

Privacy Policy

Last updated at 2024-08-08

Attention:

Thank you for using YouCloud! Your trust is very important to us. We are well aware of the importance of personal data to you. We will take appropriate protective measures according to the requirements of laws and regulations, and try our best to keep your personal data safe. Therefore, the Service Provider of YouCloud (hereinafter referred to as "YouCloud" or "We", "Us", "Our") formulates this Privacy Policy and reminds you:

This Privacy Policy applies to all the products and services of YouCloud, including but not limited to PC, web pages, providing third-party websites and application programming interfaces (APIs), and products and services that are innovated continuously.

If a certain service or services provided by YouCloud to you with separate privacy policies, the separate privacy policies and this Privacy Policy will constitute the complete Privacy Policy and take effect at the same time.

It should be noted that this Privacy Policy does not apply to services provided to you by other third parties. In order to ensure a smooth product experience, you may receive content or web links provided by third parties. Please choose carefully whether to access links, content, products and services provided by third parties, and read the privacy policies carefully before submitting personal data to third parties.

Before using our products or services, please read and understand this Privacy Policy carefully. Especially the terms marked in bold or bold underline, please read them carefully, and use them after confirming your full understanding and agreement.

If the service purchased by the user is YouCloud 365, please pay special attention to this clause. YouCloud 365 is a To B commercial application for enterprise organizations. User confirms and guarantees that you have the right to register a YouCloud 365 account on behalf of your organization and have obtained the authorization from your organization to serve as the administrator of the YouCloud 365 account. User knows, understands and confirms that as a YouCloud 365 administrator, you have the right to open account seats for other personnel of your organization according to the purchase, and at the same time, opening account seats to others means that you guarantee that you have the right to agree to and be bound by this Privacy Policy on behalf of the other account seat users, and



have management responsibilities for the other account seat users to ensure that they comply with this Privacy Policy.

Please note that we will check and update our Privacy Policy from time to time, and the relevant measures will change accordingly. We kindly request you to visit this page regularly to ensure you are always aware of the latest version of this Privacy Policy. After reading this Privacy Policy, if you have any questions or matters about it, you can send an email to feedback@youcloud.com to communicate with us.

By using or continuing to use the services of YouCloud, you agree to our collection, use, storage and sharing of your personal data in accordance with this Privacy Policy.

Part I-Explanation

1. "YouCloud" means the service products of YouCloud, including but not limited to PC (<https://youcloud.com/>).
2. "The Service Provider of YouCloud" means the team and organization that develops and provides the service products of YouCloud and services.
3. "Children" means minors under the age of fourteen.
4. "Personal Data" means various information recorded electronically or in other ways that can identify a specific natural person or reflect the activities of a specific natural person either alone or in combination with other information, but does not include anonymized information.
5. "Personal Sensitive Data" means personal private information including ID number, personal biometric information, bank account number, property information, whereabouts, transaction information, children's data, etc. (We will clearly identify specific Personal Sensitive Data in bold).
6. "Deletion of Personal Data" means the act of removing personal data from systems involved in the realization of daily business functions, so that it cannot be retrieved or accessed.
7. "Equipment" means devices that can be used to access our products and/or services, such as desktop computers, laptops, tablets or smartphones.
8. "Unique Device Identification Code (Exclusive ID or UUID) " means a string of characters programmed into the device by the device manufacturer, which can be used to uniquely identify the corresponding device (such as IMEI/android ID/IDFA/OpenUDID/GUID /SIM card IMSI information, etc.). Unique device identifiers are used in a number of ways, one of which is to serve advertisements when Cookies cannot be used (such as in mobile applications).



9. "IP address". Each device connected to the Internet will be assigned a number, which is called an Internet Protocol (IP) address. These numbers are usually assigned by geographic area. An IP address is often used to identify where a device is located when it is connected to the Internet.
10. "SSL", also known as Secure Socket Layer, is a security protocol implemented on the transmission communication protocol (TCP/IP). SSL supports various types of networks and provides three basic security services at the same time, all of which use public key and symmetric key technology to achieve the effect of data confidentiality.
11. "Cookie". A Cookie is a small file containing a character string, which is sent and stored on your computer, mobile device or other device (usually encrypted) when you log in and use a website or other network content. Similar technologies of Cookies are other technologies that can be used for similar purposes to Cookies, such as Web Beacon, Proxy, embedded scripts, etc.
12. "Account". When you register an account and provide us with some personal data, you can better use our services. When you access YouCloud, the system will use these personal data to authenticate you to prevent unauthorized personnel from accessing your account.
13. "Anonymization" means the process of technically processing personal data, making it impossible for the subject of personal data to be identified or associated, and the processed data cannot be restored.
14. "De-identification" means the process of technically processing personal data, making it impossible for the subject of personal data to be identified or associated without additional information.
15. "Server log". Normally, our server will automatically record the webpage requests you make when you visit the website. These "server logs" typically include your web request, Internet Protocol address, browser type, browser language, date and time of your request and one or more Cookies that can uniquely identify your browser.

Part II-Privacy Policy

This Part of Privacy Policy will help you understand the following:

1. How do we collect and use your personal data
2. How do we use Cookies and similar technologies
3. How do we share, transfer and publicly disclose your personal data
4. How do we protect your personal data
5. How do you manage your personal data
6. Responsibility statement to the third party



7. How do we process children's personal data
8. How your personal data is transferred globally
9. How to update this Privacy Policy
10. How to contact us
11. Dispute resolution

1. How do we collect and use your personal data

The personal data involved in this privacy policy includes basic information (including personal name, nickname, personal phone number, email address), real-name personal identification certificate (including ID card, etc.); network identification information (including system account, IP address, Email addresses and passwords related to the aforementioned); personal property information (order fee payment, recharge/points and other virtual property information, etc.); personal Internet access records (including website browsing records, software usage records, click records, operation logs, etc.); equipment information (including device model, device MAC address, operating system type, device settings, etc.); unique device identification code (such as IMEI/android ID/IDFA/OPENUDID/GUID, SIM card IMSI information, etc. describing the basic situation of personal frequently used equipment); location information (including contact address, etc.).

YouCloud collects and uses personal data for the following purposes described in this Privacy Policy, including:

1.1 Registration, login, and related services

When you register, log in and receive related services, you can create an account with your mobile phone number or email address, and we will verify your identity by sending a text message or email verification code, and you can complete the relevant **network identification information (mobile phone number , email address, user name, password)**. You understand and agree that, if necessary, we can identify you based on your registration information to prevent others from falsely using your identity to operate and affect your normal use of our products and services.

1.2 Information may need to be provided when using specific functions

1) Order information. In order to display the order information of your account, we will collect the order information generated during your use of our services to show you and facilitate your order management.



2) Information browsing and searching:

To achieve this function, we may collect necessary log information. The log information used for information display includes:

- a) Behavioral information on your operations and use, including the words or phrases you searched for, your browsing history and time, and the time and times you searched.
- b) Information provided by you voluntarily: feedback and comments. We collect this information to quickly match you with the content you need and the content you may be interested in, and also to improve our products and services.

3) Customer service

When you initiate a complaint, appeal or consultation with YouCloud, for the security of your account and system, we may require you to provide account information first, and match it with your previous personal data to verify your user identity. At the same time, for the convenience of contacting you or helping you solve problems, we may also require you to provide the following personal data: name, mobile phone number, email and other contact information, city/region information.

In addition, we will also collect your communication information with us (including text, picture, audio, video, call records), and other necessary information related to your needs. We collect this information to investigate facts and help you solve problems. If you refuse to provide the information above, we may not be able to give you timely feedback on complaints, appeals or consultation results.

4) Carry out marketing activities

When you choose to participate in the relevant marketing activities held by us, you should provide your name and contact information according to the needs of the activities. **Such information may include personal data (such as personal phone number)**, which is necessary for you to receive event feedback or gifts. If you refuse to provide such information, we may not be able to provide you with event feedback or send gifts.

5) Guarantee the safety of products, services and users

In order to help us better understand the operation of the YouCloud website and related services, so as to ensure the safety of operation and service provision, we will record network log information, as well as the frequency, crash data, usage, and performance data information of using the website and related services,.

6) Accept push messages

When you use our services, we may use your information to send emails or SMS push notifications. If you do not wish to receive these messages, you can follow our relevant prompts and choose to unsubscribe on your device, except in cases where we send messages in accordance with legal provisions or service agreements for



individual services.

7) **Exceptions to obtaining authorized consent**

You fully understand and agree that we may collect and use your personal data without requiring your authorized consent under the following circumstances, and we may not respond to your requests for correction/modification, deletion, cancellation, withdrawal of consent, or request for data:

- a. Related to national security and national defense security;
- b. Related to public safety, public health, and major public interests;
- c. Related to judicial or administrative law enforcement such as criminal investigation, prosecution, trial, and execution of judgments;
- d. For the purpose of safeguarding your or other individuals' significant legitimate rights and interests such as life and property, but it is difficult to obtain your consent;
- e. Personal data you disclose to the public on your own;
- f. Collecting personal data from legally disclosed information, such as legitimate news reports, government information disclosure, and other channels;
- g. Necessary for the agreements signed and fulfilled with you or other written documents ;
- h. Necessary for maintaining the safe and stable operation of the products and/or services provided, such as detecting and processing malfunctions of the products and/or services;
- i. Necessary for legitimate news reporting;
- j. Necessary for academic research institutions to conduct statistical or academic research based on the public interest, and de-identifies the personal data contained in the results when providing academic research or descriptive results to the public;
- k. Other situations stipulated by laws and regulations.

Please be aware that, according to applicable laws, **when we process personal data by technical and other necessary measures, which makes it impossible for the data recipient to re identify a specific individual and restore the personal data**, or when we conduct deidentification research, statistical analysis, and prediction of the collected data to improve our content and layout, and provide products or services support for business decision-making, and to improve our products and services (including using anonymous data for machine learning or model algorithm training), **the use of such processed data does not require prior notice to you and your consent**.

If we use your information for other purposes not specified in this Privacy Policy, we will seek your consent in advance.



We may issue announcements related to services to you when necessary (such as when a service is suspended due to system maintenance), which may be closely related to your rights. We suggest you read them as carefully as possible after receiving them. You may not be able to cancel these announcements related to services that are not promotional in nature.

1.3 For providing you with better services and maintain and improve the quality of our products or services, we may collect and use the following information in accordance with legal regulations and based on your specific authorization:

We may use personal data collected in our business for statistical analysis and operational improvement, such as feedback provided voluntarily by you, or automatic feedback from the system when you encounter system crashes, anomalies, etc. when using our products, and technical modifications, network maintenance, troubleshooting, internal policy and process development, and internal report generation to improve our system.

1.4 The information we obtained when you used the services:

- 1) Data of service log, including your login and logout data, clicking on advertisements, searching and viewing data while using our services, and service failure data.
- 2) Device data, including device model, device size, operating system version, and unique device identifier, to ensure network operation security.
- 3) Software data, including the version number and browser type of the software, to ensure the security of your operating environment.
- 4) The revocation of IP address takes effect after the operation and cannot take effect on operations that were already performed before the revocation. **If you stop using our products, you need to complete the cleaning of local and server data in the account on your own.** If the account is stopped without any account cancellation or server cleaning, any losses incurred will be borne by the user. We do not assume any responsibility for any problems caused by your personal behavior.

1.5 Precautions for uploading data:

The personal data uploaded while you using our products and services, may belong to you or others under legal protection, and may involve your own or others' privacy, or may be protected by copyright laws or other laws. You should ensure that you have obtained the necessary permissions to copy and upload this data, and



please make appropriate settings and take appropriate security measures to prevent the leakage of this data and the damage of the interests of the rights holders. Please pay high attention to protecting your own or others' data, and unauthorized disclosure is not allowed.

1.6 Processing of changes in the purpose of collecting and using personal data

Please understand and be aware that with the development of our business, there may be adjustments and changes to the functions and services provided by YouCloud. In principle, when a new feature or service is related to the listed scenario, the personal data collected and used will have a direct or reasonable connection with the original processing purpose. In scenarios where there is no direct or reasonable connection with the original processing purpose, we will collect and use your personal data after informing you again and obtaining your consent.

2. How do we use Cookies and similar technologies

Cookies and similar technologies are common technologies on the Internet. When you use YouCloud and related services, we may send one or more Cookies or anonymous identifiers by relevant technologies to your device to collect and store data about your access and use of our products. We mainly use Cookies and similar technologies to achieve the following functions or services:

1) Ensure the safe and efficient operation of products and services

We may set up Cookies or anonymous identifiers to authenticate and ensure security, allowing us to confirm that you are securely logged into the services or have encountered illegal activities such as theft and fraud. These technologies will also help us improve service efficiency, and increase login and response speed.

2) Helping you get a easier access experience

Using such technologies can help you avoid repeating the steps and processes of filling out personal data and entering search content. For example, Cookies help us identify you as our registered user, or save data you provide us about your preferences or other information (such as recording search history).

3) Analyze your use of our services

We may use Cookies to understand what activities you are using YouCloud for, or which services are most popular.

4) Advertising optimization

Cookies help us provide you with advertisements related to you based on your data, rather than conducting general advertising campaigns.



While using Cookies for the above purposes, we may also provide a summary of non personally identifiable data collected through Cookies to advertisers and other partners for analyzing how you and other users use YouCloud for advertising purposes.

There may be Cookies placed by advertisers and other partners on YouCloud. These Cookies may collect non personally identifiable data related to you for analyzing how users use these services, sending you advertisements that you may be interested in, or evaluating the effectiveness of advertising services. **The collection and use of such data by these Cookies of third-party is not subject to this Privacy Policy, but rather to their own personal data protection statement, and we are not responsible for the Cookies of third-party.**

You can reject or manage Cookies through a browser or user selection mechanism. Please note that if you stop using the Cookies, we may not be able to provide you with the best service experience, and some services may also be unavailable. Meanwhile, you will still receive advertisements, but their relevance to you will decrease.

We promise that we will not use Cookies for any purpose other than those stated in this Privacy Policy.

3. How do we share, transfer and publicly disclose your personal data

3.1 Share

Except for the following situations, we will not share your data with any third party without your consent:

- 1) To provide you with our critical services. We may share your data with partners and other third parties to achieve the core functions you need or provide the services you need;
- 2) To achieve the purpose stated in Article 1 "How do we collect and use personal data" of Part II in this Privacy Policy;
- 3) To fulfill our obligations and exercise our rights in this Privacy Policy or other agreements we have reached with you;
- 4) In order to abide by the law, protect us and our affiliates or partners, you or other YouCloud users, or the public interests, property or safety from damage, such as to prevent fraud and other illegal activities and reduce credit risk, we may exchange data with other companies and organizations within the scope allowed by laws and regulations. However, this does not include selling, renting, sharing, or otherwise disclosing data for profit in violation of the commitments made in this Privacy Policy.
- 5) In response to your legal needs, assist in handling disputes or controversies between you and others;
- 6) Provide your data at the lawful request of your guardian;



7) According to the individual service agreement signed with you (including the electronic agreement signed online and the corresponding platform rules) or other legal documents;

8) Provided based on social public interests that comply with laws and regulations.

We will only share your data for legal, legitimate, necessary, specific and clear purposes. We will sign strict confidentiality agreements with companies, organizations and individuals with whom we share data, requiring them to process data in accordance with our instructions, this Privacy Policy and any other relevant confidentiality and security measures. If the affiliated company change of use of personal data, it will ask for your consent again. During your use of related services, the related company will also assume the same responsibility as us to protect your data. If the above-mentioned fail to protect your data, we will hold them responsible for breach of contract in accordance with the contract and provisions of law. You agree to authorize us to pursue the legal responsibility for violating your "right to the protection of personal data" in our own name in the event of infringement of personal data.

If you find the data of YouCloud user have been stolen, sold, or stored without authorization by any third party, please report it to us and provide us as much detail as possible so we can investigate.

In order to protect your data to the greatest extent, we recommend that you read the privacy policy before using the SDK services of any third-party. In order to protect your legitimate rights and interests, if you find these SDKs or other similar applications are at risk, you are advised to immediately terminate the relevant operations and contact us in time.

3.2 Transfer

1) With the development of our business, we may conduct mergers, acquisitions, asset transfers or similar transactions, and your data may be transferred as part of such transactions. We will require the companies and organizations will hold your data to be bound by this Privacy Policy. Otherwise, we will require them to seek your authorization and consent again.

2) After obtaining your explicit consent, we will transfer your data to other parties.

3.3 Disclosure

We will only disclose your data under the following circumstances, and only if we take safety measures that comply with industry standards:

- 1) According to your needs, disclose the data you specify in the disclosure method you expressly agree to;
- 2) In cases where it is necessary to provide your data according to laws, regulations, mandatory administrative enforcement or judicial requirements, we may disclose your data based on the type of data and disclosure method required. When we receive the above request for disclosure under the premise of complying

with laws and regulations, we will require the recipient to issue corresponding legal documents, such as subpoenas or investigation letters. We firmly believe the data asked to provide should be as transparent as the law allows. We carefully review all requests to ensure that they have a legitimate basis and are limited to data that law enforcement has a legal right to obtain for specific investigative purposes.

4. How do we protect your personal data

4.1 Storage of personal data

- 1) Storage period. Unless in accordance with laws and regulations or an agreement between you and us, we will only retain your personal data for the shortest time necessary to achieve the purpose (for example, the Electronic Commerce Law of the People's Republic of China stipulates that the storage time of the data of products, services and transaction shall be not less than three years from the date of completion of the transaction). We will delete your personal data or de-identify the data as soon as possible in accordance with the requirements of laws and regulations beyond the above storage period or when you voluntarily cancel your account.
- 2) Storage area. In accordance with laws and regulations, we will only store the collected personal data of you within the territory of the People's Republic of China. We do not currently have any situation where your personal data is stored across borders or provided overseas. If it is necessary to transfer data across borders, we will separately notify you (including the purpose of data export, receiver, method and scope of use, content of use, security measures, security risks, etc.), and obtain your authorization. We will ensure that the data recipient has sufficient data protection capabilities to protect your personal data.
- 3) Termination of operation. In case of termination of operation, we will notify you in advance, and delete or anonymize your personal data.

4.1 Security of personal data

- 1) We have a standardized privacy policy to clarify the scope and purpose of personal data collection to you.
- 2) We have established a complete data security corresponding mechanism. When personal data is leaked, damaged or lost and it is listed as a security incident in accordance with our internal system and relevant national standards, we will start the early warning plan in time to protect your personal data.
- 3) We will cultivate employees' awareness of data security and provide training and assessment on their security capabilities, to enhance their awareness of the importance of protecting personal data.
- 4) We only allow our employees and partners who need to know this data to access your data, and have set up strict access control and monitoring mechanisms for this purpose. We also require all persons who may



have access to your data to fulfill corresponding confidentiality obligations. If they fail to fulfill the obligations, they may be prosecuted for legal responsibility or be suspended from the cooperative relationship with YouCloud.

- 5) We will take all reasonable and feasible measures to ensure that no irrelevant data is collected.
- 6) We have adopted reasonable and feasible security protection measures in line with industry standards to protect your data and prevent personal data from being accessed, publicly disclosed, used, modified, damaged or lost without authorization. For example, when exchanging data between your webpage and the server, it is protected by SSL protocol encryption; we also provide HTTPS protocol secure browsing mode for YouCloud website; we will use encryption technology to improve the security of personal data; the trusted protection mechanism prevents malicious attacks on personal data; we will deploy access control mechanisms to ensure that only authorized personnel can access personal data.

Although the reasonable and effective measures above-mentioned have been taken, and the standards required by relevant laws have been complied with, if your personal data and privacy are leaked due to the following events, we will do our best to remedy or provide you with assistance, however, you agree that we shall not be liable for:

- a) Data leakage caused by viruses, Trojan horse, and hacker attacks;
- b) Leakage of any personal data caused by you notifying others of your user password, causing others to have access to your user password, or sharing your registered account with others;
- c) Any other leakage of personal data not caused by YouCloud.

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. Otherwise, any losses arising therefrom shall be borne by you.

5. How do you manage your personal data

You can access and manage your personal data through the following methods:

5.1 Access to your personal data

- 1) You have the right to access your personal data, except for exceptions stipulated by laws and regulations.

You can access your personal data yourself by:

Account Information - If you wish to access or edit the basic profile information in your account, you can perform such operations by logging into your account.

- 2) If you cannot access your personal data through the above paths, you can contact us at any time through the online customer service provided by YouCloud. We will respond to your request within 15 days.
- 3) For other personal data generated during your use of our products or services, we will provide you with relevant arrangements in accordance with "5.7 Respond to your above request".

5.2 Correct or supplement your personal data

When you find your personal data we process is wrong, you have the right to ask us to make corrections or additions. You can submit a correction or supplementary application through the methods listed in "5.1 Access to your personal data".

5.3 Delete your personal data

- 1) You can delete some of your personal data through the methods listed in "5.1 Access to your personal data".
- 2) In the following situations, you can request us to delete your personal data:
 - a) If our processing of personal data violates laws and regulations;
 - b) If we collect and use your personal data without your explicit consent;
 - c) If our processing of personal data seriously violates the agreement with you;
 - d) If you no longer use our products or services, or you voluntarily cancel your account;
 - e) If we permanently no longer provide you with products or services.
- 3) After you delete data from our service, we may not immediately delete the corresponding data from the backup system, but we will delete them when the backup is updated.

5.4 Change the scope of your authorization and consent

Every business function requires some basic personal data to be completed. In addition, you can revoke part of the authorization by unbinding, modifying personal settings, deleting relevant data, etc., or by turning off the function.

When you withdraw your consent, we will no longer process the corresponding personal data. **However, your decision to withdraw your consent will not affect the previous processing of personal data based on your authorization.**

5.5 Cancellation of account by the subject of personal data

You can apply for cancellation of your account through the online application, customer service or other methods announced by us. After you cancel your account, you will no longer be able to log in and use our products and services with this account, and the rights and interests have been generated but not consumed during the use of the products and services of YouCloud under this account will no longer be available. All the



content, information, data, records, etc. under the account will be deleted or anonymized (except provided by laws and regulations or required by regulatory authorities, such as in accordance with the Cybersecurity Law of the People's Republic of China, your network operation logs will be kept for at least six months). Once the cancellation of YouCloud account is completed, it will not be restored.

If you still decide to cancel your YouCloud account after careful consideration, you can submit a cancellation application to us through the relevant function setting page of our products and/or services, or follow the operation guidelines on the YouCloud website. The logout path is: "My—Settings—Privacy Permission Settings—Account Logout".

We will reply to you as soon as possible within 15 working days after receiving your cancellation application and verifying your user identity. If you have any questions about processing your personal data, you can communicate with us through the contact information disclosed in Article 10 "Contact Us" of this Privacy Policy.

5.6 Automatic decision-making of constraint data system

In some business functions, we may only make decisions based on non-manual automatic decision-making mechanisms including data systems and algorithms. If these decisions significantly affect your legitimate rights and interests, you have the right to ask us for an explanation, and we will also provide appeal methods on the premise of not infringing on the trade secrets of this product or other user rights and social public interests.

5.7 Respond to your above request

- 1) To ensure safety, you may need to provide a written request or prove your identity in other ways. We may ask you to verify your identity before processing your request.
- 2) We will reply within 15 days. If you are not satisfied, you can also file a complaint through the contact information of customer service specified in Article 10 of this Privacy Policy.
- 3) **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 situation. We may deny requests that are unnecessarily repetitive, require excessive technical means (for example, requiring the development of new systems or fundamental changes to existing practices), pose a risk to the legitimate rights and interests of others, or are highly impractical.**
- 4) In the following circumstances, we will not be able to respond to your request in accordance with the requirements of laws and regulations:
 - a) Related to national security and national defense security;

- b) Related to public security, public health, or major public interests;
- c) Related to criminal investigation, prosecution, trial and execution of judgments;
- d) There is sufficient evidence that the subject of personal data has subjective malice or abuse of rights;
- e) Responding to your request will cause serious damage to the legitimate rights and interests of you or other individuals or organizations;
- f) Those involving commercial secrets.

6. Responsibility statement to the third party

When you visit a third-party service or program accessed by YouCloud, the third party **will collect, use, and store your relevant data or information** in accordance with its privacy policy or related agreements, and may also place their own Cookies or Web Beacons not controlled by us, and use of them is not governed by this Privacy Policy. We will strive to require third parties to take protective measures for your personal data. We recommend that you fully understand their terms of service and privacy policies before accepting or using third-party products or services. If you find the providers of products or services have violated laws and regulations, it is recommended that you terminate the relevant operations. At the same time, you can give feedback to YouCloud, and we will deal with it after verification.

7. How do we process children's personal data

- 1) **If you are a minor under the age of 18, you should obtain the consent of your guardian before using our products and/or services, and we hope you and your guardian will read this Privacy Policy together.**
- 2) **For the collection of personal data of minors with the consent of the guardian, we will only use, share, transfer or disclose the data when permitted by law, consented by the guardian or necessary to protect the minor. If your guardian does not agree with you to use our services or provide data to us in accordance with this Privacy Policy, please stop using our services immediately and notify us in time so that we can adopt corresponding policies.**
- 3) If it is proven that minors have registered to use our products and/or services without the consent of their guardians, we will negotiate with the relevant guardians and try to delete the relevant personal data as soon as possible.
- 4) Since our products do not actively collect age and other identity data, we cannot know whether there are minors, especially minors under the age of 14, using our products. However, regarding the personal data we may collect from children, we will strictly abide by the Regulations on the Protection of Children's Personal

Information Network.

5) When we know that the user is a minor, we will not collect and use the personal data of the minor beyond the scope of this Privacy Policy, nor will we disclose the identifiable personal data of the minor to any third party, except to provide necessary and urgent help to minors, or other circumstances described in this Privacy Policy. If guardians or stakeholders of minors find that there are problems about minor data in our products, please contact our customer service in time to make a complaint. After verification, we will delete, cancel the account or take other measures as required as soon as possible. If the development of relevant legislation puts forward new requirements for the privacy protection of minors, we will take further measures as soon as possible to ensure strict compliance.

8. How your personal data is transferred globally

The personal data we collect and generate in the People's Republic of China will be stored in China, except for the following circumstances:

- 1) There are clear provisions in laws and regulations;
- 2) Obtain your explicit authorization.

In view of the above situations, we will ensure that your personal data are adequately protected in accordance with this Privacy Policy. If there is an exit situation, we will conduct exit security assessments in accordance with relevant national regulations.

9. How to update this Privacy Policy

In order to provide you with better services, our business will change from time to time, and **this Privacy Policy will also be adjusted accordingly**. We will not reduce your rights under this Privacy Policy without your express consent. **We will remind you of the update of relevant content by issuing an updated version on our website, mobile terminal, or in other ways, and please visit YouCloud to understand of the latest privacy policy. Under the foregoing circumstances, if you continue to use our services, you agree to accept and be bound by the revised Privacy Policy.**

10. How to contact us

You can contact us in the following ways, and we will respond to your request within 15 days:

- 1) If you have any questions, comments or suggestions about this Privacy Policy, you can contact us by dialing our customer service number 020-35672278 or online customer service. Our office address is Qinglan,



Xiaoguwei Street, Panyu District, Guangzhou City, Guangdong Province 26th Street.

- Recipient: Guangzhou Mihui Information Technology Co., Ltd.
- Address: Floor 17, No. 26, Qinglan Street, Xiaoguwei Street, Panyu District, Guangzhou
- Zip code: 511400
- E-mail: youcloud@youmi.net

2) If you are dissatisfied with our response, especially if you believe that our processing behavior of personal data has damaged your legal rights, you can also seek a solution by filing a lawsuit with the court with jurisdiction where the defendant is domiciled.

11. Dispute resolution

- 1) The interpretation and dispute resolution of this Privacy Policy shall be governed by the laws of the mainland of the People's Republic of China. Any dispute arising from this Privacy Policy and our processing of your personal data, you agree to submit to the Guangzhou Arbitration Commission for arbitration. Once the arbitration is final, it is legally binding on both parties.
- 2) If you consider that our processing of personal data has damaged your legitimate rights and interests, you can also choose to report to the relevant government department.