Privacy Policy

Effective Date: January 1, 2025

Introduction

systhoframe LIMITED ("systhoframe," "we," or "us") respects your privacy and is committed to ensuring the confidentiality and security of your personal data and other information. When you visit and use Synthoframe ("the Product") and other services provided by systhoframe, we will collect, process, and disclose your information in accordance with this Privacy Policy ("this Policy").

We collect information from corporate/organizational users, their end users, and individual users (hereinafter collectively referred to as "you"). The specific service platforms may include websites, PC software, mobile applications, etc. This Policy will help you understand how we collect, use, and disclose your personal data and assist you in exercising your privacy rights.

Before accepting this Policy, please read it carefully, especially the **bolded clauses**. You should pay special attention to these clauses and confirm that you have fully understood and agreed to them before using the Product and other services. If you or your legal guardian do not agree with any part of this Policy, you should immediately stop using the Product and other services. If you are unable to accurately understand or agree to any part of this Policy, please do not access or use the Product or any other services provided by systhoframe. Your confirmation by clicking on the website, or your actual use of the Product or other services provided by systhoframe, will be deemed as your reading, full understanding, and agreement to be bound by the contents of this Policy.

If you have any questions, comments, or suggestions regarding the content of this Policy, you can contact us through the various contact methods provided herein.

This Policy will help you understand:

---

1. Scope of This Policy

This Policy applies when you agree to it and begin using any of our products and services, regardless of whether that product and service has its own separate privacy policy, and regardless of whether you are a browsing user (visitor) or a registered user.

Please note that this Policy does not apply to the following situations:

- Information collected by third-party services (including any third-party websites) accessed through our products and/or services.

- Information collected by other companies or organizations that place advertisements in our products and/or services.

Please be aware that if you provide your personal data to third-party websites or services while browsing or using them, your information will be subject to that third party's privacy statement or similar agreement. We are not responsible for any misuse or disclosure of the information you provide to third parties, regardless of whether you logged in or browsed the aforementioned websites or software, or used their products and/or services, through a link or recommendation from systhoframe. We strongly recommend that you understand and confirm their privacy protection status before using third-party services.

---

2. Definitions

Personal Data: Any information relating to an identified or identifiable natural person.
Applicable Privacy Laws: Any national, federal, EU, state, provincial, or other privacy, data security, or data protection law or regulation that applies to the processing of user information.
Sub-processor: An authorized third party that processes the personal data of a controller on behalf of a processor to provide part of the services and/or related technical support.
Anonymized Data: Information that cannot be traced back to a natural person by using other information that can be reasonably exploited.
Product Service: Multiple functions that the Product can provide and enable for customers, including but not limited to data collection and analysis.
EU GDPR: Regulation (EU) 2016/679 of the European Parliament and of the Council of April 27, 2016, on the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
The meanings of terms such as "data subject," "processing," "controller," and "processor" used in this Policy are defined by the Applicable Privacy Laws; if there is no such meaning or law, they are defined by the EU GDPR.

---

3. Processing of Personal Data

3.1 Roles of the Parties

As a corporate/organizational user, if you use the Product and related services to process personal data, you acknowledge that systhoframe is a
"processor" that processes the end user's personal data on your behalf , and that you determine the means and purposes of the processing ("controller"). You represent that you will comply with any Applicable Privacy Laws at all times, including but not limited to having a valid legal basis for processing such data, such as obtaining the prior consent of the end user. In this case, the Synthoframe Data Processing Addendum will apply where applicable.

3.2 Personal Data We Collect

We collect personal data in four ways: information provided by your organization, information you provide, information collected automatically, and information collected from other sources. More details are as follows. We will take reasonable and practical measures to avoid collecting irrelevant personal data. If you do not provide the relevant information, you may not be able to register as our user or use and enjoy certain products and services we provide, or the expected effects of the relevant products and/or services may not be achieved.

In the process of providing services to you, we will collect, use, store, disclose, and protect your personal data in accordance with the terms of this Policy. If it is necessary to collect personal data beyond the scope of this Policy, we will provide you with a separate explanation of the scope and purpose of the information collection before collecting the necessary information to provide the corresponding service. If you choose not to provide the aforementioned information, it may affect your use of the relevant services.
You authorize us to process your personal data during your use of our products and services. If you cancel your account, we will stop using and delete or anonymize your personal data within a reasonable period. However, for the purposes of resolving disputes, establishing legal defenses, conducting audits, pursuing legitimate business purposes, enforcing our agreements, and/or complying with applicable laws, some information will continue to be retained for a certain period until the period stipulated by law expires or the purpose for retaining the information is no longer necessary. In addition, please note that since anonymized data cannot identify or be associated with you, it is not considered personal data. Therefore, we do not need to obtain your authorization or consent to store and process anonymized data, and we do not need to notify you.

3.2.1 Information Your Organization Provides

Personal profile information: Your personal data may be provided by your company/organization. When your company/organization opens an account for you to use the Product and/or services, it will provide some of your personal data, including your account name, corporate email address, department/organizational structure, job title, etc. You acknowledge and confirm that your company/organization has obtained your authorization to submit the aforementioned information to us.

3.2.2 Information You Provide

To help you become our user: We collect the information you provide when you create a Synthoframe account. When you create a Synthoframe account, you must provide us with an account name, login password, and your mobile phone number or email address. The mobile phone number or email address you submit is used for registration, login, account binding, password retrieval, and receiving verification codes. It is also one of the designated contact methods for you to receive relevant business notifications (including new product releases, service changes). After completing the Synthoframe account registration, you can add additional information to your personal profile, including (1) other personal data such as your gender and work location; and (2) contact information such as your address and/or contact number. Not providing such additional information will not affect your normal use of Synthoframe services. The information of category (1) you provide will help us better understand your needs so that we can introduce targeted products to you; the information of category (2) will help us promote and publicize products, mail business notifications (including bills), or conduct business communication with you in the manner described. If you only need to use the browsing and searching services of the Synthoframe website, you do not need to register as our user or provide the aforementioned information.
To provide you with services: According to relevant laws and regulations, we may require you to provide real identity information for real-name authentication, and you should provide the relevant necessary information through your account. To facilitate your provision of such information, we provide real-name authentication based on your mobile phone number. You can also choose an appropriate method based on your identity attributes. You understand and agree that systhoframe has the right to independently or entrust a third party to review the authenticity, accuracy, and validity of the information you provide for real-name authentication.
Input content: When you use Product Services that utilize AI technology, we collect the text commands, keywords, and other content you input (collectively referred to as "input content").

3.2.3 Information Collected Automatically

Device information: Based on the specific permissions you grant during software installation and use, we will receive and record your device information (including device model, operating system version, device settings, unique device identifiers, and other hardware and software characteristics) and device location-related information (including IP address, GPS location, Wi-Fi access points, Bluetooth, and base stations and other sensor information that can provide relevant information). We may associate the above two types of information to provide you with consistent services on different devices.

Log information: When you use the services provided by our website or client applications, we will automatically collect detailed information about your use of our services as network logs, including your search query content, IP address, browser type, telecom operator, language used, date and time of access, and records of the webpages you have visited.

User account support information: Based on your use of the Product Services, we will record and analyze information including user consultation records, fault reports, and troubleshooting processes (including call records or communications) to respond to your help requests more promptly and improve our services.

Audio, video, and photo information: When you use specific functions of our services (including voice search, scanning, and taking photos), we will collect the above information after obtaining your specific permission. Refusing to provide this information will only prevent you from using the above functions but will not affect your normal use of other functions of our products and/or services. In addition, you can turn off the relevant functions in the permission management settings of your mobile device at any time.

Location information: When you enable the device location function and use our location-based products and/or services, we collect your location-related information, including: when you use our products and/or services through a mobile device with a location function, geographical location information collected through GPS or Wi-Fi, etc. You can stop us from collecting your geographical location information at any time by turning off the location function, but you may not be able to use the relevant services or functions, or the expected effects of the relevant services may not be achieved. After turning off the location function, you can still obtain corresponding location-based Synthoframe services by manually entering the geographical location.

Payment-related information: In order to help you successfully complete the subscription, cancellation of subscription, payment, and refund for paid product services, and to provide you with continuous customer service, technical support, and other services during the subscription period, we will require you to provide complete contact information and payment/refund account information.

Crash data, performance data, and other diagnostic data: To ensure the security of our services and better understand the operational performance of the Product, we may record information related to your use of the application, including usage frequency, crash data, overall usage, performance data, and other diagnostic data.

Information collected by default using mobile applications: When you use a mobile application, it may be necessary to request certain device permissions to collect corresponding personal data and provide you with relevant business functions or services. The following are the business functions related to iOS and Android system permissions, the purpose of requesting these permissions, and whether your permission will be sought in advance. The interface and method for disabling these permissions may be different on different devices (such as devices using the Android system); for specific details, please contact the device and system developers.

iOS Permissions:

Permission	Business Function/Service	Purpose	Ask before enabling?	Can the user disable the permission?

Network Access	Connect to the network; download necessary data.	Connect to the network; download necessary data.	No	Yes
Network Status	Determine network status; provide necessary prompts when the network is abnormal.	Determine network status; provide necessary prompts when the network is abnormal.	No	Yes
WIFI Status	Determine network status; provide necessary prompts when the network is abnormal.	Determine network status; provide necessary prompts when the network is abnormal.	No	Yes
Keep screen awake	Keep the screen on.	Keep the screen on.	No	Yes
Vibrate	Provide necessary vibration notifications when the user long-presses the screen display window.	Provide necessary vibration notifications when the user long-presses the screen display window.	No	Yes

Android Permissions:

Permission	Business Function/Service	Purpose	Ask before enabling?	Can the user disable the permission?
Network Access	Connect to the network; download necessary data.	Connect to the network; download necessary data.	No	Yes
Network Status	Determine network status; provide necessary prompts when the network is abnormal.	Determine network status; provide necessary prompts when the network is abnormal.	No	Yes
WIFI Status	Determine network status; provide necessary prompts when the network is abnormal.	Determine network status; provide necessary prompts when the network is abnormal.	No	Yes
Keep screen awake	Keep the screen on.	Keep the screen on.	No	Yes

Vibrate	Provide necessary vibration notifications when the user long-presses the screen display window.	Provide necessary vibration notifications when the user long-presses the screen display window.	No	Yes

3.2.4 Information Collected from Other Sources

Account information:

- When you use the services of our affiliates or partners, they may share your account information with us under your authorization.
- If you log in or otherwise connect to use our services, we will request your personal data from a third party. For personal data that we need but the third party has not provided, we will still require you to provide it. If you refuse to provide it, you may not be able to use certain functions of our products and/or services normally. If you agree to provide it, you will authorize us to read the relevant information registered in your third-party account (such as nickname, profile picture, etc.).
- We will confirm the legitimacy of the source of personal data in accordance with the Applicable Privacy Laws and the agreement with the third party. We will process your personal data obtained from third parties in compliance with the Applicable Privacy Laws.

3.3 How We Process Your Personal Data

3.3.1 We process your personal data for the following purposes:

Provide necessary information: To provide services to you, we will send you necessary information, notifications, or communicate with you on business matters, including but not limited to verification codes necessary to ensure the completion of the service, and push notifications necessary when using the service.

Provide and improve better products and/or services: We perform data analysis to provide you with higher quality products and/or services, further understand how you access and use our products and/or services, and respond to your personalized needs, such as language settings, location settings, personalized help services and instructions, or otherwise respond to you and other users.

Deliver ads and marketing to you: To display information tailored to your personalized needs, we use your service usage information to create feature models and user profiles, and to display and push information and potential commercial advertisements to you, including but not limited to news about our products, market events, promotional offers, promotional information from our third-party partners, or other content you may be interested in. Such information will be clearly marked as "tailored," and if you do not wish to receive our commercial emails, you can reply by following the instructions in the message or use the unsubscribe method provided in the message to withdraw your consent.

Design, develop, and promote new products and services: We may design, develop, and promote brand new products and services based on personal data statistics; we will conduct statistics on the usage of our services and may share these statistics with the public or third parties, but these statistics do not contain any of your personal data.

Enhance the security of our services: To improve the security of your use of services provided by us and our partners, ensure a safe operating environment, identify abnormal account status, protect the personal and property safety of you, other users, or the public from infringement, better prevent phishing websites, fraud, network vulnerabilities, computer viruses, network attacks, network intrusions, and other security risks, and more accurately identify violations of laws and regulations or our relevant agreements and rules. We may process your account information, integrate device information, relevant network logs, and information

legally shared by partners to assess your account and transaction risks, conduct identity verification, detect and prevent security incidents, and take necessary recording, auditing, analysis, and processing measures in accordance with Applicable Privacy Laws.
Maintain and enhance the security and stability of the Product: Manage software authentication or software upgrades.
Collect product feedback: Allow you to participate in surveys about our products and services, or surveys initiated through our products and services. Your participation in surveys will be entirely at your discretion, and you can choose what information to provide.
Others: For security, legal investigation, and other purposes, we may aggregate, analyze, and mine your data (including for commercial use), but such information should be anonymized data.

3.3.2 If we process your personal data beyond the purposes described at the time of collection, or the processing of your personal data exceeds the scope of direct or reasonable relevance, we will notify you again and obtain your explicit consent.

3.3.3 In order to provide you with a better service experience, improve our products and/or services, or for other purposes you have agreed to, subject to compliance with Applicable Privacy Laws, we may, with your explicit consent, use the information collected through one of our products and/or services in an aggregated or personalized manner for other products and/or services we provide that you use. For example, information collected when you use one of our products or services may be used to provide specific content or display information related to you in another product or service you use, rather than universally pushed information.

3.4 Our Legal Basis and How We Process Your Personal Data

We can only process your personal data when we have a "legal basis" to do so. We use different legal bases depending on the different reasons for processing your personal data (in other words, the "purpose" of our processing). These legal bases are: consent, contractual necessity, legitimate interests (of us or a third party), compliance with a legal obligation, performance of a public interest task, and protection of vital interests. Here, we explain the legal bases we rely on when processing your personal data.

3.4.1 Your Consent

We will process your personal data with your prior explicit consent. If you have agreed to our processing of your personal data, we will only process it for the purposes specified in this Policy. You have the right to withdraw your consent, but your withdrawal will not affect the legality of our processing of your personal data before that. Please note that if our processing is based on your consent and you refuse or withdraw your consent, we may not be able to provide certain services related to that personal data.

3.4.2 Contractual Necessity

If you have the legal capacity to enter into an enforceable contract, when you register, access, or use the Product and its services, we will process the user information necessary for the conclusion or performance of a contract with you. This means we process your information to activate the products and services you have purchased, provide software update notifications, and provide customer support, etc.

3.4.3 Legitimate Interests

We will process your personal data when it is necessary for the purposes of a legitimate interest (whether of us or a third party), provided that these interests are not overridden by your interests or fundamental rights and freedoms.
Your rights: When we process your personal data on the basis that it is necessary for the purposes of a legitimate interest pursued by us or a third party, you have the right to object and seek to limit our use.

3.4.4 Compliance with Legal Obligations

We may process your personal data if it is necessary for compliance with a legal obligation. This includes our obligations to take measures to ensure user safety or comply with valid legal requests, such as orders or disclosure requirements from regulatory agencies, law enforcement agencies, or courts.

3.4.5 For the Performance of a Public Interest Task

We may process your personal data if it is necessary for the performance of a public interest task, including conducting research, preventing and detecting crime, protecting children and promoting public safety, security, and integrity, which are provided for by Applicable Law.
Your rights: When we process your personal data on the basis that it is necessary for the performance of a public interest task, you have the right to object and seek to limit our use.

3.5 How We Share Your Personal Data

3.5.1 Principles

Under normal circumstances, we will not share, transfer, or disclose your personal data with any other organizations or individuals, except in the following situations:

- **Obtain explicit consent:** After obtaining your explicit consent, we may share your personal data with other parties as needed to provide you with specific services. If a third party intends to use the information for purposes beyond the scope of the original authorization and consent, they must obtain your consent again.
- **Legal conditions:** We may share your personal data with others based on legal and regulatory requirements (including those related to national security or defense), litigation and arbitration awards, or requests lawfully made by administrative and judicial authorities. In addition, in order to fulfill statutory obligations or duties, we may share necessary personal data.
- **Emergency situations:** When it is necessary to respond to public health emergencies, or in an emergency to protect the life and health and property safety of a natural person, we may share your personal data.
- **Public interest:** We may share your personal data when it is necessary within a reasonable scope for public interest, such as news reporting and commentary activities.
- **Information that has been made public:** We may share personal data that you have made public on your own and personal data collected from legally public sources (such as legal news reports, government information disclosure, and other channels).
- Other situations stipulated by laws and regulations.

You fully understand and agree that the sharing, transfer, and public disclosure of anonymized data, and ensuring that the data recipient cannot restore and re-identify the data subject, does not constitute external sharing, transfer, and public disclosure of personal data. The storage and processing of such data do not require separate notification and your explicit consent.

3.5.2 Service Providers

Partnering with third-party Software Development Kit ("SDK") service providers: Our Synthoframe mobile product includes SDK plugins provided by our authorized partners. These third-party SDKs may collect or process some of your personal data/device permissions (see the table below for details). We conduct strict security checks on the relevant SDKs and use technical measures to ensure that they process personal data in accordance with this Policy and any other relevant confidentiality and security measures. We will promptly inform you on this page of the latest situation regarding the collection of user information by third-party SDKs. Due to version upgrades, policy adjustments, and other reasons, the types of data processed by third-party SDKs may undergo certain changes, and you can visit the third-party SDK's page for more information.

Name	Usage Scenario	Types of Information Collected	Device Permissions
Posthog	Logging	User information, user behavior information, device information, page error logs	None

We may share personal data with third-party vendors who provide services or functions on our behalf, including the following service providers: (i) providing Product Services; and (ii) providing the information, products, and other services you request. In order to provide you with the functions/services you choose, we need to share the necessary personal data with the relevant third party. Third-party services include storage services provided by Amazon Web Services, real-name authentication services provided by Google LLC, and AI model services provided by Open AI L.L.C. and Anthropic, PBC. Some cookies and similar technologies may also be provided by third parties. Service providers can only access and collect information to the extent necessary to perform their functions and are not allowed to share or process the information for any other purpose.

If you are an end user of a corporate/organizational user and your corporate/organizational user administrator chooses to activate, manage, and use a third-party product or service through our Product, we may need to share the information necessary for you to activate, manage, and use such third-party product or service with that third-party service provider; otherwise, you will not be able to use that third-party service. When the corporate/organizational user administrator activates a third-party service, they must read, fully understand, and comply with the product functions and privacy policy of the third-party service.

Similarly, if you, as an individual user, choose to activate, manage, and use a third-party product or service through our software, you agree that we share the necessary information with that third-party service provider; otherwise, you will not be able to use that third-party service. When you activate a third-party service, you must read, fully understand, and comply with the product functions and privacy policy of the third-party service.

3.5.3 Third Parties

With your consent, when you use your Synthoframe account to log in to a third-party product or service, we will share your basic information (name, profile picture) and other information you have authorized with the aforementioned third party.

3.5.4 Affiliates and Authorized Partners

We may entrust trusted partners to provide services, and therefore, we may share some of your personal data with our partners to provide better customer service and optimize the user experience. We will only share your personal data for legitimate, proper, necessary, specific, and explicit purposes, and will only share the personal data necessary to provide the service. Our partners are not authorized to use the shared personal data for any other purpose.

3.5.5 Transfer

If systhoframe merges, is acquired, or undergoes bankruptcy liquidation with another legal entity, or other situations involving mergers, acquisitions, or bankruptcy liquidation, and if personal data is transferred, we will require the new holder of your personal data to continue to be bound by this Policy, otherwise we will require the company, organization, or individual to re-obtain your authorization and consent.

3.5.6 Information You Voluntarily Share with Others

You can use our website to report issues encountered in searches and provide reviews, etc., to help other users get more accurate information.

You can use our sharing function to share your personal data with specific or non-specific social contacts (e.g., various social platforms). Before sharing, please fully consider the trustworthiness of the information recipient. We recommend that you check the privacy statement of the social network or third-party service provider you use to understand how they handle your information and make an informed decision.

3.5.7 Public Disclosure

We will only publicly disclose your personal data in the following situations:

- With your explicit consent or based on your voluntary choice, we may publicly disclose your personal data.
- In order to protect the personal and property safety of Synthoframe users, affiliates, or the public from harm, we may disclose your personal data in accordance with Applicable Privacy Laws or the terms of the relevant agreements and rules of the Synthoframe platform.
- **Legal obligations and rights:** If required by law, legal process, litigation, or mandatory requirements of government authorities, we may publicly disclose your personal data.

3.5.8 Sub-processors

For corporate/organizational users, we use certain sub-processors to assist us in providing Product Services to you. You can find the latest list of our sub-processors here, including their names, the subject, nature, and duration of their processing of personal data, their location, and relevant data security information.

---

4. Cookies and Similar Technologies

4.1 What are Cookies

To ensure the normal operation of the website, to provide you with a more convenient access experience, and to recommend content that you may be interested in, we will store small data files called Cookies on your computer or mobile device. Cookies usually contain an identifier, the site name, and some numbers and characters. systhoframe can only read the Cookies it provides.

4.2 How We Use Cookies

With the help of Cookies, your preferences or paid service purchase data can be stored. When you visit again next time, we will display the information you need; or systhoframe can identify your referral website through Cookies so that systhoframe can track the effectiveness of its own advertisements.

4.3 Your Rights

We will not use Cookies for any purpose other than those stated in this Policy. You can manage Cookies according to your preferences and can also clear all Cookies saved on your computer or mobile device. Most

web browsers have the function of blocking Cookies. However, if you do so, you will need to change the user settings every time you visit our website. For details on how to change browser settings, please visit the relevant settings page of the browser you are using.

4.4 Similar Technologies We Use

In addition to Cookies, we may also use other similar technologies on the website, such as web beacons and pixel tags. For example, the emails we send to you may contain address links to our website content. If you click on this link, we will track this click to help us understand your preferences for products or services, so that we can proactively improve the customer service experience. Web beacons are usually transparent images embedded in websites or emails. With the help of pixel tags in emails, we can know whether the email has been opened. If you do not want your activities to be tracked in this way, you can unsubscribe from our mailing list at any time. However, be sure to carefully check the information in the emails and links. Due to the limitations of current technology and the various malicious attack methods that may exist, even if we do our best to strengthen security measures, we cannot always ensure the security of the information. Therefore, we strongly recommend that you take active measures to protect the security of your personal data, including but not limited to using complex passwords, regularly changing passwords, and not disclosing your account password and other personal data to others.

---

5. Data Security and Retention

5.1 systhoframe attaches great importance to the security of your information.
We strive to take various reasonable physical, electronic, and managerial security measures to protect personal data and prevent unauthorized access, public disclosure, use, modification, damage, or loss of personal data. We use pseudonymization and encryption technologies to improve the security of personal data; we use trusted protection mechanisms to prevent malicious attacks on personal data; we deploy access control mechanisms to ensure that only authorized personnel can access personal data; we organize security and privacy protection training courses to raise the awareness of employees of the importance of protecting personal data.

5.2 We will take all reasonable and practicable steps to avoid collecting irrelevant personal data.
We will only retain your personal data for the period necessary to achieve the purposes outlined in this Policy, unless an extended period is permitted by Applicable Privacy Laws. After the aforementioned personal data retention period expires, we will proceed to delete or anonymize your personal data.

5.3 Please understand that due to the limitations of the internet industry and the rapid development of technology and the possibility of various malicious attack methods, even if we do our best to strengthen security measures, we cannot always ensure the security of the information.
Therefore, we strongly recommend that you take active measures to protect the security of your personal data, including but not limited to using complex passwords, regularly changing passwords, and not disclosing your account password and other personal data to others.

5.4 In the event of an unfortunate personal data security incident (leakage, loss, etc.), we will promptly notify you in accordance with Applicable Privacy Laws: the basic situation of the security incident and its possible impact, the measures we have taken or will take to handle it, the independent prevention and risk reduction advice you can rely on, and remedial measures.

We will promptly notify you of the relevant information about the incident via email, letter, phone, push notification, etc. When it is difficult to notify data subjects one by one, we will publish an announcement in a reasonable and effective manner. At the same time, we will also report the handling of the personal data security incident in accordance with the requirements of the regulatory authorities.

5.5 Please note that the internet is not an absolutely secure environment, and when you interact with others through third-party social software, emails, and text messages embedded in our website, regarding your geographical location, whereabouts, or other information, we are not sure whether the third-party software is fully encrypted during the information transmission process.
Please be sure to ensure the security of your personal data.

5.6 If the product and services cease to operate, we will take reasonable measures to protect the security of your personal data, including timely cessation of further collection of personal data;
The notice of cessation of operation will be notified to users in the form of one-on-one service or an announcement; the personal data held will be deleted or anonymized.

5.7 We will store the collected user personal data within Singapore, specifically on Amazon Web Services. Amazon Web Services will assist us in providing data storage security services for you. If you use the AI functions of the Product Service, we will store the input content and generated output content in the United States and other regions, including Singapore.

---

6. Data Subject Rights

You have rights and choices over your personal data. For individual users, we are responsible for responding to your requests within the relevant period specified by Applicable Privacy Laws. For end users of corporate/organizational users, please submit your request to the relevant corporate/organizational user, and we will be responsible for responding to the request of the corporate/organizational user within the relevant period specified by Applicable Privacy Laws.

6.1 Access Your Personal Data

You can access your personal data in the following ways:

- **Account information:** You can log in to the website or client application to query, manage, update, and delete the basic information and contact information submitted when using the service, and perform account association or identity verification.
- **Usage information:** You can view your usage record information on our website, client applications, and other services, and you can also contact us through the methods provided at the end of this Policy to access such information. Please note that in order to ensure the authenticity of your exercise of rights, we will provide you with your personal data after verifying your identity, unless otherwise stipulated by Applicable Privacy Laws.
- **Other information:** If you encounter operational problems during this access or need to obtain personal data that was not previously available, you can contact us through the methods provided at the end of this Policy, and we will provide it after verifying your identity, unless otherwise stipulated by Applicable Privacy Laws.

6.2 Correct Your Personal Data

If you need to change the real-name authentication information of your Synthoframe account, you need to contact us through customer service, phone, email, etc., and we will assist you with the corresponding operations.
After verifying your identity, and on the premise that the correction does not affect the objectivity and accuracy of the information, you have the right to correct or update incorrect or incomplete information, which you can do yourself on our website or client application; or in some cases, especially when the data is incorrect, submit your correction request to us through the contact information provided at the end of this Policy to ask us to correct or update your data, unless otherwise stipulated by Applicable Privacy Laws. However, for security and identification reasons, you may not be able to modify some of the initial registration information submitted when you registered.

6.3 Delete Your Personal Data

In accordance with Applicable Privacy Laws, you can submit a request to us via email to delete your personal data in the following situations:

- The purpose of processing has been achieved or is no longer necessary;
- We stop providing the product or service, or the retention period has expired;
- You have withdrawn your consent;
- Our processing of your personal data violates laws, administrative regulations, or agreements; and
- Other situations stipulated by Applicable Privacy Laws.

When we respond to your deletion request, we will also notify the entities that have obtained your personal data from us to delete it in a timely manner, unless otherwise required by laws or regulations, or these entities have obtained your independent authorization. When you delete your information from our services, we will delete or anonymize your personal data within a reasonable period.

6.4 Copy Your Personal Data

If you need to copy your personal data, you can contact us through the methods provided at the end of this Policy. After verifying your identity, we will provide you with a copy of your personal data that we have processed during the provision of services (such as basic information, identity information), unless otherwise stipulated by laws and regulations

6.5 Withdraw Your Consent

If you want to change the authorized scope of relevant functions (including location, address book, camera), you can modify your personal settings through your device, or make modifications in the relevant function settings interface of our product or service. If you encounter operational problems during this process, you can contact us through the methods provided at the end of this Policy. When you withdraw your authorization for us to collect relevant personal data, we will no longer collect the information, and we will not be able to provide you with the corresponding services mentioned above. Your withdrawal of consent will not affect the legality of our processing of your personal data before that.

6.6 Cancel Your Account

You know and understand that this Product is a corporate product/service, and your account is dependent on the company's management. You can directly close/delete your account by contacting your company, or by contacting our customer service to provide you with an effective account cancellation form (unless otherwise required by laws and regulations). Once you (or your company) cancel your account, you will not be able to use our services. To protect your or others' legitimate rights and interests, we will judge whether to support your cancellation request based on your use of our products. For example, if your paid service period has not expired, we will not immediately support your request, but will notify you of the remaining

service period first. Unless otherwise required by laws and regulations, after your account is canceled, all information in your account will be cleared, and we will delete your personal data according to your request. If you authorized logging into our services through a third-party account (such as Instagram, Facebook, etc.), you need to apply to the third party to cancel your account.

6.7 Restrict the Processing of Your Personal Data

You have the right to request a restriction on the processing of your information in the following situations: (a) you are contesting the accuracy of the information, (b) the information has been processed unlawfully but you oppose its deletion, (c) you need the information to be retained for the establishment or defense of a legal claim, or (d) you have objected to the processing and are waiting for the outcome of that objection request. You can contact us to exercise your rights: support@synthoframe.com.

6.8 Object to the Processing of Your Personal Data

You also have the right to object to the processing of your information in certain circumstances. This right applies when we are performing a public interest task, pursuing a legitimate interest of ours or a third party, or in certain situations where your data is used to promote scientific or historical research. When submitting an objection request, please provide all relevant information, including the processing activity you are objecting to, the reasons for your objection, and how the processing activity affects you, as well as any additional information that you believe will help us review your request. We will stop the specific processing if we do not have a compelling legitimate reason to continue the processing or if it is not required for a legal claim. You can contact us to exercise your rights: support@synthoframe.com.

6.9 Migrate Your Personal Data

In cases where we have a contractual necessity or consent as a legal basis, you have the right to data portability. This means you have the right to receive your information in a structured, commonly used, and machine-readable format and to share it with a third party. You can contact us to exercise your rights: support@synthoframe.com.

6.10 File a Complaint

You have the right to file a complaint with the competent supervisory authority about how we process your personal data, or to file a lawsuit in a court with jurisdiction. You can directly submit a personal data rights request to us via email: support@synthoframe.com. Generally, we will process your request within one (1) month of receiving it. In special circumstances, we may delay our response to you with an appropriate explanation, but this delay will not exceed one (1) month. If you are not satisfied with our response, especially if you believe that our personal data processing behavior has harmed your legitimate rights and interests, you can also seek a solution by filing a lawsuit in the court of the domicile or registration place of systhoframe LIMITED.

6.11 Be Notified in Advance of the Cessation of Our Products and Services

If some or all of our products and services are forced to cease operations for special reasons, we will notify you fifteen (15) days in advance on the homepage of the product or service or on the website, or contact you through email or other appropriate means, and we will stop collecting your personal data. At the same time, the personal data we hold will be deleted or anonymized in accordance with Applicable Privacy Laws, unless otherwise stipulated by laws and regulations.

6.12 Request Us to Explain Personal Data Processing Rules

In some business functions, we may make certain business decisions based on automated decision-making mechanisms, including information systems and algorithms, such as displaying personalized recommendations to you. If you believe that these decisions have seriously affected your legitimate rights and interests, you have the right to ask us to explain the rules for processing your personal data, and we will provide you with sufficient remedies accordingly.

6.13 Response to the Above User Requests

For security purposes, users may be required to provide a written request or otherwise prove their identity. We may ask users to verify their identity before processing the request. For your reasonable requests, we do not charge a fee in principle, but for repetitive requests that exceed a reasonable limit, we will charge a certain cost fee depending on the situation. We may refuse requests that are unnecessarily repetitive, bring inconvenience in practice (for example, developing a new system or making fundamental changes to existing practices), pose a risk to the legitimate interests of others, or are very impractical (for example, involving information stored on backup tapes), and inform you of the reasons for the refusal.
However, please note that in the following situations, in accordance with the requirements of laws and regulations, we will not be able to respond to your requests for correction, deletion, cancellation, etc.:

- Directly related to national security and defense security;
- Directly related to public safety, public health, and major public interests;
- Directly related to criminal investigation, prosecution, trial, and execution of judgments;
- There is sufficient evidence that you are malicious or abusing your rights;
- Responding to your request will cause serious harm to your or other individuals' and organizations' legitimate rights and interests;
- Involving trade secrets.

7. Minor Users

7.1 The products and services we provide are mainly for adults.
Minors are not allowed to create their own user accounts without the consent of their parents or guardians. If you are a minor under sixteen (16) years of age, we require you to ask your parents or guardians to read this Policy carefully and only use our services or provide us with information after obtaining their consent.

7.2 In the case of collecting personal data of minors with the consent of parents or guardians to use our products or services, we will only use, share, transfer, or disclose this information to the extent permitted by laws and regulations, with the explicit consent of the parents or guardians, or when it is necessary to protect the minor.

7.3 If we find that we have collected personal data of a minor without prior verifiable parental consent, we will delete the data as soon as possible, and we are not responsible for any losses caused to you by such deletion.

7.4 If a guardian has any reason to believe that we have collected personal data of a minor without the guardian's consent, please contact us through the contact information specified at the end of this Policy, and we will take measures to delete the relevant data as soon as possible.

8. Our Global Operations and Data Transfer

8.1 The personal data collected and generated by our operations is stored within Singapore and the United States, unless in the following situations:

- Applicable Privacy Laws have clear provisions;
- Your explicit authorization has been obtained;
- You conduct online cross-border transactions or other personal voluntary actions.

8.2 In the above situations, we will ensure that your personal data is fully protected in accordance with this Policy.

---

9. Privacy Policy Updates

9.1 As products and services are continuously updated and changed, this Policy may change to comprehensively and promptly inform you of the personal data processing rules.

9.2 We will not reduce your rights under this Policy without your explicit consent.
We will publish any changes we make to this Policy on a dedicated page.

9.3 For major changes, we will also provide a more prominent notice (including for some services, we will notify you through website promotions or even provide pop-up prompts to explain the specific changes to this Policy), and we will reserve a reasonable period for you to consider whether to accept these changes before they take effect.
If you continue to use our products and services after the new version of the policy and user agreement takes effect, it means that you have fully read and are willing to be bound by the updated policy and user agreement. If you do not agree to such changes, you can stop using our products and services.

9.4 The major changes mentioned in this Policy include but are not limited to:

- Major changes in our service framework, such as the purpose of personal data processing, the type of personal data processing, the method of personal data processing, etc.;
- Major changes in our ownership structure, organizational structure, etc., such as changes in ownership due to business adjustments, bankruptcy mergers, etc.;
- Major changes in the main recipients of personal data sharing, transfer, or public disclosure;
- Major changes in your rights to participate in personal data processing and the way they are exercised;
- Changes in the department, contact information, or complaint channels responsible for personal data security;
- When the data protection impact assessment report shows high risk.

---

10. Contact Us

If users have any questions or comments on the content of this Policy or its implementation and operation, please contact us. You can send your questions to support@synthoframe.com. If you want to contact our Data Protection Officer, you can contact us through the above email and address.

Generally, we will reply within one (1) month of receiving your request. In special circumstances, we may delay our reply to you with an appropriate explanation, but this delay will not exceed three (3) months. If you are not satisfied with our response, especially if you believe that our personal data processing behavior has harmed your legitimate rights and interests, you can also seek a solution by filing a lawsuit in the court of the domicile or registration place of systhoframe LIMITED.

Appendix: Additional Clauses for Applicable Privacy Laws

Part A - Additional Clauses for EEA, UK, and Swiss Data Protection Legislation

Part A of this Appendix applies only to users located in the European Economic Area ("EEA"), the United Kingdom ("UK"), or Switzerland. In these regions, we comply with the provisions and requirements of the EU GDPR regarding the processing and protection of your personal data. In the EEA, UK, and Switzerland, the general terms of this Policy (Sections 1-10) and this Appendix together constitute our notice of our personal data processing practices and govern our personal data processing practices. The general terms shall prevail over any content not mentioned in Part A of this Appendix, but if the content of Part A of the Appendix conflicts with the general terms, the content of Part A of this Appendix shall prevail.

Data Transfer

If personal data is transferred outside the EEA, UK, or Switzerland, we ensure that the following measures are taken for legal transfer, for example:

- The recipient of the personal data is located in a country that has been granted an "adequacy" decision by the European Commission.
- The recipient has signed the "Standard Contractual Clauses" based on the European Commission's decision, which requires the recipient to protect your personal data.
- In the absence of appropriate safeguards, we will obtain your explicit consent for the transfer of your personal data.
- At the same time, we will use appropriate technologies, such as encryption or de-identification, to protect your personal data.
-

Part B - Additional Clauses for U.S. State Privacy Laws

Part B of this Appendix applies only to users located in the state of California ("California"), with the exception of Section 2.5, which applies to all U.S. residents. In this region, we comply with the provisions and requirements of the California Consumer Privacy Act of 2018 (as amended by the California Privacy Rights Act of 2020) and its implementing regulations (collectively, the "CCPA & CPRA") regarding the processing and protection of your personal data. In California, the general terms of this Policy and this Appendix together constitute our notice of our personal data processing practices and govern our personal data processing practices. The general terms shall prevail over any content not mentioned in Part B of this Appendix, but if the content of Part B of the Appendix conflicts with the general terms, the content of Part B of this Appendix shall prevail.

1. Sale and Sharing of Your Personal Data (in the past twelve (12) months)

In this section, we will inform you of the types of personal data we have sold or shared in the past twelve (12) months, the types of recipients of the personal data, and the purpose of the sale or sharing. According to the definition of the CCPA & CPRA, "sharing" means a business sharing, renting, publishing, disclosing, disseminating, making available, transferring, or otherwise communicating a consumer's personal data to a third party, orally, in writing, electronically, or otherwise, for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including a transaction between a business and a third

party for the benefit of the business for cross-context behavioral advertising where no monetary exchange occurs.

Sale of your personal data (in the past twelve (12) months): We do not currently sell your personal data to any third party. If we sell your personal data in the future, we will notify you in advance through this Appendix and respect your right to limit or refuse this action.

Sharing of your personal data (in the past twelve (12) months): Please refer to Section 3 of the general terms of this Policy for specific details. In principle, we do not provide services for children (in Part B of this Appendix, a child is defined as a natural person under sixteen (16) years of age). However, please note that we do not have the ability to identify age. Therefore, we cannot determine whether the personal data we share contains personal data of children.

2. Data Subject Rights

Right to know what data is being collected before collection: You have the right to know what personal data we have collected about you, including the categories of personal data, the categories of sources from which the personal data is collected, the commercial purpose for collecting, selling, or sharing personal data, the categories of third parties to whom the personal data is provided, and the specific personal data fields we have collected about consumers. For how to exercise this right, please refer to Sections 3.2 and 3.3 of the general terms of this Policy.

Access to your personal data: You have the right to access your personal data. For how to exercise this right, please refer to Section 6.1 of the general terms of this Policy.

Deletion of your personal data: You have the right to request that we delete your personal data. For how to exercise this right, please refer to Section 6.3 of the general terms of this Policy. However, if any of the following situations occur, we may choose not to respond to your deletion request:

- Completing the transaction for which the personal data was collected, fulfilling a written warranty or product recall provision under federal law, providing a product or service requested by the user or reasonably expected by the user in the context of the business relationship with the user, or otherwise performing a contract between the business and the user;
- Helping to ensure the security and integrity of user personal data to the extent that processing such information is reasonably necessary and appropriate;
- Debugging to identify and repair errors that impair existing intended functionality;
- Exercising freedom of speech and ensuring the ability of other users to exercise their own freedom of speech or other rights provided by law;
- Complying with the California Electronic Communications Privacy Act, Penal Code Part 2, Chapter 12, Section 3.6 (Section 1546 et seq.);
- Engaging in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to or complies with all other applicable ethical and privacy laws, where deleting the information may make it impossible to complete or seriously impair the ability to complete the research;
- Solely for internal uses that are reasonably consistent with the user's expectations based on the user's relationship with the business and are compatible with the context in which the information was provided.

Correction of your personal data: You have the right to request that we correct incorrect personal data we have collected. For how to exercise this right, please refer to Section 6.2 of the general terms of this Policy.

Opt-out of the sale or sharing of your personal data: If you are a U.S. resident, you can opt-out of the "sharing" of personal data for cross-context advertising purposes as defined by the California Consumer Privacy Act ("CCPA") by contacting us at support@synthoframe.com. We do not sell customer personal data.

Equal service: You have the right not to receive discriminatory treatment for exercising your privacy rights under the CCPA, including:

- Refusing to provide you with products or services;
- Charging different prices or rates for products or services, including through the use of discounts or other benefits or imposing penalties;
- Providing products or services to you at a different level or quality of service;
- Suggesting that a user will receive products or services at a different price or rate, or a different level or quality of product or service;
- Other discriminatory measures.

However, please understand that the provision of various functions of our products and services depends on the processing of certain personal data. When you choose to restrict us from processing certain personal data, you should understand that the functions associated with it will become unavailable.

Privacy rights response report: If you need information about our response to privacy rights, please contact us at support@synthoframe.com.