Aubor Privacy Policy

Last updated: 2025-10-27

Effective date: 2025-10-28

Aubor Oriental (Beijing) Digital Technology Ltd. and its affiliated companies (hereinafter collectively referred to as "We" or " Aubor ") are committed to protecting your personal privacy.

" Aubor Privacy Policy" (hereinafter referred to as "this Policy") applies to all products and/or services provided by Aubor platform, including Aubor applications (mobile clients) and Aubor WeChat mini programs (collectively referred to as "Services"). When you use our services, we will collect and process your relevant information, so please read this policy carefully and make sure you understand our rules for collecting and processing your personal information (including how to collect, use, save, and share this information), and provide you with ways to access, update, delete and protect this information.

When you agree to this Privacy Policy, or start and continue to use our products or services in an appropriate manner without contacting us to express contrary opinions through appropriate means, you will be deemed to have fully understood and agreed to this Policy. During the reading process, if you have any questions, comments, suggestions or complaints, especially if you believe that our personal information processing has harmed your legitimate rights and interests, you can complain/suggest about our services through appropriate regulatory channels, or contact us through the following emails:

Customer service: info@allesin.com

Privacy Office : info@allesin.com

If you are a minor under the age of 18, in accordance with relevant laws and regulations, please obtain the consent of your parent or legal guardian before using our products or services. At the same time, if you are a child under the age of 14, please be sure to read the "Aubor Children's Privacy Protection Statement" and ensure that you and your guardian or parent clarify the relevant information about children's privacy protection.

This policy mainly explains to you:

definition

In this policy,

Affiliated companies: companies directly or indirectly controlled by Aubor; or companies that directly or indirectly control Aubor; or jointly control the same company with Aubor; or companies directly or indirectly controlled by the same company as Aubor, including but not limited to parent companies, subsidiaries; subsidiaries controlled by the same parent company as Aubor, etc.

Personal information: Various information recorded electronically or by other means that can be used alone or in combination with other information to identify an individual or reflect the activities of a specific individual.
Sensitive personal information: including personal biometric information, communication records and content, health information, transaction information, precise location information, etc. When we provide you with specific products or services that involve the collection of sensitive personal information, we will obtain your consent through a prominent and clear notice before collecting sensitive personal information about you.
Smart devices: refer to non-standard computing devices produced or manufactured by hardware manufacturers that have human-machine interfaces and can transmit information through wireless networks, including smart home appliances, smart wearable devices, smart air purification equipment, etc.
Application: refers to the mobile application developed by Aubor (including mobile client, Aubor applet, Aubor WeChat applet), which can help end users remotely control smart devices and connect to the Aubor Internet of Things (IoT) platform .

11. What personal information do we collect?
In order to provide you with our services, we will ask you to provide the personal information necessary for such services. If you do not provide personal information, we cannot provide you with corresponding products or services.

12. Information you voluntarily provide to us
Registered Account Information: When you register for an account with us, we collect your account name and contact information, including your email address, phone number, username and login credentials. During your interaction with our products, we may further collect nickname, country code, language preference or time zone information from your account.
When you choose to authorize the use of a third-party account to log in, we will obtain your shared account information (default system avatar, nickname, region information) from the third party and bind it to your Aubor account for quick login. We will use your personal information in accordance with the third party's agreement and the terms of sharing personal information in the privacy policy published by the third party, and in compliance with relevant laws and regulations.
Non-registered account information: When you are still in the understanding stage of our products, you can try it out without registration/login, that is, log out or do not create an account ("login-free" or "guest" mode), you can still use Visitor IDs to use many of our products or services, such as searching or browsing features on our apps. When you use login-free or guest mode, we will not collect your account and related information. The information collected is limited to your authorization information for additional functions, device and usage information, including the operating system of your mobile phone. The collection of the mobile device's operating system in guest mode is strictly necessary for the basic functionality of the application, such as ensuring compatibility and stable operation.When you use products and/or services that require location services, we will obtain location information based on your authorization. When you choose to exit the login-free/guest mode, we will immediately and permanently delete all information generated by your status as a guest.
However, if the service you use or purchase is based on your account information, please go to

the registration/login page to register or log in.

User feedback: When you use our services and submit service-related feedback and suggestions to us, we will collect your email address, mobile phone number and feedback content (added pictures or videos), as well as the submitted problem log, this information will be used to promptly handle your application problems and smart device-related failures.

At the same time, based on different application products and services, Aubor will collect corresponding and necessary personal information in order to provide you with products and services.

Information collected based on additional features provided

In order to provide you with more convenient and better products and/or services and strive to improve your experience, we will collect and use your personal information in the following additional services provided to you. If you do not provide this information, it will not affect your use of the basic services of the Aubor application, but you will not be able to obtain the user experience brought to you by these additional services. These additional services include:

Additional services based on location information:

When you turn on the positioning function of your mobile device through system authorization and use location-based services, we will collect and use your location information so that you can use the Aubor application to configure the network with your smart device. And when you use our specific products or services (weather services/home management), based on your consent, we will collect real-time precise or non-precise geolocation information about you, when you use the geofencing function, and when the location changes generated by creating scenes, we will apply for permission to collect background location in order to locate the user's location and complete the automated capability of user pre-screening. You can stop our collection of your location information by turning off location services in the system of your mobile device. To add the device function, you need to obtain positioning permission (Android system only). Enter Add Device. The function of searching for nearby devices requires Bluetooth scanning. Bluetooth needs to apply for positioning, otherwise it will affect the user's device addition.

Go to [My]-[Settings]-[Privacy Permission Settings]-turn off/on the [Location Information] permission

Camera/webcam based additional services:

You can use this function to scan the QR code to add the device you purchased after turning on the camera/camera permission. Please know that even if you have agreed to turn on the camera/camera permission, we will only obtain information when you actively scan the QR code and use the camera/camera to take pictures. The QR code scanning function collects light sensor information and determines whether the flash function needs to be displayed based on the light sensor data.

Go to [My] - [Settings] - [Privacy Permission Settings] - turn off/on [Camera/Camera]

Additional services based on photo album (picture library/video library) access and upload of pictures/videos:

You can use this function to upload your photos/pictures/videos after turning on the album permissions to implement the function of reporting device usage problems and providing proof. When you report a device usage problem, we will use the photos/pictures you upload to locate your problem.

Go to [My]-[Settings]-[Privacy Permission Settings]-turn off/on [Album] permissions

Additional services related to microphone-based voice technology:

After turning on the microphone permission, you can use the microphone to implement voice functions, including shooting videos and waking up the voice assistant. During these functions, we will collect your voice information to identify your command needs. Please know that even if you have agreed to turn on the microphone permission, we will only obtain voice information through the microphone when you actively click the microphone icon in the App or record a video.

Go to [My]-[Settings]-[Privacy Permission Settings]-turn off/on the [Microphone] permission

Additional services based on storage permissions (Android):

We apply for this permission from you to ensure the stable operation of the client. After you enable us to read/write your device's storage, we will read or write the necessary information for images, files, and crash log information from your device's storage space to provide you with information release the function of recording crash log information locally.

Go to [My]-[Settings]-[Privacy Permission Settings]-turn off/on the [Storage] permission

Additional features based on message notification permissions:

We apply for this permission from you in order to push you notifications about products or services. In particular, if you purchase relevant services, we need to send you alerts so that you can capture real-time status.

Go to [My]-[Message Center]-[Settings] in the upper right corner-turn off/on the [Message Push] permission

Additional functions based on "floating window" (Android system):

We apply for this permission from you. When you bind a camera in the application, it can be used to display the camera's real-time video in a floating window.

Turn off/on the [floating window] permission through the permission management settings of your mobile phone system.

Additional services based on Bluetooth technology:

You can enable Bluetooth functions after turning on Bluetooth permissions, including device control, device status acquisition, device discovery, and device network configuration. In these functions, we will communicate with the terminal device through Bluetooth. Please know that even if you have agreed to turn on Bluetooth permissions, we will only use Bluetooth for communication in these scenarios: display device status on the home page and device panel; perform device control on the home page and device panel; identify devices and configure network settings on the home page and add device page.

Go to [My]-[Settings]-[Privacy Permission Settings]-turn off/on [Bluetooth] permissions

Additional services based on HomeKit technology (iOS system only):

You can enable related functions after turning on HomeKit permissions, including device discovery, device network configuration, device control, and device status. In these functions, we will exchange data with the [Home] App that comes with the iOS system through HomeKit. Please know that even if you have agreed to enable HomeKit permissions, we will only use it in these scenarios: on the homepage and add device page for discovering HomeKit devices and HomeKit device network configuration; in [Settings] - [HomeKit Information] for Discover HomeKit devices and HomeKit device configuration networks.

Go to [Me]-[Settings]-[Privacy Permission Settings]-turn off/on [HomeKit] permissions

Additional services based on HealthKit technology (iOS system only):

You can enable related functions after turning on the HealthKit permission, including counting weight, height data, running and swimming data. In these functions, we will exchange data with the [Health] App that comes with the iOS system through HealthKit. Please know that even if you have agreed to enable HealthKit permissions, we will only use it in these scenarios: body fat scales, bracelets, and watch devices write data to HealthKit; read data from HealthKit in the health center.

Go to [My]-[Settings]-[Privacy Permission Settings]-[Health]-[Current Application]-Turn off/on [HealtKit] permissions

Additional services based on Face ID (iOS system only):

You can use the relevant functions after turning on Face ID, and use the facial recognition verification provided by the iOS system for safe and convenient account password-free login, eliminating the need to repeatedly enter the account password. The iOS system will not provide Face ID data to us, and we will not and cannot collect and store your Face ID data. You can also turn this feature on/off at any time.

Go to [Me]-[Settings]-[Account and Security]-turn off/on [Face ID]

Additional functions based on fingerprint permissions (Android only): We apply for this permission from you so that you can log in to the App without a password through fingerprint ID. We will not save and upload your fingerprint information.

Go to [Me]-[Settings]-[Account and Security]-turn off/on [Fingerprint ID]

Additional functionality based on permissions bound to the notification listener service (Android only)

We apply for this permission from you so that after the smart device connects to the App, it can monitor the App notification bar messages and synchronously send the App messages to the mobile smart device for display to you.

Go to [Device Panel] - [Settings] - [Message Push] - turn on/off permissions (off by default)

You understand and agree that the above additional services require you to turn on your location information (geographic location), camera (camera), photo album (picture library), microphone (voice), internal and external storage, "floating window", and Bluetooth in your device , Homekit, Healthkit, Face ID, listener service, and fingerprint access permissions to achieve the collection and use of the information involved in these permissions. You can check the status of the above permissions item by item in your device settings, and you can decide whether to turn these permissions on or off at your own discretion.

Please note that when you turn on any permission, you authorize us to collect and use relevant personal information to provide you with corresponding services. Once you close any permission, you cancel the authorization, and we will no longer continue to collect based on the corresponding permission and use related personal information, and cannot provide you with services corresponding to this permission. However, your decision to turn off permissions will not affect the previous collection and use of information based on your authorization.

13. Information we collect automatically

Mobile device information: When you interact with our products, in order to ensure your normal use of our services, maintain the normal operation of our services, improve and optimize our service experience, and protect your account security, we will automatically collect mobile device information , including mobile device model, login IP address, wireless connection information,

operating system type and version, application version number, push notification identifier, log files and mobile network information. At the same time, we will collect your software version number. To ensure the security of the operating environment or as needed to provide services, we collect information about the mobile applications and other software you use and the application's application installation list (for the purpose of application performance monitoring).
Usage Information: During your interactions with our Site and Services, we automatically collect usage information related to visits, clicks, downloads, sending/receiving messages and other uses of our Site and Services.
Log information: When you use our application, in order to improve your user experience, system and exception logs will be uploaded for analysis, including your IP address, usage habits, operating system version, and date or time of access, so that we can accurately identify problems and help you solve problems when using the service.
Please note that separate mobile device information and service log information are information that cannot identify a specific natural person. If we combine such non-personal information with other information to identify a specific natural person, or combine it with personal information, such non-personal information will be treated as personal information during the period of combined use, Unless we obtain your authorization or otherwise provided by laws and regulations,we will anonymize and de-identify such information.

14. Information related to smart devices
When you use a smart device, we collect information inherent in the smart device itself and information generated during your use of the smart device.
Basic information about smart devices: When you use a smart device connected to our products or services, we will collect basic information about the smart device, including the name of the smart device, device ID, online status, activation time, firmware version and upgrade information .
Information collected during the process of connecting smart devices: Based on the type of smart device you need to connect, whether it is connected through Wi-Fi, connected through Wi-Fi after establishing a local connection through Bluetooth, connected through Bluetooth or through Zig- Bee method, the Mac address and Wi-Fi information (SSID, BSSID) of smart devices will be collected.
Information reported by smart devices: Depending on the different smart devices you choose to connect to our products or services, we may collect information reported by your smart devices. In order to help you better understand the use of our services, the following smart devices are used as examples. The information reported by them is only applicable when you use this type of service:
For example: when you voluntarily use smart cameras (IPC services) and connect to the Aubor platform: you connect doorbells, door locks, and smart surveillance cameras with cameras through Aubor services to monitor the security of your residence or view relevant monitoring content, After you add the device and use the smart camera, when the device recognizes that a person or object is moving, the smart camera will capture the surveillance screen (in picture format) for you to view.The information at this time will be automatically uploaded to the cloud for you to save, but we will not use this picture for additional purposes and will automatically delete this information after the retention period. When you actively choose and successfully

purchase the cloud storage value-added service, the smart camera will upload the video you shot to the cloud for storage so that you can play it back and view it on the app. We will retain your video information according to the cloud storage service you purchased. , and will not be used for other purposes. When you choose to delete pictures in advance in the Aubor app, you can delete them in the message center. If you need to delete a video and execute this command on the app, the cloud will respond to the deletion command and immediately delete the video you choose to delete. Please note that when you choose to turn off the motion detection function, the smart camera will not actively record the captured images, which will affect your original intention of using the smart camera.

For example: when you voluntarily use a certain health-related smart device and connect to the Aubor platform, if you select one or more smart devices, the corresponding information will be recorded:

Smart body fat scale or fitness tracker: height, weight, body fat mass (BFM), body mass index (BMI) and skeletal muscle mass (SMM), body fat rate, muscle mass, body fat index, obesity level, ideal Weight, weight control, visceral fat index, net weight, body water, bone mass, protein rate, BMR, metabolic age, body score, body shape, subcutaneous fat rate, subcutaneous fat mass, heart rate;

Wristbands and similar smart devices: heart rate, steps, calories, mileage, heart rate, sleep records, training records, body temperature, blood oxygen, systolic blood pressure, diastolic blood pressure, and pressure.

Smart fitness equipment represented by smart rope skipping: start time, jumping mode, number of rope skipping, exercise duration, calories burned, maximum number of jumps to maintain, number of rope skipping, average speed, maximum speed, and heart rate during exercise.

In particular, when you actively agree and enable the sharing function connected to a third-party health platform, such as Apple Health, Google Fit, and Fitbit, we will share your health information with the third party only for measurement and analysis related to your health status. The following list shows the content of the information that is transferred when you use a smart device and decide to share the information with a third party.

wristband

body fat scale

apple health

Steps, calories, mileage, heart rate, sleep records

Height, weight, body fat percentage, BMI, weight

Fitbit

/

Weight, body fat percentage

If you choose to use Apple Health, please carefully refer to the relevant "User Agreement" and "Privacy Policy" issued by Apple Health. For details, please view: https://www.apple.com/legal/privacy/en-ww/

If you choose to use Fitbit, please carefully refer to the relevant "User Agreement" and "Privacy Policy" issued by Fitbit. For details, please view: https://www.fitbit.com/global/us/legal/privacy-policy

The purpose of sharing information is to measure and analyze health indicators related to you. Otherwise, we will not disclose such health information to any other third party or use

health-related information for other purposes not defined in this policy. You can disconnect the authorized connection between the Aubor application and the third-party health platform at any time by managing your health settings in the health management center on your mobile device . When we add new third-party sharing channels, we will never share your information if you do not use that channel.

15. Purpose and legal basis for processing personal information

The purposes for which we process your information are as follows:

To provide you with services: We process your account information, mobile device information, usage information, location information and smart device-related information to provide the products and services you request. The legal basis for such processing is the performance of our contract with you in accordance with our User Agreement.

Improve our services: We process your mobile device information, usage information, location information and smart device-related information to ensure the functionality and security of our products, develop and improve our products and services, analyze our operational efficiency, and prevent and track fraud or inappropriate use. The legal basis for such processing is the performance of our contract with you in accordance with our User Agreement.

Non-marketing communications: We process your personal information for the purpose of sending you important information about our services, changes to our terms/conditions and policies, and/or other administrative information. At the same time, we will also send you notifications related to the services you purchased, including alert services. You can check the [Message Push] in the Aubor App ([Me]-[Message Center]-[Settings]-[Message Push]) to manage whether you require to receive such message communications. When you choose to turn off push notifications, We will no longer push such information to you. The legal basis for such processing is the performance of our contract with you in accordance with our User Agreement.

Data analysis: In order to enable you to better enjoy the convenient life brought by smart devices, we will analyze your use of Aubor services or smart devices, and analyze products or usage scenarios related to you so that you can better enjoy our products. To bring convenience, we will use your bound smart device information to recommend other smart devices that can be intelligently linked with your bound devices (smart device recommendation service). If you do not agree with us analyzing your data, you can enter the privacy settings of the Aubor App ([My]-[Settings]-[Privacy Permission Settings]-[Data Analysis]) to close your choice. The legal basis for such processing is your explicit consent. You can withdraw your consent at any time in the privacy settings, which will not affect the basic services.

Personalized recommendation service: We will process your account information, usage information, and mobile device information to provide you with customized services based on the type of device you use (including recommending and displaying product information and advertisements suitable for you), and inviting you to participate in user surveys for the products you use. This type of information is necessary to make personalized recommendations to you. If you refuse to provide it, we will not be able to recommend personalized information or services to you, display recommended purchase services, or send targeted push messages to you. Currently, Aubor does not make automated decisions regarding the processing of your personal information, but only provides scenario-based recommendation services based on your smart device type. If you do not agree with Aubor processing your personal information to obtain

personalized services, you can enter the Aubor application or the privacy settings in the application ([My]-[Settings]-[Privacy Permission Settings]- [Personalized recommendation service]) to close your selection. The legal basis for such processing is your consent. Please note that the basic scenario recommendation function only provides available scenario services (including device automation and convenient execution) based on your distribution network equipment, and is not a personalized recommendation service.

Compliance: We only process your personal information when we are required to disclose it by law, or when we believe it is necessary or appropriate to:

(a) comply with applicable laws, regulations, legal process or requests from public agencies and governmental authorities;

(b) enforce our Terms of Use and other agreements, policies or standards, including investigating any potential violations;

(c) protect our and/or other users' rights, privacy, safety or property, including you; and seek available detection, prevention, remediation or limitation of damages we may be required to provide or address security, fraud or technical question.

We also use the personal information we collect from you in other ways for which we will provide specific notice at the time of collection and obtain your consent as required by applicable law. If there are any changes in the purposes for which your personal information is processed, we will notify you of such changes via email and/or a prominent notice on our website and inform you of the choices you have regarding your personal information.

16. Who do we share your personal information with?

Aubor only shares your personal information in ways known to you. We will share your personal information with the following parties:

Disclose your personal information to third party service providers who provide certain business-related services to us, including website hosting, data analysis, payment and credit card processing, infrastructure provision, IT services, customer support services, email delivery services and others similar services to ensure they can provide services to us.

Disclose your personal information to customers and other business partners who directly or indirectly provide you with the smart devices and/or networks and systems you use to access and use our Site and Services.

In the event of a reorganization, merger, sale, joint venture, assignment, transfer or other disposition of all or a portion of our business, assets or stock (including, but not limited to, the foregoing in connection with any bankruptcy or similar proceeding), to an affiliate or Disclosure of your personal information by other third parties. In such event, you will receive clear notice via email and/or on our website of the change in ownership, incompatible new uses of your personal information, and your choices regarding your personal information.

We will share your personal information reasonably and lawfully under the following necessary or appropriate circumstances:

(a) Comply with applicable laws, regulations, legal procedures, policies and/or standards, or the requirements of corresponding public agencies and government authorities;

(b) enforce our Terms of Use and other agreements, policies and standards, including investigating any potential violations;

(c) protect our operations, business and systems;

(d) protect our and/or other users’ rights, privacy, safety or property, including you; and
(e) Risk management, detection and identification of illegal, fraudulent, deceptive or malicious activities.
(f) Disclose your personal information to the company's subsidiaries or affiliates for regular business activities.
In addition to the third parties mentioned above, we will only disclose your personal information to other third parties with your consent.
When you use services provided by a third party, we will share the corresponding information after ensuring that the third party obtains your authorization and consent, and in other circumstances that comply with laws and regulations. You can learn how third parties will process your personal information through the relevant information listed in this list. We will also strictly restrict the behavior of third parties in obtaining personal information to protect the security of your personal information. Please click "Third-party Information Sharing and SDK Service List" to view the details of third-party information sharing.
In addition, in order to ensure the stable operation of Aubor applications or to implement related independent functions, we will embed third-party SDKs in the applications. Please note that third-party SDKs may change their personal information processing types due to version upgrades, policy adjustments, etc. Please refer to their published official instructions. Please click "Third-party Information Sharing and SDK Service List" to view third-party SDK details.

17. Transfer of collected information
Aubor operates globally, so the personal information we collect in accordance with this policy may be transferred, stored and processed between different countries or regions. The applicable laws and regulations in the country or region where we operate may be different from the applicable laws in your country/region of residence, but we will strictly abide by the laws, regulations and requirements related to personal information protection (please click to view Aubor Global Data Center and Storage Condition). Therefore, within the framework of personal information protection, in order to facilitate our operations, we may transfer personal information to the countries or regions where we operate. Our privacy and security practices are designed to protect your personal information globally, regardless of where your information resides.
Including, the European Commission has determined that certain countries outside the European Economic Area (EEA), the UK or Switzerland have mechanisms that adequately protect personal information. When personal information of users in the European Economic Area, Switzerland or the United Kingdom is transferred to recipients located in countries outside the European Economic Area, Switzerland or the United Kingdom that are not deemed to have an adequate level of information protection, we will ensure that "EU Standard Contracts" are followed "Terms" for information transfer. You can click here to view the agreement concluded under the EU Standard Contractual Clauses approved under Article 46 of the GDPR. "In addition to the SCCs, we implement supplementary measures such as strong encryption for data in transit and at rest, and strict access controls to ensure that the transferred data enjoys a level of protection essentially equivalent to that within the EU."
In particular, the personal information we collect and generate during our operations in mainland China will be stored and processed in data centers in mainland China, unless cross-border

transmission is permitted in accordance with applicable laws.
If you would like to know more about our security measures, you can contact us directly through this policy.

18. Rights related to personal information
We respect your rights and will also hold your personal information.
You do not have to pay any fees to enforce your individual rights. According to the relevant requirements of the local information protection law, if your account services are in mainland China, then we will complete the verification and processing of your needs within 15 working days; if your account services are outside mainland China, then We will respond to your request within 30 days.
If you decide to send us a request by email, please indicate what information you would like to change, whether you would like your personal information to be deleted from our database, or what limitations you would like to have in our use of your personal information. Please note that for security reasons we will ask you to verify your identity before processing your request further.
You can exercise your rights related to your personal information through the following designated paths:
Right to access personal information: If you request access to the personal information we process about you (that is, apply to us for a copy of your personal information), you can go to [My] - [Settings] - [Privacy Policy Management] in the application 】-[Personal information export] to obtain information;
Right to modify personal information: If you ask us to correct inaccurate or incomplete personal information related to you, you can modify the information in the following 2 ways:
1. Modify the "Registered Account" (email/mobile phone number): [My]-[Settings]-[Account and Security]-[Modify Account];
2. Modify "nickname and/or time zone": [My] - [Personal Information];
Right to delete personal information: If you request to delete your personal information, you can go to [My]-[Settings]-[Account and Security]-[Delete Account] in the upper right corner and follow the prompts to cancel your account. and further delete your personal information;
Right to restrict the processing of personal information: When requesting to temporarily or permanently restrict us from processing some or all of your personal information, please delete your account or [My] through [My]-[Settings]-[Account and Security] in the application. 】-[FAQs and Feedback] to give us, or submit your application via info@allesin.com ;
Right to withdraw personal information processing: When we use your personal information based on your consent or our legitimate interests, if you choose to object or refuse our use of your personal information, please refer to the following "Withdrawal of Consent" processing method to withdraw your consent to processing decision:
1. As mentioned above, you can revoke your consent by changing the device permissions obtained through the application's [My]-[Settings]-[Privacy Permission Settings] in the device system settings, including location, camera/camera, Photo album (picture library/video library), microphone, Bluetooth settings, message notification push and other related functions;
2. For non-marketing communications that you agree to, turn off your choices through [Me]-[Message Center]-[Settings];
3. When you agree to the data analysis function, turn off your choice through

[My]-[Settings]-[Privacy Permission Settings]-[Data Analysis];
4. In the personalized push service you agreed to, go to [My]-[Settings-[Privacy Permission Settings]-[Personalized Push Service] to close your choice;
5. Unbind the smart device through the application, and the information about your use of the smart device will not be collected;
6. By using the login-free/guest mode of the application and exiting the use of location information-related services, we will not collect personal information about you at this time;
7. If you have previously agreed to associate your Aubor account with a third-party service, such as a third-party health platform, please unbind it on the third-party platform.
When you withdraw your consent or authorization, we will be unable to continue to provide you with the services corresponding to the part where the authorization was withdrawn. However, your withdrawal of consent or authorization will not affect the with drawal of personal information processing previously carried out based on your consent.
If you still have more questions, please go to [Me] - [FAQs and Feedback] in our app, or please send an email to info@allesin.com

19. Information security measures
We maintain commercially reasonable physical, administrative and technical safeguards to maintain the integrity and security of your personal information. Aubor provides a variety of security strategies to effectively ensure the information security of users and devices.
In terms of device access, we use Aubor’s proprietary algorithms to ensure data isolation, access authentication and authorization applications.
In terms of data communication, communication using security algorithms and transport encryption protocols as well as commercial-grade information encrypted transmission based on dynamic keys is supported.
In terms of data processing, strict data filtering and verification and a complete data review process are adopted.
In terms of data storage, all confidential information of users will be securely encrypted for storage.
In addition to the above-mentioned technical security guarantees, Aubor has also formulated a series of security guarantees at the institutional and management control levels, including assigning positions and responsibilities, holding security and privacy protection training courses, strengthening employee data protection awareness, controlling access rights and other measures , to prevent data loss, illegal use, unauthorized access or leakage, tampering or damage.
If you believe your interaction with us is no longer secure for any reason (For example, if you believe)by sending an email to info@allesin.com as set out below .
If a security incident occurs that affects the security of your personal information, we will notify you without undue delay and, where feasible, not later than 72 hours after becoming aware of it, where the incident is likely to result in a high risk to your rights and freedoms.through your reserved email address, phone number, message center push, etc., and inform you of suggestions and other information to reduce or prevent related risks. When necessary, we will take corresponding remedial measures in a timely manner in accordance with the internal security incident emergency plan, and report to the relevant competent authorities in accordance with

regulations.
We have obtained Enterprise Privacy Certification (EPC). For more information about EPC.

20. Information retention period

We will process your personal information within the shortest period required to achieve the purposes stated in this policy or as required by laws and regulations, unless a longer period of time is required based on specific legal requirements. We will determine the appropriate retention period based on the amount, nature and sensitivity of the personal information, and after the retention period, we will destroy your personal information.
To meet your requested products and services in accordance with the User Agreement and this Policy;
When you explicitly request to delete your personal information, we will set this as a task and no longer retain your personal information.
When we confirm that the purpose of collection and processing of personal information has been completed based on 1), or after we confirm your deletion or cancellation request based on 2), or after we terminate the operation of the corresponding products or services, we will stop retaining and your personal information will be deleted. Generally, we will no longer retain your personal information once the specified information retention period is reached. If we are unable to destroy the information for technical reasons, resulting in the retention of personal information beyond the storage period, we will take appropriate measures to prevent further use of your personal information, including anonymization.

21. Protection of children's personal information

Aubor attaches great importance to the protection of children's personal information. If you are under 14 years old (or the prescribed age in your country/region), you must carefully read the " Aubor Children's Privacy Protection Statement" before you use our services and obtain the written consent of your parent or legal guardian in advance. Aubor protects children's personal information in accordance with the relevant laws and regulations of each region, country or region. Please note that if we discover that a child's personal information has been collected without prior, verifiable parental or legal guardian consent, we will seek to delete the relevant personal information as quickly as possible.

22. Statement on Policy Changes

We will update this policy at least annually as our information practices change. If we make any material changes, we will notify you via email (sent to the email address specified in your account) or post a notice within the Application before the changes take effect. We recommend that you periodically browse the Application to obtain the latest information on our privacy practices.

23. Contact us

If you have any comments or questions about this Privacy Policy, or if you have any questions about our collection, use or disclosure of your personal information, please contact us through [My] - [FAQs and Feedback] in the Aubor app or provide the information below Contact us and specify "Privacy Policy". When you have rights requests and questions related to personal information, we have a professional privacy and security team to solve your problems. If your

question itself involves a larger matter, we may ask you to provide more information to confirm the nature and impact of the matter. If you are not satisfied with the response you receive, you can refer your complaint to the appropriate supervisory authority. When you consult us, we will provide information on possible complaint channels based on your actual situation, and will complete verification and processing of your needs within 15 working days.

Contact details and address:

Aubor Oriental(Beijing) Digital Technology Co., Ltd.

Mailing address: 11/F, Donghuang Mansion, 16 Guangshunnan Street, Wangjing Street, Chaoyang District, Beijing, China

Email:Privacy office:info@allesin.com; Customer Service Tea: info@allesin.com;