

TrustAsia Privacy Policy

Latest Update: November 11, 2024

Welcome to use products and services provided by TrustAsia Technologies, Inc. ("TrustAsia", "we" or "us"). We deeply understand the significance of your personal information and will make every effort to ensure the security and reliability of your personal information. We are committed to maintaining your trust and adhere to the following principles to protect your personal information: Accountability Principle; Purpose Limitation Principle; Consent Principle; Data Minimization Principle; Security Principle; Individual Participation Principle; Transparency Principle, etc. Additionally, TrustAsia commits to adopting corresponding security safeguards in accordance with established industry standards to protect your personal information. Please carefully read and understand this Private Policy (hereinafter referred to as "this Policy", or "this Private Policy") before using our products or service.

This Privacy Policy explains how we will collect, use, share, and disclose your personal information, how we store and safeguard such information, and your rights with respects to your personal information along with how to exercise them. In addition to this Policy, **we may provide real-time notifications (including pop-ups, page prompts, etc.) and feature update notifications in specific contexts to inform you of the corresponding purposes, scope, and methods of information collection. These notifications and updates constitute an integral part of this Policy and have the same legal effect.**

Before you commence use of our products and services, you must carefully read (minors must read under the supervision of a parent or legal guardian) and understand this Policy, with particular attention to the terms highlighted in bold or bold-underline. Only proceed with use after you have fully understood and voluntarily agreed to these provisions.

Specifically, when you proactively provide personal information through relevant pages covered by this Policy or manifest consent to our collection of such information through your actions, we have legitimate grounds to deem that you have fully read, understood, and voluntarily agreed to be bound by this Policy. Upon your voluntary use of this website and related services, this Policy shall become legally effective between you and us.

Contents

I Scope of Application

II How Do We Collect and Use Your Personal Information

III How do We Use COOKIES or Similar Technologies

IV Personal Information That We May Share, Transfer and Disclose

V How Do We Store and Protect Your Personal Information

VI Your Rights

VII Third-Party Services

VIII Our Protection of Minors

IX Our Protection of Personal Information of the Deceased

X How Your Personal Information Is Transferred Globally

XI Notice and Revision

XII How to Contact Us

I Scope of Application

This Policy applies to all products, services and applications provided to you through various websites, APPs, mini-programs, and emerging technological platforms (collectively, “TrustAsia Applications”) operated by TrustAsia and its affiliates. Where standalone privacy policies or similar legal documents (“Subsidiary Policies”) exist for specific products/services, such documents shall constitute an integral part of TrustAsia’s Privacy Framework. In the event of conflicting provisions, the Subsidiary Policies shall prevail.

This Policy exclusively governs **personal information** processed during your use of TrustAsia Applications and related services, **including: (a) your personally identifiable information; (b) information of third parties submitted by you upon obtaining their explicit authorization.** Information attributable to legally distinct entities shall be processed pursuant to executed contracts or mutually agreed arrangements with such entities.

This Policy does not apply to third-party products/services (including WeChat, Alipay, other payment platforms or companies that provide advertising services through TrustAsia) . Your engagement with third-party services shall be governed exclusively by agreements between you and such third parties.

It should be noted that as a user utilizing our products, technologies and services to provide products/services to your own end-users (“Your Users”), you must independently establish privacy policies or equivalent legal instruments with Your Users in compliance with applicable laws.

We collect information strictly necessary for core functionality and utilize such data within proportionate, purpose-bound parameters.

II How Do We Collect and Use Your Personal Information

1. How do we collect your personal information

During your use of TrustAsia applications and related services, personal information may be processed under the following scenarios:

1) Information voluntarily provided to us by you:

We will collect and store information that you actively provide to us when using TrustAsia Applications, including information you actively fill in, information generated when purchasing products/services, or when contacting us.

2) Information automatically collected by us:

When you use TrustAsia's products, services, and applications, we will collect information about your device, location, etc. in accordance with relevant laws and regulations and the scope of your authorization.

3) Information obtained from third parties:

We may also obtain your relevant information from related parties, partners, credit agencies, and other third-party institutions that are legally established and legally retain your relevant information.

2. How do we use your personal information

We provide you with services including but not limited to business consulting, electronic certification, digital certificates, identity authentication, electronic signatures, cryptography, blockchain and its derivative products and technical services. When you use the aforementioned services, we need to collect different types of information from you depending on the content of the service. The scope of information we collect is limited to the relevant information necessary to provide you with the corresponding services, in order to provide you with various services, improve our service quality, and comply with national laws, regulations, and regulatory requirements.

The specific types of services we provide and the corresponding information we collect are as follows:

Personal Information	Purpose of Use	Legal Basis for Processing
Name, Nationality, Mobile Number, E-mail, Verification Codes, Username, APP ID	We use this information to: ● Create and/or validate your account per your request ● Enable password resets ● Provide user support ● Record transactions or issue order confirmations ● Enforce our terms, conditions, and policies	Processing is necessary for the fulfillment of our contract with you to deliver services.
Name, Job Title, E-mail, Phone Number, Supplementary ID Documents (when required), National ID/Passport/Driver's License (for foreign nationals), Username, Live-holding-ID/Passport/Driver's License Photo (for foreign nationals/green card holders)	We use this information to: ● Validate your/your organization's identity for certificate issuance ● Validate CSA membership data ● Display organizational information	
Mobile Number, Username	We use this information to validate whether you possess an existing account.	
Transaction Records (such as the date and time of paying service	We use this information to validate billings, order expenses, and other information. We provide you with access to your	

fees) (necessary information), Bank Card Information, Alipay, Wechat Pay Third-party Account Information (sensitive personal information)	transaction records so that you can view your transaction history.	
Log Information, Device Information, OCSP Query Service	We use this information to improve our services and responses.	Improve our strategy and services to align with our legitimate interests.

1) User Registration

- a) **To become a registered user of TrustAsia Applications:** You can register an account on the TrustAsia Applications registration page by submitting your name, nationality, phone number, email address, and verification codes. Becoming a registered user of TrustAsia Applications will enable us to provide you with the relevant services you need. If you do not provide the required information, you will not be able to use our corresponding services.
- b) **Real - Name Authentication:** If you undergo real - name authentication, we will also collect your ID card/passport photo, facial image, voice recording, video, and any other authentication information required from you. If you are a corporate user, you need to provide photos of your business license, corporate bank account number, and ID card/passport photos of the legal representative/manager and authorized handler. Failure to provide such information will prevent us from offering you products and/or services related to electronic certification, digital certificates, identity authentication, cryptographic technology, and blockchain technology.
- c) **We provide you with channels for feedback.** Specifically, if you wish to consult us about certificate application, renewal, after - sales service, becoming a TrustAsia

partner, or automatic deployment, you can directly communicate with our online customer service via the TrustAsia website or call our hotline to inquire about product/service purchase or usage. During the online conversation, we may need your contact information for further communication. You can decide whether to provide it based on your own needs.

2) Purchase of Products and Services

- a) **Digital Certificate:** When you purchase our digital certificate products and services, we require you to provide **certain personal information (such as name, phone number, ID number, video/photo of holding the ID card, and email address)** to complete the application and validation for certificate issuance.

Additionally, to facilitate the delivery of the digital certificate or service to you, you are required to provide us with **certificate information, service term information, and payment status information** as prompted. The collection of this information is necessary to comply with relevant laws and regulations and to meet the requirements for certificate issuance. Failure to provide such information will only prevent you from obtaining the relevant certificate products and will not affect your ability to browse, search, or use other functions on the corresponding website.

Furthermore, to validate the accuracy and completeness of the information you provide, we will cross - check it with state organs, financial institutions, and enterprises that have legally retained your information. If we need to collect your information from the aforementioned verification entities during the verification process, we will inform them of the source of the personal information in accordance with laws and regulatory requirements and confirm the legality of the source of the personal information.

- b) **Electronic Signatures or Electronic Seals:** Before you use the electronic signature or seal services we provide, you are required to supply us with your digital certificate information, seal information or handwritten signature trace information, the original text or digital digest of the content to be signed, and the result of the digital signature computation. Failure to provide such information will render you unable to utilize our electronic signature or seal services.
- c) **Real-name Authentication Service:** Before you use the real-name authentication service we provide, if you are an individual user, you are required to provide us with

your name, bank account information, real - name mobile phone number, photos of both sides of your ID card, and all the information on the ID card (name, gender, ethnicity, date of birth, address, citizen ID number, personal photo, issuing authority, and the validity period of the document). If you are a foreign national, you will need to provide information from the relevant pages of your passport for validation and authentication, as well as one or more items of identity validation information such as your facial image, voice, or video. If you are a corporate user, you are required to provide one or more of the following details of the legal representative and the person handling the affairs of the company: name, ID number, and mobile phone number. Failure to provide such information will prevent you from using our identity validation service.

When you provide information of another person, you must ensure that you have obtained their lawful and valid authorization and that they also agree to be bound by this Policy. You will be fully responsible for any damages caused to others by the information you provide. The information you provide will remain authorized for our use during your use of our services. If the information owner objects or we become aware that the information owner does not wish to be bound by this Policy, we will delete the relevant information. It should be specifically noted that if there are special requirements by relevant laws, regulations, or policies, the information will be retained for the corresponding period as required by the policy. For example, for digital certificate products, domestic electronic authentication service data must be retained for at least five years after the certificate expires, and international electronic authentication service data must be retained for at least two years after the certificate expires (Matter electronic authentication service data must be retained for at least five years after the certificate expires).

3) Information on the Services You Use and the Manner of Use

During your use of our services, in order to identify the abnormal status of your account, understand product suitability, provide you with basic services such as browsing and searching, ensure the normal operation of the service, and optimize service experience, we may directly or indirectly collect and store information about the services you use and how you use them and correlate them. Such information includes:

- a) **Log information:** When you use our services, we may automatically collect your detailed usage of our services and save them as relevant network logs. For example, your login account, search query content, IP address, browser type, network environment, language used, date and time of visit, and web browsing records, length of stay, refresh records, etc.
- b) **Device information:** We may receive and record information about the device you use when you use our services, such as operating system and version, client version, device identifier (MAC address and other information), location related information (such as IP address).
- c) **Digital Certificate Management Service:** When you use our related products or services for digital certificate operations and management, we need to collect historical data such as browsing and operations generated during your use.
- d) **OCSP Query Service:** When the related products and/or services you use include the OCSP query function, we need to obtain some of your network information, such as device identification, version, IP and other information.
- e) **Notification:** For your contact information (for example, contact email, phone number) that you provide during the use of the service, we may send multiple types of notifications to one or more of them during operation for user message notification, identity verification, security verification, user experience research and other purposes. In addition, we may also send you commercial information about services, functions or activities that you may be interested in by email, text message, or phone call. If you do not want to receive this kind of information, you can unsubscribe through the product or service platform or the unsubscription method presented in the email.
- f) **Payment Settlement:** If there is payment and settlement occurred during our service process, during the payment and settlement process, you can choose the payment service provided by our related parties or third-party payment institutions that cooperate with us (including Alipay, WeChat Pay, Apple Pay, UnionPay, NetsUnion and other payment channels, hereinafter referred to as "payment institution"). During the payment service process, we may need to share your order number and transaction amount information in our service with these payment

institutions so that they can confirm your payment instructions and complete the payment.

- g) **Order Information Management:** In order to display the order information of your account and protect your after-sales rights and interests, we will collect **order information, transaction and consumption records, and virtual property information (sensitive personal information)** generated during your use of our services to show them to you and facilitate your order management. In the event of a transaction refund, we may ask you to provide your bank account information, including **bank card information, Alipay, and WeChat Pay third-party account information (sensitive personal information)** to process your refund request.
- h) **Transaction Status Confirmation and Post-Sale Dispute Resolution:** In order to confirm the transaction status and provide you with after-sales and dispute resolution services, we will collect **your transaction and payment information** related to the progress of the transaction through the transaction partner and payment institution you selected based on the transaction, and share such transaction and payment information with the relevant above-mentioned service providers.
- i) **Customer Response:** When you contact our customer service personnel or use other user response functions (such as submitting after-sales requests, personal information protection complaints or suggestions, other customer complaints and needs), we may require you to provide necessary personal information to match and verify your user identity, in order to protect your account and system security. We may also save your **contact information (sensitive personal information) (that you use when contacting us or other contact information that you actively provide to us), the content of your communication/call recordings with us, and the content of your feedback in the platform response function (including text/picture/audio/video/call recordings, etc.), and other necessary information related to your needs**, so as to get in touch with you or help you solve problems, or record the treatment plans and results of the related problems.
- j) **Provide You with Security:** In order to improve the security of using the services provided by us and our partners, protect the personal and property safety of you or other users or the public from infringement, better prevent risks such as phishing websites, fraud, network vulnerabilities, computer viruses, network attacks,

network intrusions, and more precisely identify violations of laws and regulations or our service-related agreements, we may collect, use or integrate your **account information, transaction information, device information, log information, and information shared by our related parties and partners with your authorization or in accordance with the law**, to comprehensively judge your account and transaction risks, conduct identity verification, detect and prevent security incidents, and take necessary recording, auditing, analysis, and disposal measures in accordance with the law.

- k) **Improve Our Service:** We may invite you to participate in surveys about our services to help us improve existing services or design new services; at the same time, we may use your information for website updates.
- l) **For Other Reasonable and Necessary Purposes:** If a product/service that needs to collect your personal information is not specified in this Privacy Policy, or we go beyond the stated purpose and have a direct or reasonable relationship with the collection of your personal information, we will separately explain to you by updating this Privacy Policy, page prompts, pop-up windows, in-site letters, website announcements or other methods convenient for you to know before collecting and using your personal information, and provide you with a way of consent for independent choice, and collect and use it after obtaining your express consent.

You understand and agree that device information and log information alone cannot identify a specific natural person. If we combine the aforementioned information with other personal information to identify a specific natural person, or use it in conjunction with information that can identify a natural person, we will anonymize and de-identify such personal information during the period of combined use, except as otherwise authorized by you or required by laws and regulations. During the period of combined use, we will process and protect this information in accordance with this Policy.

4) Exceptions to Authorization and Consent

According to relevant laws and regulations, in the following circumstances, collecting and using your personal information does not require your authorization or consent:

- a) Related to the performance of obligations stipulated by laws and regulations;

- b) Directly related to national security and national defense security;
- c) Directly related to public security, public health, or major public interests;
- d) Directly related to criminal investigation, prosecution, trial and execution of judgments;
- e) Necessary for the conclusion and performance of a contract to which you are a party, or necessary for the implementation of human resources management in accordance with legally established labor regulations and collective agreements.
- f) For the protection of your or other personal life, property and other major legitimate rights and interests, but it is difficult to obtain the consent of the person;
- g) The collected personal information is either disclosed to the public by yourself or already publicly available through lawful means;
- h) Personal information is collected from legally disclosed information, such as legal news reports, government information disclosure and other channels;
- i) Necessary to sign and perform a contract according to your request;
- j) Necessary for legal news reporting;
- k) Other circumstances specified by laws.

III How do We Use COOKIES or Similar Technologies

To ensure the normal operation of our services and provide you with a more convenient access experience, we may obtain and use your information through COOKIES or similar technologies, and store such information as log information. A COOKIE is a small amount of data that is sent from a web server to your browser and stored on your computer's hard disk.

We use our own COOKIES or similar technologies, which may be used for the following purposes:

- 1) Remember your identity. For example, COOKIES or similar technologies can help us identify you as our registered user, or save your preferences or other information provided to us;
- 2) Analyze your use of our services. We can use COOKIES or similar technologies to understand what activities or services you use the service for.

You should be able to control whether and how cookies are accepted by your browser. Please consult the documentation accompanying your browser for further information. If you refuse our use of COOKIES and similar technologies to collect and use your relevant information, you can manage or reject COOKIES and/or similar technologies through your browser's settings, provided that your browser has this function. Alternatively, you can delete COOKIES and/or similar technologies that have been stored on your computer, mobile device, or other device.

You understand and are aware that some of our products/services can only be realized through the use of COOKIES or similar technologies. If you refuse to use or delete COOKIES or similar technologies, you may not be able to use our related products/services properly or obtain the best service experience through our products/services, and may also have a certain impact on your information protection and account security.

IV Personal Information That We May Share, Transfer and Disclose

1 Sharing

We attach great importance to the protection of your personal information. Unless otherwise agreed by you, we will not share your information with any third party other than us, except in the following circumstances:

- 1) Obtained your prior explicit consent or authorization, or in response to your lawful request and consent.
- 2) The sharing necessary to implement our contractual purposes/services/functions. In some cases, in order for your normal use of the services you need, we need to share your information with third parties to achieve the functionality of our products and/or services, including:
 - a) sharing corresponding transaction order information and payment amount information with third-party payment institutions that provide payment services;
 - b) To provide you with specific products and services to fulfill contractual purposes, it is necessary to share with the corresponding suppliers, service providers, partners, and node operators to process the personal information you provide, obtain comparison results, and ultimately deliver the specific products and services to you. With your knowledge and explicit consent, we will collect and share certain personal information with them, which specifically includes: **the name, mobile phone number, email address, position, ID card number, and photo or video of the person holding the ID card of the person handling the affairs.**

If you are purchasing specific products and services on behalf of one or more companies, you will also need to provide **the name and ID card number of the legal representative of the corresponding company, identity verification information of the person handling the affairs, and supplementary documents to prove personal identity (if necessary).** You must inform and obtain the explicit consent of the data subject, that is, for the purpose of fulfilling the contract / service / function, we need to share with the corresponding suppliers, service providers, partners, and node operators to process the personal information you provide,

obtain comparison results, and ultimately deliver the specific products and services to you.

3) Necessary sharing with related parties. To facilitate your unified management, ensure system and account security, your personal information may be necessary to be shared between us and our related parties, including:

- a) Information related to your account will be shared within our products and our related parties as necessary to help you save time and simplify the operation process.
- b) Your account information, device information, and other information reflecting your usage habits and preferences may be shared with our related parties to provide you with a consistent and personalized browsing, advertising, and other service experience across our products, services, and applications and those of our related parties.

4) To achieve the other purposes described in the first Article How Do We Collect and Use Your Personal Information of this Policy.

5) Fulfill the provisions under this Policy or other agreements (including electronically signed agreements and corresponding platform rules) we have entered into with you.

6) To comply with relevant laws and regulations, or to safeguard national interests, public interests, and in accordance with applicable laws and regulations, to protect the business secrets of us and our affiliates or partners, and the property or safety of you or other service users from harm (for example, to prevent fraudulent and other illegal activities and to reduce credit risks), we may exchange information with third parties. The aforementioned information does not include information disclosed for the purpose of profit, such as being sold, rented, or shared.

7) Provide your information at the lawful request of your guardian.

We will only share your personal information for legitimate, reasonable, necessary, specific, and clear purposes. We will sign strict non-disclosure agreements with companies, organizations, and individuals with whom we share personal information, and require them to process the personal information you provide with the same or higher level of confidentiality measures.

2 Transfer

If we sell or purchase any business or undergo a merger, we will disclose information to third parties. In such cases, we will disclose your data to potential buyers of such businesses. If we engage in sales, mergers, or collaborations with other companies or businesses, or sell part or all of our assets, we will also disclose information to third parties. In these transactions, user information may be included in the transferred assets. If any of the aforementioned situations occur, we will notify you in advance through website announcements or other forms.

3 Disclosure

We will only disclose your information under the following circumstances and under the premise of adopting safety protection measures that comply with industry standards:

- 1) According to your needs, disclose the information you specify in a disclosure method that you explicitly agree to.
- 2) In cases where it is necessary to provide your information based on legal, regulatory, mandatory administrative or judicial requirements, we may disclose your information based on the type of information and disclosure method required. On the premise of complying with laws and regulations, when we receive the above request for disclosure of information, we will require the recipient to provide corresponding legal documents, such as subpoenas or investigation letters.

We carefully review all requests and provide your personal information to the relevant institutions only after ensuring that the requests are legally valid and that the institutions have the right to obtain such personal information for specific investigative purposes.

4 Exceptions to Obtaining Prior Authorization When Sharing, Transferring, or Disclosing Information

Under the following circumstances, sharing, transferring, and disclosing your information does not require your prior authorization and consent:

- 1) Directly related to national security, national defense security, public safety, public health, or significant public interests;
- 2) Directly related to criminal investigation, prosecution, trial and enforcement of judgments, etc.;
- 3) Necessary for the conclusion and performance of a contract to which you are a party, or necessary for the implementation of human resources management in accordance with legally established labor regulations and collective agreements;
- 4) Necessary for the performance of statutory duties or legal obligations;
- 5) In response to sudden public health incidents, or in emergency situations where it is necessary to protect the life, health, and property safety of persons.
- 6) Processing your personal information that you have disclosed yourself or that has been legally disclosed within reasonable limits, except where it has a significant impact on your rights and interests or where you have expressly refused;
- 7) Processing your personal information within reasonable limits for the purpose of conducting news reporting, public opinion supervision, and other activities in the public interests;
- 8) Other circumstances specified by laws and regulations.

According to legal regulations, sharing, transferring, or disclosing de-identified personal information, provided that the data recipient cannot recover and re-identify the personal information subject are not acts of external sharing, transfer, and public disclosure of information. The storage and processing of such data will not require separate notice to you and your consent.

V How Do We Store and Protect Your Personal Information

1 Personal Information Storage

1) The Location of Information Storage

The information we collect and generate during our operation within the territory of the People's Republic of China will be stored in China, except for the following circumstances:

- a) Clearly stipulated by laws and regulations;
- b) Obtaining your authorization and consent;
- c) Transmission of personal information collected within the territory to overseas entities is necessary for the purchase/usage of the products or services and is essential to achieve the contractual purposes.

With regard to the transfer of personal information abroad, we and our partners and suppliers comply with the applicable laws for the cross-border transfer of personal information between different countries/regions, ensuring that your personal information is adequately protected, for example through anonymization and secure storage.

2) The Duration of Information Storage

During your use of our products and/or services, your personal information will be retained for as long as the purposes for which it was collected or used are being served, and will also be subject to any mandatory retention periods required by law. For example, in accordance with the relevant requirements of the Electronic Signature Law of China, the retention period for information must be at least five years after the electronic signature certification certificate becomes invalid. After the retention period has expired, we will delete your personal information or anonymize it as required by applicable law.

3) The Method of Information Storage

Stored by means of paper, electronic, optical, magnetic, or similar methods.

2 Personal Information Protection

We attach great importance to your personal information security. We use various security technologies and procedures, and take all reasonable and feasible measures to protect your information from loss, improper use, unauthorized access or disclosure.

1) Data Security Protection Measures

We use security protection measures that meet industry standards, including the establishment of proper regulations and the development of security technologies, to

prevent your information from unauthorized access, use, and modification, and to prevent data damage or loss. Network services have adopted a variety of encryption technologies. For example, we use encryption techniques (e.g., TLS) to encrypt and protect your data, and adopt isolation technologies for secure isolation. When using information, such as information display and information associative computing, we use a variety of data desensitization technologies to enhance the security of information in use. We adopt strict data access control and multiple identity authentication to protect information from being abused.

2) Other Security Measures Taken for Information Protection

We manage and standardize the storage and use of information by establishing a data classification and grading system, data security management specifications and data security development specifications.

We implement comprehensive security control over data through non-disclosure agreements, monitoring and auditing mechanisms.

We also hold security and privacy protection training courses to strengthen employees' awareness and understanding of personal information protection policies and relevant regulations.

We only allow TrustAsia employees and partners who need to know this information to access your information, and have established a strict access control and monitoring mechanism. We also require all persons who may have access to your information to fulfill corresponding confidentiality obligations. Failure to meet these obligations may result in legal action or termination of the partnership with TrustAsia.

3) Security Incident Handling

In order to deal with possible risks such as personal information leakage, damage and loss, we have formulated a number of systems to define the classification and grading standards of security incidents and security vulnerabilities and the corresponding processing procedures. We have also set up a specific emergency response team for processing security incidents. The team will conform to the requirements of security incident handling and launch emergency plans for different security incidents to stop losses, analyze situation, locate issue, formulate remedial measures, and cooperate with relevant departments to trace and crack down on security incidents. We also regularly organize internal training and

emergency drills to help our relevant personnel to understand the corresponding emergency response strategies and procedures.

In the event of an information security incident, we will promptly inform you in accordance with the requirements of laws and regulations, **including the basic situation and possible impact of the security incident, the response measures we have taken or will take, and the suggestions on your independent prevention and risk reduction, the remedies for you, etc.** At the same time, we will promptly inform you of the situation related to the incident by email, letter, phone call, push notification, etc. If there is difficulty in informing the information subject one by one, we will issue an announcement in a reasonable and effective manner. Meanwhile, we will also actively report the handling of information security incidents in accordance with the requirements of the regulatory authorities.

Please understand that due to technical restrictions and limitations in risk prevention, even if we do our best to enhance security measures, we cannot always guarantee one hundred percent of information security. You need to understand that the system and communication network you use to access the service may have problems due to factors beyond our control.

The Internet is not an absolutely secure environment. Moreover, communication methods such as email, instant messaging, social software, or other service software cannot be guaranteed to be fully encrypted. We recommend that you use complex passwords and pay attention to protecting your information security when using these tools. If our physical, technical, or managerial protective measures are compromised, resulting in unauthorized access to, public disclosure of, alteration of, or destruction of information, and thereby causing damage to your legitimate rights and interests, we will assume the corresponding legal liability.

Please be sure to properly keep your account, password and other identity elements. When you use our services, we will identify you through your account, password and other identity elements. Once the aforementioned information is disclosed, you may suffer losses and adverse effects. If you find that your account, password and/or other identity elements may or have been leaked, please contact us immediately so that we can take corresponding measures in a timely manner to avoid or reduce relevant losses.

By submitting your personal information through TrustAsia platforms, you agree and authorize TrustAsia to collect, use, share, and protect the personal information you provide.

If you wish to withdraw your authorization for any special reason, please contact us promptly so that we can take the necessary actions.

VI Your Rights

You can access and manage your personal information in the following ways:

1 Access

You have the right to access your personal information, except as otherwise provided by laws and regulations. If you wish to exercise your data access rights, you may do so through the following means:

- 1) If you want to access or edit your basic personal information in your account, change your password, add authentication methods, or make other security-related changes, you can perform these settings by logging into your account.
- 2) If you are unable to access this personal information through the above methods, you may contact us through the feedback channels specified in this Policy. After verifying your identity, we will provide you with the relevant information, except as otherwise provided by laws and regulations or as otherwise agreed in this Policy.

2 Correcting or Supplementing Your Personal Information

When you find that the personal information we process about you is inaccurate, you have the right to request that we correct or supplement it. You may submit a request for correction or supplementation through the methods described in “1 Access.” If you are unable to access this personal information through the aforementioned means, you may contact us through the feedback channels specified in this Policy.

We will respond to your request for correction or supplementation within 30 days.

3 Delete Your Personal Information

You may delete certain personal information on your own through the methods described in “1 Access.”

You may request us to delete your personal information in the following circumstances:

- 1) If our processing of personal information violates laws and regulations;

- 2) If we collect or use your personal information without obtaining your explicit consent;
- 3) If our processing of personal information breaches our agreement with you;
- 4) If you no longer use our products or services, you may proactively contact your account manager or use the contact information specified in this Policy to apply for account cancellation;
- 5) If we no longer provide you with products or services, except as otherwise required by relevant laws, regulations, or policies.

If we decide to honor your deletion request, we will also notify the entities that have obtained your personal information from us and require them to delete it promptly, unless otherwise required by laws and regulations or unless these entities have obtained your independent authorization.

When you correct, supplement, or delete your personal information, we may not immediately delete the corresponding information from our backup systems, but we will delete this information when the backup is updated, except as otherwise required by laws and regulations.

4 Changing the Scope of Your Consent

Certain basic personal information is required for each product, service, or application to function. For the collection and use of any additional personal information, you may grant or withdraw your consent at any time.

You can do this by deleting or modifying your personal information, contacting us, or reaching out to our staff member assigned to you.

Once you withdraw your consent, we will cease processing the relevant personal information. However, your decision to withdraw consent will not affect the processing of personal information that was conducted based on your prior authorization.

5 Account Cancellation by the Information Subject

You may cancel your previously registered account at any time through the following methods:

- 1) Contact your account manager;
- 2) Call the hotline number provided in this Policy.

After account cancellation, we will cease to provide you with products or services and will delete your personal information as requested, except as otherwise required by laws and regulations.

6 In Response to Your Above Request

For security purposes, we may ask you to verify your identity before processing your request. For your reasonable request, we do not charge fees in principle, but for repeated requests that exceed reasonable limits, we will charge a certain cost depending on the circumstances. For those that are unnecessarily repetitive, require excessive technical means (for example, requiring the development of new systems or fundamental changes in existing practices), pose a risk to the legal rights of others, or are very impractical (for example, involving information stored on backup magnetic tapes), we may deny the request.

We will not be able to respond to your request in the following circumstances:

- 1) Related to our fulfillment of obligations stipulated by laws and regulations;
- 2) Directly related to national security and national defense security;
- 3) Directly related to public security, public health, and major public interests;
- 4) Directly related to criminal investigation, prosecution, trial and execution of judgments;
- 5) We have sufficient evidence to demonstrate that you have subjective malice or abuse of rights;
- 6) For the protection of your or other personal life, property and other major legitimate rights and interests, but it is difficult to obtain the consent of the person;
- 7) Responding to your request will cause serious damage to the legitimate rights and interests of you or other individuals or organizations;
- 8) Those involving trade secrets.

VII Third-Party Services

TrustAsia Applications may access or link to the services (including websites or other forms of service) provided by third parties or other similar applications (such as in the form of embedded codes, plug-ins, etc.).

Currently, the third-party service providers we access mainly include the following types:

- 1) Used for message push function, including in-site push notifications, specific event reminder, etc.;
- 2) Used for payment-related services, including order payment, transaction verification, income settlement, payment information summary statistics, etc.;
- 3) Used for behavior verification and interface access limit functions, including behavior verification services for critical operations such as sending text messages, sending emails, changing passwords, and changing API keys;

When you use services provided by third parties within TrustAsia, these third parties may collect user information from you. After obtaining your explicit consent, the third party may obtain your name, phone number, and other information necessary for providing the third-party service. As for the information you voluntarily provide to the third party while using their services, we will regard it as your permission for the third party to obtain such information. Regarding the information generated while you use the third-party service, it should be agreed upon by you and the third party in accordance with the law regarding the collection and use of such information. **Before providing information to a third party, we will make commercially reasonable efforts to assess the legality, legitimacy, and necessity of the third party's information collection. We will enter into relevant legal documents with the third party and require them to handle your personal information in compliance with laws and regulations and the signed legal documents, and to take protective measures for your information. If you refuse to allow the third party to collect, use, or transfer the aforementioned information while providing the service, it may result in your inability to use the corresponding third-party services within the TrustAsia Applications. However, this will not affect your use of other functions of TrustAsia.**

Third-party push, payment, behavior verification or other third-party services are operated by relevant third parties. Your use of such third-party services (including any information you provide to such third parties) is subject to the third party's own terms of service and information protection statement (not this Policy), and you need to read their terms carefully. **This Policy only applies to the personal information we collect, and does not apply to any services provided by third parties or information usage rules of third parties. If you find that there may be risks involved in these third-party services, it is recommended that you terminate the relevant operations to protect your legal rights and contact us in time.**

VIII Our Protection of Minors

Our products, websites and services are primarily intended for adults. Minors under the age of 14 shall not create their own user accounts without the consent of their parents or guardians. In cases where we process the personal information of minors under the age of 14 with the consent of their parents or guardians, we will only provide or publicly disclose such information when required by judicial or administrative authorities, with the explicit consent of the parents or guardians, or when necessary to protect the minors under the age of 14.

If we discover that we have collected personal information from minors under the age of 14 without obtaining verifiable parental consent in advance, we will endeavor to delete the relevant data as soon as possible.

IX Our Protection of Personal Information of the Deceased

We will protect the personal information of the deceased in accordance with the Personal Information Protection Law of the People's Republic of China. Where a user (natural person only) dies, his/her close relatives may, for the purpose of their own lawful and legitimate interests, exercise such rights as consulting, copying, correcting and deleting the relevant personal information of the deceased via the contact methods listed in Article XI How to Contact Us of this Policy, unless otherwise arranged by the deceased prior to his/her death.

You understand and confirm that in order to fully protect the rights and interests of the deceased user's personal information, the close relatives of the deceased user who apply for exercising the rights of this article need to follow the specific procedures of TrustAsia and submit the deceased user's identity certificate, death certificate, identity documents of the applicant, kinship certification documents of the applicant and the deceased user, and provide the type and purpose of the right to be exercised.

X How Your Personal Information Is Transferred Globally

Under normal circumstances, personal information that we collect and generate within the territory of China will be stored within the territory of China.

To meet the needs of certificate application, since the final validation party for some of our products is an overseas partner, this means that, after obtaining your authorization and consent, your personal information may be transferred to jurisdictions outside the country/region where you purchased the product/service, or accessed from these jurisdictions.

These jurisdictions may have different data protection laws, or may not have relevant laws at all. In such cases, we will ensure that your personal information is protected to a level equivalent to that within the territory of China. For example, we will request your consent for the cross-border transfer of personal information and, in accordance with the requirements of relevant domestic laws and regulations, sign standard contracts for the cross-border transfer of personal information with the overseas parties.

Regarding the cross-border transfer of personal information, your information will ultimately be transferred to the terminal enterprises listed in the table below, depending on the type of actual product/service.

Company Name	DPO Contact Number	Contact E-mail
Sectigo Limited	+001 2017094352	eric.staudinger@sectigo.com
DigiCert, Inc.	+001 8017019600	dpo@digicert.com
GMO GlobalSign Ltd.	+44 1622766766	dpo@globalsign.com
Asseco Poland S.A.	+48 426756360	daneosobowe@assecods.pl

XI Notice and Revision

We may amend this Privacy Policy and notify you of the updates. Any modifications to this Policy will form part of the Policy. For material changes, we will inform you through more conspicuous notifications (including website announcements, push notifications, pop - up prompts, or other means). If you do not accept the revised terms, please cease using our services. We encourage you to review this Privacy Policy at any time to understand how we protect your personal information. Material changes referred to in this Policy include, but are not limited to:

- 1) Major changes in our service model, such as the purpose of processing personal information, the type of personal information processed, and the way of using personal information;
- 2) Major changes in our ownership structure, such as changes in owners caused by business adjustments, and bankruptcy mergers;
- 3) Major changes in the main objects of personal/organizational information sharing, transfer or public disclosure;
- 4) Major changes in your right to participate in the processing of personal/organizational information and its exercising method;
- 5) Major changes in the responsible department, contact information and complaint channels for handling personal/organizational information security;
- 6) Occurrence of other circumstances that are important or may seriously affect your personal rights and interests.

With any revision we make your satisfaction a top priority. We encourage you to review our TrustAsia Privacy Policy each time you use our services. If you continue to use TrustAsia services after the revision of this Policy, it indicates that you have fully read, understood, and accepted the revised Policy and are willing to be bound by it.

XII How to Contact Us

You can contact us via the following methods:

- 1) If you have any questions, comments or suggestions about the content of this Policy, you can contact us by sending an email to support@trustasia.com or by a call to 400-880-8600;
- 2) If you find that your personal information may be leaked, you can complain and report it by sending an email to support@trustasia.com or by a call to 400-880-8600;

Generally, we will deal with it within fifteen working days after receiving your question, comment or suggestion and verifying your user identity. If you are dissatisfied with our handling, you can file a complaint or report to the department responsible for personal information protection.

Name of operating entity: TrustAsia Technologies, Inc.

Office Address: F/32 Building B. New Caohejing International Business Center, 391 Guiping Rd, Xuhui District, Shanghai, China

- 3) We may periodically revise this Privacy Policy in accordance with laws and regulations or business adjustments.

You need to understand that we will only collect, use, process, and store your personal information in accordance with the revised Privacy Policy after you have confirmed and agreed to the changes. You have the right to refuse to agree to the revised Privacy Policy. However, please be aware that if you refuse to agree to the revised Privacy Policy, it may result in your inability to use or continue to fully utilize the relevant services and features of TrustAsia, or to achieve the desired service outcomes.