again 3. When verifying user identity 4. A mobile phone number is required when

			a user communicates with a counterparty after placing an order in P2P 5. User can copy the phone number from contacts and paste in our mobile top-up page
	Email address	1. Account creation 2. Identity verification 3. Event promotion	1. When users sign up for the first time 2. When users logs in again 3. When verifying user identity 4. When promoting platform events
	Finflux account and password	Account creation	When users sign up for the first time
	Finflux nickname	Account creation	When users set and modify nicknames
	Finflux avatar	Account creation	When users set and modify avatars
Financial information	Bank account (bank card number, etc.)	1. P2P trading 2. Fast trade 3. Fiat deposit and withdrawal	When adding payment and receipt methods
	Third-party payment account (Alipay, WeChat, etc.)		
Trading information	Finflux order information	Trading function	When users view orders
	Finflux asset information	Asset management	1. When users view assets 2. When users place orders and make trades
	Finflux deposit and withdrawal information	Asset management	Users view deposit and withdrawal history
	User wallet address	Deposit and withdrawal function	When adding deposit and withdrawal addresses
	User hardware wallet address	Used for completing hardware wallet transactions	When importing a hardware wallet; When signing transactions for DApps from a hardware wallet; When sending assets from a hardware wallet; When performing same-chain / cross-chain
	Trading signature information		

			swaps with a hardware wallet; When signing transactions with a hardware wallet using WalletConnect.
Message information	SMS	Authentication	1. When users sign up 2. When users log in 3. When changing the password 4. When setting the trading password 5. When binding and unbinding a mobile phone 6. When binding and unbinding an email 7. When binding 2FA (two-factor authentication) 8. When canceling the account 9. During the identity verification for trading
	Voice message		
	Email		
	Google verification code		
Multimedia information	Photo	1. P2P dispute settlement 2. Customer service 3. Withdrawal function 4. Identity verification	1. When users appeal for P2P orders 2. When users send feedback to customer service 3. When adding wallet addresses 4. When performing KYC identity verification
	Audio	1. P2P dispute settlement 2. When users send feedback to customer service	1. When users appeal for P2P orders 2. When users send feedback to customer service
	PDF file	1. P2P dispute settlementls 2. Fiat withdrawal account verification	1. When users appeal for P2P orders 2. When the user's fiat withdrawal account needs to be verified

	Video	1. P2P dispute settlement 2. When users send feedback to customer service	1. When users appeal for P2P orders 2. When users send feedback to customer service
App activities	App interaction information (page visits, button clicks, etc.)	Product experience enhancement (user activity analysis)	When users use app services
	In-app search history	Show search history	When users search for trading pairs
	User-generated content	1. P2P dispute settlement 2. Customer service	1. When users appeal for P2P orders 2. When users send feedback to customer service
App information	App version	Product experience enhancement	When users use app services
	App language		
	App package name		
	Download channel		
	Crash log		
	Diagnostic log		
	Performance data (CPU, memory, etc.)		
Device information	Network operator	1. Trading security protection 2. Product experience enhancement (user activity analysis)	1. When users use app services
	Device brand		
	System and version		
	Device model		
	Screen width and height		
	Time zone offset		
	Device manufacturer		
	Number of cameras		
	Device storage		
	Device RAM		
	System language		
	Network type		
	SIM card status		
	Browser user agent		
	CPU name		
	CPU instruction set		
	Motherboard model		
	Display specifications		
	Radio firmware version		
	Gyroscope data		

	IP address		
	MAC address		
	Fingerprint ID		
	Advertising ID		
	Android ID		
	OAID		
	IMEI		
	Widevine ID		
	GUID		
	SSID		
	Ledger device ID	Used for completing hardware wallet transactions	When importing a hardware wallet; When signing transactions for DApps from a hardware wallet; When sending assets from a hardware wallet; When performing same-chain / cross-chain swaps with a hardware wallet; When signing transactions with a hardware wallet using WalletConnect.
	Ledger device name		
	Ledger MTU		
	Bluetooth status		
Sensors Data analysis SDK	Device information (IMEI, Android ID, OAID, IDFA, IDFV, UUID, IMSI, MAC address, browser type, telecom operator, device brand)	Product experience enhancement	When users use app services
	Log information (service usage, IP address, language used, time of access)	Product experience enhancement (user activity analysis)	
	Location information (location information resolved by IP address, GPS location information)		
	Unique application number (app unique identifier, app name, and app version number)		

Aurora Push SDK	Device identifier (IMEI, IDFA, Android ID, GAID, MAC, OAID, IMSI, MEID, UAID, etc.)	Used to push notifications to user devices	Push notifications
	Device hardware information (device model, device screen resolution, device hardware manufacturer, device product name, etc.)		
	Operating system information (operating system version, system name, system language, etc.)		
	Network information (network type, operator name, base station information, IP address, Wi-Fi information, SSID, BSSID)		
	Push information log (used for you to query push service records and understand the delivery status of push information)		
	Location information (used to provide push notifications targeted at specific regional groups)		
	Software list information (software list and software running list information)		

Article 11 Application and Usage of Information Permission

We may call certain application and information permissions from users. Provided is a list of requested permissions and the reason they are required. Users should note that once they agree to the Privacy Policy, the corresponding device permissions will not be granted by default. When key or sensitive device permissions are required, Finflux will prompt you with a pop-up window to request your consent when you make use of the corresponding function. Once a permission is granted, it may be revoked at any time through your device settings. Refusing to grant device permissions will not affect the normal operation of unrelated functions.

Android Permissions	Description	Usage Scenario and Purpose
android.permission.INTERNET	Allow app to access network	Allow app to access network
android.permission.ACCESS_NETWORK_STATE	Allow app to access network status	Allow app to access network status
android.permission.ACCESS_WIFI_STATE	Allow apps to access Wi-Fi status	Allow apps to access Wi-Fi status
android.permission.FOREGROUND_SERVICE	Allow app to start foreground service	Allow the market ticker widget to obtain real-time market data
android.permission.USE_BIOMETRIC	Allow app to use biometric authentication	Allow for the collection of fingerprint data for security verification
android.permission.USE_FINGERPRINT	Allow app to use fingerprint hardware	
android.permission.VIBRATE	Allow app to use vibrator	1. Receive offline push notifications and trigger a vibration alert 2. Trigger a vibration alert when performing KYC identity

		verification 3. Trigger a vibration alert upon clicking an in-app button
android.permission.WAKE_LOCK	Allows preventing processor from going to sleep or screen dimming	1. Ensure that the screen remains on when performing KYC identity verification 2. Prevent the processor from going to sleep when WorkManager triggers a background task
android.permission.READ_PHONE_STATE	Allow read-only access to phone status	1. Risk control environment determination function, collecting device information (IMEI), network information and location information, etc. 2. Performance and stability analysis, collecting device information (IMEI), network information and location information, etc.
android.permission.CAMERA	Allow app to access the camera device	1. Collect facial data when performing KYC identity verification 2. Collect QR code data when authorizing login through scanning QR code
android.permission.POST_NOTIFICATIONS	Allow app to send notifications	1. Activate the system notification bar when receiving push

		notifications from Aurora
android.permission.READ_EXTERNAL_STORAGE (Below Android 13)	Allows app to read data from external storage	1. Image selection, such as: KYC identity verification, wallet address extraction, etc. 2. Collect photos and video (including audio) information for P2P appeals 3. Collect video (including audio) information as identity credentials for P2P merchants 4. Collect facial video (including audio) information for KYC identity verification on third-party platforms 5. Screenshot sharing to save photo data6. Screenshot detection Risk warning
android.permission.WRITE_EXTERNAL_STORAGE (Below Android 13)	Allow app to write to external storage	
android.permission.SYSTEM_ALERT_WINDOW	Allows app to create a window and display it above all other apps	Floating window for market monitoring
android.permission.SYSTEM_OVERLAY_WINDOW		

android.permission.WRITE_SETTINGS	Allows app to read or write system settings	Save device ID to system settings for fingerprint risk control
Clipboard	Allow app to access clipboard contents	1. Collect the verification code from clipboard when performing identity verification 2. Collect the address from clipboard when adding a wallet address 3. Collect the red packet code from clipboard when receiving a red packet
freemme.permission.msa	Allow obtaining device identifier	Collect device identifiers for fingerprint risk control
com.asus.msa.SupplementaryDID.ACCESS (ASUS Devices)	Allow obtaining device identifier information (OAID)	Collect OAID for fingerprint risk control
com.google.android.c2dm.permission.RECEIVE	Allow creation of IID tokens	Older versions of Google Play services require the creation of IID tokens for FCM push notifications
com.google.android.gms.permission.AD_ID	Allow access to advertising ID	1. Collect advertising ID for FCM push notifications 2. Use of appsflyer traffic attribution analysis
com.kubi.Finflux.permission.JPUSH_MESSAGE	Allow receiving push notifications	Aurora push notifications
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	Allow obtaining installation referrer information	Firebase is used to collect statistics on

		app performance, such as crash information, etc.
com.kubi.Finflux.permission.liantian.RECEIVE	Allow checking whether the license is valid	When starting the app
com.kubi.Finflux.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	Broadcast receivers registered by an application are not exported and are not visible to other applications on the device.	When using the app
android.permission.READ_APP_BADGE com.sec.android.provider.badge.permission.WRITE com.htc.launcher.permission.READ_SETTINGS com.htc.launcher.permission.UPDATE_SHORTCUT com.sonyericsson.home.permission.BROADCAST_BADGE com.sonymobile.home.permission.PROVIDER_INSERT_BADGE com.anddoes.launcher.permission.UPDATE_COUNT com.majeur.launcher.permission.UPDATE_BADGE com.huawei.android.launcher.permission.CHANGE_BADGE com.huawei.android.launcher.permission.READ_SETTINGS com.huawei.android.launcher.permission.WRITE_SETTINGS com.oppo.launcher.permission.READ_SETTINGS com.oppo.launcher.permission.WRITE_SETTINGS me.everything.badger.permission.BADGE_COUNT_READ me.everything.badger.permission.BADGE_COUNT_WRITE	Allow modifying the app's icon	The desktop icon displays a red dot count when receiving a new message
android.permission.ACCESS_ADSERVICES_AD_ID	This permission allows the app to obtain the device's	When use google ad service

	advertising identifier through Google Play services.	
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	This permission allows the app to access data about the effectiveness of advertising campaigns.	When use google ad service
android.permission.BLUETOOTH_ADMIN(Below Android 12)	Allows applications to discover and pair Bluetooth devices	Scan nearby Bluetooth and pair to support hardware wallet transactions.
android.permission.BLUETOOTH(Below Android 12)	Allows applications to connect to paired Bluetooth devices	
android.permission.BLUETOOTH_SCAN(Android 12 and above)	Required to be able to discover and pair nearby Bluetooth devices	
android.permission.BLUETOOTH_CONNECT(Android 12 and above)	Required to be able to connect to paired Bluetooth devices	
android.permission.ACCESS_FINE_LOCATION	Allows an app to access precise location	1. Collect GPS data when entering the Finflux homepage (as required by government regulations) 2. Collect location information to detect nearby Ledger devices. 3. Verify user location when scanning QR codes to claim coupons.
android.permission.ACCESS_COARSE_LOCATION	Allows an app to access approximate location	

iOS Permissions	Description	Usage Scenario and Purpose
Location service	Location service - approximate location	1. Risk control 2. Verify user location when scanning QR codes to claim coupons
Photo	Photo	Identity verification, deposit and withdrawal, scan QR code
Microphone	Microphone recording	Payment through Forter
Camera	Camera	Identity verification, deposit and withdrawal, scan QR code
Face ID	Face Verification	Log in
Network	Network permissions (only for national banks)	First-time network access for domestic devices
Push notification	Push notification permissions	Push notifications
IDFA	Device unique identifier	Data reporting from third-party SDKs like Firebase
Clipboard	Clipboard	1. Collect the verification code from clipboard when performing identity verification 2. Collect the address from clipboard when adding a wallet address 3. Collect the red packet code from clipboard when receiving a red packet

NSBluetoothAlwaysUsageDescription	Bluetooth access permission	Scan nearby Bluetooth and pair to support hardware wallet transactions.

Users may opt to disable some or all requested permissions requested by the app through device settings. The display and configuration of permissions may differ depending on the device. If the corresponding function cannot be found, users may contact the device/system manufacturer for assistance.

Article 12 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 Finflux:

（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 13 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 14 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 Finflux 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 Finflux accounts (e.g., Finflux Wallet account or Finflux 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 & Third Parties: For example, unless prohibited by applicable law, joint marketing partners, resellers or third party service providers may share information about you with us so that we can better understand which of our Services may interest 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 15 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 in 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.

Article 16 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' 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 17 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 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.

(1) **Service Name:** Google Drive
Purpose of Usage: To back up wallet secret phrases to Google Drive
Usage Scenario: When user backup wallet secret phrases
Type: wallet secret phrases
Transfer Method: Data is transmitted over the network
Retention and Usage Period: End users' personal information is retained only for the minimum period necessary to achieve the purpose
Official website: https://www.google.com/drive
Privacy policy: https://policies.google.com/privacy

(2) **Service Name:** Google Authentication
Purpose of Usage: To authorize user's Google account for backing up wallet secret phrases
Usage Scenario: When user backup wallet secret phrases
Type: Personal information(Passwords、Email addresses、Phone numbers、User agents), Device information(IP addresses)
Transfer Method: Data is transmitted over the network
Retention and Usage Period: Firebase Authentication keeps logged IP addresses for a few weeks. It retains other authentication information until the Firebase customer initiates deletion of the associated user, after which data is removed from live and backup systems within 180 days.
Official website: https://developers.google.com/identity
Privacy policy: https://policies.google.com/privacy

(3) **Service Name:** iCloud
Purpose of Usage: Use iCloud features to back up the user's secret phrases to the cloud.
Usage Scenario: When user backup or import wallet secret phrases
Type: Personal information(Passwords、Email addresses、Phone numbers、User agents), Device information(IP addresses),Secret phrase
Transfer Method: Data is transmitted over the network

Retention and Usage Period: End users' personal information is retained only for the minimum period necessary to achieve the purpose
Official website: https://developer-mdn.apple.com/cn/icloud/
Privacy policy: https://www.apple.com/legal/privacy/en-ww/

(4) **Service Name:** Facebook
Purpose of Usage: Attribution and marketing analytics services
Usage Scenario: When the app starts and when the account registration is completed
Type: Device information (operating system、model、language information,、network operator、network type、IP address、Android ID、ADID、IDFA、IMEI、Advertising Source Details、Carrier Name）、Account information(UID)、Credit Card
Transfer Method: Data is transmitted over the network
Retention and Usage Period: End users' personal information is retained only for the minimum period necessary to achieve the purpose
Official website: https://developers.facebook.com/
Privacy policy: https://www.facebook.com/privacy/policy

Article 19 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 Data Transfer.

We may transfer your personal information with our affiliates, trusted third-party partners, and service providers located around the globe. Where we plan to transfer your personal data to third countries or international organizations outside your country of residence that do not benefit from an adequate decision and where additional protections are required, we implement appropriate technical, organizational, and contractual measures to ensure that such transfers comply with the relevant data protection laws.

Article 21 Deletion of personal information.

1. When personal information becomes unnecessary due to the passage of the retention period or the accomplishment of the processing purpose, the Platform shall promptly destroy such personal information.

2. The procedure of personal information destruction is as follows:

A. Once the User has deleted their accounts and not to use any of the services provided by the Platform, the Platform will process the accounts as dormant User and securely manages the personal information of such User in a separate database.

B. Personal information of dormant users will enter the data retention period as set out in Article 3 of the Privacy Policy.

C. The personal information will be destroyed through automatic deletion by the system after the retention period.

3. The method of personal information destruction is as follows:

A. Personal information stored in electronic form is permanently deleted to prevent playback of the record.

B. Personal information recorded or stored on paper documents is shredded or incinerated.

Article 22 Your Rights.

You have the rights to:

(1) **Request information in relation to the collection and use of your Personal Information:** This enables you to be informed at all times about the purposes for processing your Personal Information.
(2) **Request access to your Personal Information**: This enables you to receive a copy of the Personal Information we hold about you and to check that we are lawfully processing it.
(3) **Request correction of the Personal Information that we hold about you**: This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
(4) **Request erasure of your Personal Information**: This enables you to ask us to delete or remove Personal Information where there is no good reason for us continuing to process it, if we have processed your information unlawfully, or where we are required to erase your personal data to comply with local law. We may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at the time of your request.
(5) **Object to processing of your Personal Information:** Where we are relying on a legitimate interest (or those of a third party) and you want to object to processing. In some cases, we may demonstrate that we have legitimate grounds to process your information which can override your objection.

(6) **Request to stop direct marketing**: Where we are processing your personal data for direct marketing purposes, you have the right to notify us in writing requesting that we cease or do not begin processing your Personal Information for direct marketing purposes.
(7) **Request the transfer of your Personal Information to you or to a third party**: We will provide to you, or a third party you have chosen (where technically feasible), your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.
(8) **Withdraw consent at any time where we are relying on consent to process your Personal Information**: You may withdraw your consent for our processing of your Personal Information. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide you with continued access to the Services.
To exercise these rights, please contact us via DataProtection@finfluxnow.com. We will respond to your requests within 72 hours after receiving them.

Article 23 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 24 Data Protection Officer

1. The Platform values the protection of customers' personal information highly and does its best to ensure that their personal information is not damaged, compromised or leaked. However, the Platform shall not be responsible for the information damaged by unexpected accidents that arise from basic dangers inherent at networks and all kinds of disputes that arise from postings made by visitors to the website, even though the Platform has taken technological security measures.

2. The Platform’s customer support center offers swift and sincere replies to customers’ inquiries about the protection of their personal information. In addition, customers who wish to contact the chief privacy officer at the Company may contact him/her by below e-mail. We will answer your inquiries on the protection of personal information swiftly and sincerely.

Data Protection Officer

email: DataProtection@finfluxnow.com

Article 25 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 26 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 27 Publication 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.