

Privacy Protection Agreement

Last updated: October 9, 2023

Effective date: April 16, 2021

****Special Note:** The “Timekettle Privacy Policy” (hereinafter referred to as this “Policy”) is only applicable to the products and services provided by****Shenzhen Timekettle Technologies Co., Ltd. (hereinafter referred to as “Timekettle” or “We”) to you. Please read this Policy carefully before using this software, in order to make sure you have fully understood and accept all the terms hereof. Otherwise, please do not register, log in, or use it. Please pay special attention to the important contents related to the sensitive personal information and to your rights and interests of personal data, which have been indicated in bold. If you are a minor under the age of 18, please read and fully understand this Policy accompanied by your guardian, and use Timekettle products and services after obtaining the consent of your guardian.****We are committed to protecting the privacy of children under the age of fourteen ("Children") in our company. Please refer to the "Children's Privacy Protection Agreement" at the end of this**

agreement for more details.

This Policy will help you understand the following:

- I. Definition and interpretation
- II. How do we collect and use your Personal Data
- III. How do we use cookies
- IV. How do we share, transfer and publicly disclose your Personal Data
- V. How do we protect and store your Personal Data
- VI. How do you manage your Personal Data
- VII. Protection of minors' personal information
- VIII. Notice and revision
- IX. How to contact us
- X. "Children's Privacy Protection Agreement"

I. Definition and interpretation

- 1. Timekettle Products & Services: include Timekettle APP (hereinafter referred to as the “Software”).
- 2. Translation Service: refers to such service as translation provided to users by Timekettle’s operator, Shenzhen Timekettle Technologies Co., Ltd., hereinafter referred to as the “Service”.
- 3. Shenzhen Timekettle Technologies Co., Ltd.: Timekettle’s operator, a high-tech company engaged in artificial intelligence, hardware and software services, and solving cross-language communication barriers.

Registered address: Room 602, Building 1, Pingshan Civilian

Enterprise Science and Technology Park, No. 65, Lishan Road, Pingshan Community, Taoyuan Sub-district, Nanshan District, Shenzhen. Phone: +86-755-86725036. For more information about our company and platform, you can contact us through the contact information provided in Article 9 hereof.

4. User(s): refer to users who register, log in, and use the Software, as well as enable, browse, or upload data to Timekettle and is more frequently referred to herein as “you”.
5. Account: refers to the user account that you are entitled to after you complete the registration of real information and you are responsible for keeping; you shall be responsible for all actions under your account.
6. Personal Data: Personal Data refers to various information recorded electronically or by other means that can identify the personal identity of a natural person individually or in combination with other information, including but not limited to the name, date of birth, identity document number, personal biometric information, address, and telephone number of a natural person. For the avoidance of doubt, Personal Data includes but is not limited to sensitive personal information.
7. Sensitive Personal Information: Sensitive personal information refers to the Personal Data that may harm personal and property safety and

easily lead to damage to personal reputation, physical and mental health or discriminatory treatment once disclosed or illegally provided or abused. Sensitive personal information includes, but is not limited to, identity document numbers, personal biometric information, bank account, communication content, and health physiological information.

8. Personal Data Subject(s): Personal Data Subject refers to the natural person identified by Personal Data.
9. De-identification/de-identify: De-identification/de-identify refers to the technical processing of Personal Data to make it impossible to identify the Personal Data Subject without the aid of additional information.
10. Anonymization/anonymize: Anonymization/anonymize refers to the technical processing of Personal Data through which the Personal Data Subject cannot be identified and the processed information cannot be recovered.
11. Device: Device refers to a device that can be used to access Timekettle, such as a desktop computer, laptop, tablet, or smart phone.
12. Unique Device Identifier(s): Unique device identifier (proprietary ID or UUID) refers to a string of characters encoded into a device by the device manufacturer that can be used to uniquely identify the device.

Unique device identifiers have a number of uses, including the ability to deliver ads when cookies are not available. We identify devices or applications with device startup time, system version, device model, physical memory, hard disk capacity, system update time, carrier, time zone, country, language, IP address, OAID, advertising identifier (for example, IDFA), and other information.

13. IP Address: Each device connected to the Internet will be assigned a number, called an Internet Protocol (IP) address. These numbers are usually assigned by geographical area. IP addresses are often used to identify the location of a device when it is connected to the Internet.
14. SSL: SSL, also known as Secure Socket Layer, is a security protocol implemented over the Transport Communication Protocol (TCP/IP). SSL supports various types of networks and provides three basic security services, all of which achieve the effect of information confidentiality by public key and symmetric key technology.
15. Information Collection Technology: The “automatic collection” referred to herein includes the following methods:
 - (1) Cookie: Cookie is a small text file placed by the website server in the client (your computer, mobile phone or other smart terminal) when you browse the web page, which can be used to improve your use experience.
 - (2) Log Files: Log files store several pieces of data that are automatically

collected. Such data includes Internet Protocol (IP) addresses, browser types, Internet service provider (ISP), reference exit pages, operating systems, date and time stamps, and click-stream data.

(3) ET Tag (Entity Tag): ET tag is an HTTP protocol header that passes behind an Internet browser and an Internet server, which can replace cookies and can be used to track individual users, allowing us to better understand and improve our services.

16. The laws, regulations and administrative rules applicable to this Policy are those of the mainland of the People's Republic of China.

II. How do we collect and use your Personal Data

You understand and agree that:

- 1. We will use the collected Personal Data in accordance with the provisions of this Privacy Policy and for the purpose of realizing the functions of our products and/or services.**
- 2. After collecting your Personal Data, we will de-identify the data through technical means, and the de-identified information will not be able to identify the subject. Please understand and agree that in this case, we have the right to use the information that has been de-identified, and we have the right to analyze the User database and make commercial use of it without disclosing your Personal Data.**
- 3. Please note that all Personal Data provided by you during the use of our products and/or services will continue to be authorized to us**

for use during your use of our products and/or services, unless you delete it or reject our collection through system settings. When you cancel your Account, we will stop using and delete your Personal Data.

4. We may compile statistics on the use of our products and/or services and may share such statistics with the public or third parties to demonstrate the overall use trends of our products and/or services, but such statistics do not contain any identification information about you.

5. When we display your Personal Data, we will desensitize your information by means of content replacement and anonymous processing to protect your information security.

6. If we want to use your Personal Data for other purposes not specified herein, or if the information collected for a specific purpose is to be used for other purposes, we will seek your consent in advance by requesting you to check the box on your own initiative.

Your Personal Data that we may need to collect and use when you use our products and/or services includes the following two types:

1. The necessary information that you must authorize us to collect and use so that we can provide the basic functions of our products and/or services to you. If you refuse to provide the relevant information, you will not be able to use our products and/or services.

2. The information that you may choose to authorize us to collect and use so that we can provide the additional functions of our products and/or services to you. If you refuse to provide it, you will not be able to use the relevant additional functions or achieve the functional effect we intend to achieve, but it will not affect your normal use of the basic functions of our products and/or services.

Timekettle will only **collect and use your Personal Data** for the following purposes as stated in this Policy:

(I) Registration of Timekettle Account

When you use Timekettle for Account registration, **we will collect your personal email address and Account password set by you to create your Timekettle Account.** After successful registration, your personal email will be your Timekettle Account, and you can log in to the Timekettle APP by entering your Account and password.

If you log in to the Timekettle APP using the associated account of WeChat, Google or Facebook, we will collect your avatar, nickname and email account. In this case, your WeChat, Google or Facebook account will be your Timekettle Account, and you can log in to Timekettle with the associated account. The achievement of associated login depends on the correct login status of your associated account. If your Account is not logged in or logged in with other account, you can only log in using the bound personal email.

For services that require logging in to the Timekettle APP account, we may verify your identity based on the foregoing information you provide to ensure that we are providing services for you.

(II) Translation function

When you are using Timekettle translation function, including but not limited to simultaneous interpretation mode, touch mode, and loudspeaker mode. In order to better provide headset connection, recording, translation, text-to-speech, speech-to-text and other related services, we will collect necessary User information according to the specific function of the service you are using:

- 1. Location information. For intelligent allocation of optimal servers.**
- 2. System default language. Used to match the APP default language and translation default language for you.**
- 3. Information about other Bluetooth devices that are being connected. Used to determine if the headset function can be performed normally.**
- 4. Custom translation information. Used to save the professional terms, place names, fixed collocations, idioms and other information set by the User, so that it can be synchronized through the User Account after the phone is changed.**
- 5. Custom setting information. Used to save the headset parameter information that has been set by the User in the specific function, so**

that it can be synchronized through the User account after changing the phone.

(III) Display and purchase of goods

1. Ordering and paying for virtual goods

For paid virtual goods in Timekettle, including but not limited to offline packages, you need to place the order and pay the corresponding amount of currency to use it. In order to realize the ordering function of paid virtual goods, **we need to get your Timekettle Account**. After the order is placed, you can choose to use the balance of Timekettle account or the payment service provided by the third-party payment agency cooperating with Timekettle (Google In-App Purchase and other non-balance payment methods, hereinafter referred to as "Google In-App Purchase"). The payment function will collect your Timekettle Account. **However, we need to share your Timekettle order number and transaction amount with these payment agencies to enable them to confirm your payment order and complete the payment.**

Order management function

In order to facilitate you to inquire about and manage the order information, **we will collect the order information generated during your use of our services for displaying to you and facilitating you to manage your orders.**

(IV) Customer service function

When you contact us or apply for resolving sales, after-sales disputes, in order to guarantee the security of your Account, **we need you to provide necessary Personal Data to verify your User identity. When using the customer service system, the User also needs to grant the camera permission if the camera feedback is needed.**

For the convenience of contacting you, helping you solve problems as soon as possible or recording the solutions and results of relevant problems, **we may save the records of your communication and call with us and other relevant contents (including the Account information, order information, and other information provided by you to prove relevant facts, or the contact information left by you). If you have any inquiry, complaint or suggestion regarding specific order, we will use your Account information and order information.**

We may also use other information about you, **including the information you provide when you contact customer service**, as reasonably necessary to provide the services and improve the quality of the services.

(v) Statistical Features

In order to provide better products and/or services and improve user experience, we collect device attribute information (e.g. your hardware model, operating system version, device configuration, unique device identifier, International Mobile Equipment Identity Code IMEI, network

device hardware address MAC, advertising identifier IDFA, etc.), device connection information (type of browser, telecommunication carrier, language used) and device status information (e.g. device sensor data, list of device application installations). For information collected from your various devices, we may correlate them so that we can provide you with consistent service across these devices.

(VI) Ensuring transaction security

In order to improve the security of your use of the services provided by us and our affiliates and partners, protect the personal and property safety of yours or other users or the public from infringement, and better prevent security risks such as phishing sites, fraud, network vulnerabilities, computer viruses, network attacks, and network intrusions, and more accurately identify the violations of laws and regulations or Timekettle's relevant protocols, **we may use or integrate your Account information, transaction information, device information, software usage records, click records and the information shared by our affiliates and partners with your authorization or in accordance with the laws** to comprehensively judge the risk of your Account and the transaction, carry out identity verification, detect and prevent security incidents, and take necessary recording, auditing, analysis and disposal measures according to the laws.

The aforesaid services may require you to enable the access

permissions of your unique device identifier, geo-location (location information), location (access rough location), microphone and phone storage in your device to us, so as to realize the collection and use of the information involved in these functions. You can enable or disable these permissions at any time in your phone or device settings.

Please note that, by enabling such permissions, you authorize us to collect and use such Personal Data to achieve the above functions, and by disabling such permissions, you cancel such authorization, and we will no longer continue to collect and use your Personal Data, and be unable to provide you with the above functions corresponding to such authorization. Your decision to disable such permissions will not affect the preceding processing of Personal Data performed under your authorization.

Please note that, according to relevant national laws and regulations, Timekettle does not need your authorization or consent to collect and use your Personal Data under the following circumstances:

1. Directly related to national security and national defense security;
2. Directly related to public security, public health and major public interests;
3. Directly related to criminal investigation, prosecution, trial and execution of judgement;
4. For the purpose of safeguarding the life, property and other important

legitimate rights and interests of yours or other person, but it is difficult to get your consent;

5. The Personal Data involved are disclosed to the public by you;
6. Collection of Personal Data from lawfully publicly disclosed information, such as lawful news reports, government information disclosure and other channels;
7. Necessary to maintain the safe and stable operation of the products or services provided, such as finding and dealing with faults of the products or services;
8. Related to the performance of Timekettle's obligations under the laws and regulations.

You should know that if, according to the applicable laws, we take technical measures and other necessary measures to process Personal Data, making the data receiving party unable to re-identify specific person and it cannot be recovered, or we de-identify the collected information for research, statistical analysis and forecast, so as to improve the content and layout of Timekettle, provide product or service supports for business decision-making, and improve our products and services (including the use of anonymous data for machine learning or model algorithm training), we should not be required to notify you and obtain your consent separately to use such processed data.

III. How do we use cookies

We do not use cookies for any purpose other than those described herein. You can also manage or delete cookies according to your preference, or clear all the cookies saved in the software.

IV. How do we share, transfer and publicly disclose your Personal Data

(I) Share

1. We will not share your Personal Data with any company, organization and individual other than Timekettle and its partners, except:

(1) We have obtained your explicit consent or authorization in advance;

(2) We provide it according to the applicable laws and regulations, legal proceedings, mandatory administrative or judicial requirements;

(3) It is necessary to provide it to protect the interests, property or security of “Timekettle” or partners of “Timekettle”, you or other Timekettle users or the public from being damaged to the extent permitted by the laws and regulations;

(4) Only by sharing your information, can we realize the core functions of our products and/or services, or provide the services you need;

(5) We resolve your dispute or controversy with others under your

request;

(6) It is provided in line with relevant agreements you signed (including electronic agreements signed online and corresponding rules) or other legal documents;

(7) It is used based on academic research;

(8) It is used based on public interests in accordance with the laws and regulations.

2. We may share your Personal Data with our affiliates, but we will only share the necessary Personal Data and will be constrained by the purposes stated herein. If our affiliate intends to change the purpose of processing your Personal Data, we will seek your authorization and consent again.

3. We may share your order information, Account information, device information and location information with third parties such as partners to ensure the smooth completion of the services provided to you. However, we will only share your Personal Data for lawful, just, necessary, specific, and clear purposes, and will only share the Personal Data necessary to provide services. Our partners will have no right to use the shared Personal Data for any other purpose.

Our partners include the following type:

Suppliers of goods or technical services. We may share your Personal Data with third parties that support our functions. These supports include

providing us with infrastructure related technical services, translation recognition services, payment services, data processing, and so on. We share such information for realizing the core shopping function of our products and/or services. For example, we need to share your order number and order amount with the third-party payment agency so that it can confirm your payment instruction and complete payment. We will carry out strict security monitoring over the partners' acquisition of the Software Development Kit (SDK) and Application Interface (API) of the information to protect the data security.

At present, the third-party SDKs accessed are as follows:

WeChat SDK

Application scenario: used to realize authorized login via WeChat and WeChat sharing functions.

Type of collected personal information: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

Apple SDK

Application scenario: used to realize authorized login via Apple ID function.

Type of collected personal information: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

Facebook SDK

Application scenario: used to realize authorized login via Facebook

function.

Type of collected personal information: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

Google SDK

Application scenario: used to realize authorized login via Google function.

Type of collected personal information: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

Baidu SDK

Application scenario: used to track the status of application usage, and subsequently used to further optimize products or provide operational data support.

Type of collected personal information: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

iFLYTEK SDK

Application scenario: used for offline package download statistics

Type of collected Personal Data: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

ReadSpeaker SDK

Application scenario: online voice play

Type of collected Personal Data: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

Baidu Statistics SDK

Application scenarios: To provide better products and/or services and improve user experience.

Types of personal information collected: unique device identifiers (network device hardware address MAC address), device application installation list.

[Third party privacy policy or official website](#)

Tencent Bugly

Application scenario: used for statistics of abnormal data and flashback logs.

Type of collected personal information: Unique Device Identifier

[Third-Party Privacy Policy or Website](#)

Tencent Real-Time Communication

Application scenario: For instant messaging functions.

Type of collected personal information: Network type, device type, system version.

[Third-Party Privacy Policy or Website](#)

Sensors Date SDK

Application scenario: used to track the status of application usage, and subsequently used to further optimize products or provide operational data support.

Type of collected personal information: Device information, Android ID,

Log information, Location information, Unique application number

[Third-Party Privacy Policy or Website](#)

Tencent SDK

Application scenario: Provide a built-in browser to facilitate users to view instructions, official website, etc.

Type of collected personal information: Device Information, Application Information, Wi-Fi Status and Parameters, Location Information, Wi-Fi Nearby, CellID.

[Third-Party Privacy Policy or Website](#)

AndroidUtilCode SDK

Application scenario: Get device information to better locate and solve problems encountered by users.

Type of collected personal information: Device information, AndroidID

[Third-Party Privacy Policy or Website](#)

4. Exchanging information with other enterprises or organizations in order to abide by laws, implement or apply our usage conditions and other agreements, or to protect the rights, property or security of Timekettle, you or other Timekettle users, such as to prevent illegal activities such as fraud and to reduce credit risk. However, this does not include Personal Data that is sold, let, shared or otherwise disclosed for profit in violation of the commitments made in this Privacy Policy.

(II) Transfer

We will not transfer your Personal Data to any company, organization and individual, except:

- 1. We have obtained your explicit consent or authorization in advance;**
- 2. We provide it according to the applicable laws and regulations, legal proceedings, mandatory administrative or judicial requirements;**
- 3. It is provided in line with relevant agreements you signed (including electronic agreements signed online and corresponding platform rules) or other legal documents;**
- 4. In merging, acquisition, asset transfer or similar transactions involving Personal Data transfer, we will ask the new company or organization holding your Personal Data to continue to be bound by this Privacy Policy; otherwise, we will ask the company or organization to re-seek your authorization and consent.**

(III) Public disclosure

We will only publicly disclose your Personal Data under the following circumstances:

Upon your request, disclose the Personal Data you specify under the disclosure method you clearly agreed.

When it is necessary to provide your Personal Data according to the requirements of the laws and regulations, mandatory administrative law enforcement or judicial requirements, we may publicly disclose your Personal Data based on the required Personal Data type and disclosure method. Under the premise of compliance, when we receive the request of information disclosure, we will require the issuance of corresponding legal documents, such as summon or investigative letter. We firmly believe that the information that we are required to provide shall be as transparent as possible to the extent permitted by law. We have cautiously reviewed all requests to ensure that they have legal bases, which are limited to the data obtained by the law enforcement authorities for specific investigation purpose and with legal rights. To the extent permitted by the laws and regulations, the documents we disclose are all protected by encryption keys.

(IV) Exceptions

Under the following circumstances, we do not need your authorization or consent to share, transfer, publicly disclose your Personal Data:

- 1. Related to national security and national defense security;**
- 2. Related to public security, public health or major public interests;**

- 3. Related to judicial or administrative enforcement such as criminal investigation, prosecution, trial and execution of judgement;**
- 4. For the purpose of safeguarding the life, property and other important legitimate rights and interests of yours or other person, but it is difficult to get your or other person's consent;**
- 5. Personal Data that you have made public;**
- 6. Collection of Personal Data from lawfully publicly disclosed information, such as lawful news reports, government information disclosure and other channels.**

You should know that if, according to the applicable laws, we take technical measures and other necessary measures to process Personal Data, making the data receiving party unable to re-identify specific person and it cannot be recovered, we should not be required to notify you and obtain your consent separately to share, transfer, publicly disclose such processed data.

V. How do we protect and store your Personal Data

(I) Protection of your Personal Data

We have used safety protection measures that meet industry standards to protect your Personal Data from unauthorized access, public disclosure, use, modification, damage, or loss. We will take all reasonable and feasible measures to protect your Personal Data. For example: We use HTTPS encryption to transfer your Personal Data, exchange data (such as

credit card information) between your browser and “Services” under the protection by SSL encryption, use encryption techniques to ensure data confidentiality, use trusted protection mechanisms to prevent data from being maliciously attacked, and deploy access control mechanisms to ensure that only authorized personnel can access Personal Data.

We will use a variety of safety protection measures within a reasonable level to ensure information security. For example, we use encryption techniques (e.g., TLS, SSL), anonymization processing, and other means to protect your Personal Data. In order to prevent viruses, Trojans or other malicious programs and websites, we may detect the applications installed and programs running in your device, or whether there are security risks in the information stored in the memory of the device; in order to prevent illegal acts such as fraud, hacking, and identity counterfeit, and to perform security inspection, we may analyze and use Unique Device Identifiers, login IP addresses, operational logs to facilitate the adoption of security measures or providing security prompts to Users.

We build specialized management systems, processes, and organizations to ensure information security. For example, we strictly restrict the scope of personnel accessing the information, requiring them to follow confidential obligations and conduct a review.

4. We will take all reasonable and feasible measures to avoid

collection of unrelated Personal Data. We will only keep your Personal Data within the time required for the purposes specified herein, unless it is required to extend the retention period or permitted by law.

5. In the event of an unfortunate Personal Data security incident, we will, in accordance with the requirements of the laws and regulations, promptly inform you of: the basic information and possible impact of the security incident, the disposal measures we have taken or will take, the suggestions for you to prevent and reduce risks independently, and the remedial measures for you, etc. We will inform you of the event-related information by means of email, letters, calls, pushed notifications, etc. When it is difficult to inform Personal Data Subjects one by one, we will post announcement in a reasonable and effective way. In addition, we will also report the handling of individual data security events in accordance with the requirements of the regulatory authorities.

(II) Storage of your Personal Data

- 1. If we terminate the service or operation, we will notify you in advance and delete or anonymize your Personal Data after terminating the service or operation.**
- 2. We store your Personal Data for the period specified by laws and regulations or for the shortest period required for providing you with**

Timekettle products and/or services.

VI. How can you manage your Personal Data

(I) Access your personal information

You have the right to inquire your information in the following way by yourself:

Open Timekettle and click “My” to access the Account.

Open Timekettle and click “My” to view virtual goods orders, top-up record and consumption record

(II) Correct and supplement your personal information

You are entitled to request us to make correction when you find any error in your personal information we processed. **You can contact customer service in accordance with the contact information herein for the corresponding consultation and operation.**

(III) Delete your Personal Data

In the following cases, you can request us to delete your Personal Data:

1. Our processing of Personal Data violates the laws and regulations;
2. We collect and use your Personal Data without your consent;
3. Our processing of Personal Data violates the agreement with you;
4. You no longer use our products or services, or you cancel your Account;
5. We no longer provide you with products or services.

Please know that if you publish information on Timekettle, any user who logged in to Timekettle will be able to read, collect or use your information. You can delete it in the APP by yourself. If you can not delete your Personal Data from the community forum, please contact customer service in accordance with the contact information herein. Sometimes we may not be able to delete your Personal Data. In this case we will inform you of such case and the reason.

If we decide to respond to your deletion request, we will also notify the entities which have obtained your Personal Data from us, requiring them to delete in time, unless otherwise stipulated by laws and regulations, or these entities have been independently authorized by you. When you delete any information from our service, we may not immediately delete the corresponding information from the backup system, but will delete it when the backup is updated.

(4) How to cancel your account

If you have the need to cancel your account, please contact our online customer service or send an email to [support@timekettle.co], Once we receive the email, it will be processed for you within 5 to 10 business days.

Online customer service entrance: sidebar function selection-contact us-online customer service.

VII. Protection of minors' personal information

1. We attach great importance to the protection of minors' personal information. If you are a minor under the age of 18, you should obtain the consent of your parents or statutory guardians in advance before using our products and/or services. We will protect the personal information of minors in accordance with relevant national laws and regulations.
2. For the collection of personal information of minors with the consent of parents or statutory guardians, we will only use or publicly disclose such information when permitted by law, having obtained the express consent of a parent or guardian, or where it is necessary to protect the minor.
3. If we find that we have collected personal information from minors without the prior consent of a verifiable parent or statutory guardian, we will try to delete the relevant data as soon as possible.

VIII. Notice and revision

1. **To provide you with better services and with the business development of Timekettle, this Privacy Policy will also be updated correspondingly. However, we will not reduce your rights under this Privacy Policy without your express consent. We will issue updates via Timekettle and notify you of the updates via Timekettle or otherwise as appropriate before they take effect. Please also visit**

Timekettle to keep up to date with the latest Privacy Policy.

For major changes, we will additionally provide a more prominent notification (we will explain the specific changes of the Privacy Policy by means including but not limited to email, SMS or making special notes in the browsed pages).

Major changes referred to herein include, but are not limited to:

- (1) Major changes in our service mode. For example, the purpose of processing personal information, the type of processed personal information, and the use method of personal information, etc.;
- (2) Changes in owner due to business adjustments, bankruptcy, M&A, etc.;
- (3) Changes in the main object of personal information sharing, transfer or public disclosure;
- (4) Major changes in your right to participate in the personal information processing and how it is exercised.

IX. How to contact us

If you have any questions, opinions or suggestions for this Privacy Policy or your personal information, please contact us by accessing the Online Customer Service System, sending an email to [support@timekettle.co] or call our Online Customer Service. We will reply to or deal with your questions, comments or suggestions in a timely manner.

X. "Children's Privacy Protection Agreement"

We recommend that parental consent be obtained in advance for minors under the age of fourteen ("Children") to participate in online activities. If you are a child, please notify your guardian to read this agreement together and seek their consent and guidance before using our services or providing personal information. By clicking "Agree" to this agreement online or by using/continuing to use our company's services, or submitting personal information, you represent that you have obtained permission from your guardian, and your guardian agrees to our collection, use, storage, sharing, transfer, and disclosure of your personal information in accordance with this agreement (including any updated versions).

In addition to the provisions of the "Privacy Protection Agreement," we will also comply with the following terms when collecting and processing children's personal information. In case of any inconsistency between the following terms and the "Privacy Protection Agreement," the provisions of the following terms shall prevail:

Parents or guardians of children may proactively contact us by calling the official customer service hotline or contacting customer service to exercise the rights granted to the parents or guardians of children under the following terms.

Before collecting, using, transferring, or disclosing children's personal information, we will provide prior notification to the parents or guardians

of children through the contact information provided by the parents or guardians when registering an account for the child and only collect, use, transfer, or disclose the child's information with their consent.

Upon receiving the above notification, parents or guardians may refuse. If the parents or guardians refuse our collection, use, transfer, or disclosure of the child's personal information in accordance with the "Privacy Protection Agreement," we will not collect, use, transfer, or disclose the child's information. However, this may mean that the child cannot fully utilize certain features of our products. If the parents or guardians refuse the use of essential child personal information (such as location information and device identification codes) necessary for the operation of our products, the child will be unable to use our products entirely.

Access to children's personal information by our staff shall require approval from the person responsible for the protection of children's personal information or their authorized administrators, record access details, and take technical measures to prevent unlawful copying or downloading of children's personal information.

Parents or guardians act on behalf of the child to exercise all rights afforded to the child under the "Privacy Protection Agreement."

Parents or guardians may revoke the authorization for us to collect, use, transfer, or disclose the child's personal information. However, this may mean that the child cannot fully utilize certain features of our products. If

the parents or guardians revoke authorization for essential child personal information (such as location information and device identification codes) necessary for the operation of our products, the child will be unable to use our products entirely.

If we transfer children's personal information to third parties, we will conduct security assessments ourselves or delegate them to third-party organizations.

If we cease the operation of products or services, we will promptly cease the collection of children's personal information, delete the children's personal information we hold, and notify the parents or guardians of the cessation of operations.

Effective date of this Privacy Policy: [April 16], 2021