UNV-Link User Privacy Policy

Version: 1.15
Last updated on 8th Jul, 2025

Thank you for choosing Bresee.
Jinan Boguan Intelligent Technology Co., Ltd. (referred to as , Bresee, we, or us hereafter) takes "continuously creating and building an intelligent and beautiful society with AI technology" as its corporate development vision. Rooted in the fields of smart IoT, intelligent transportation, and smart industry, it provides a panoramic AI algorithm solution system and technical support services to realize AI empowerment in ecological scenarios across multiple levels and fields. Bresee is committed to building a better world by providing professional, reliable and cutting-edge products and services.
Bresee is committed to protecting your personal information and privacy and maintaining your trust with us. We abide by the following principles to protect your personal information: **integrity, consent, clear purpose, restricted collection, minimum necessary, transparency, balanced rights with responsibility, security, and privacy compliance**.
This privacy policy is intended to help you understand: 1) your personal information that we collect; 2) how we collect your personal information; 3) how we use your personal information; 4) how we protect your personal information and your rights; 5) answers to your questions and how to contact us.
Understanding these contents is essential for you to exercise your personal rights and protect your personal information. Please read through this policy carefully before you use or accept our products or services.
This policy contains the following sections:

(1) Scope of this policy

1. This policy applies to the products and services we provide to you. Unless otherwise stated in this policy, **it does not apply to other third-parties who collect personal information from you**. 2. Please note that as a user of our products, if you use our technology and services to serve your users, you must separately establish a privacy policy or similar legal document with your users in accordance with relevant legal requirements. This policy does not apply to the processing of personal information involved in the services you provide to your users using our service.

(2) Definitions

Personal information: Any information related to identified or identifiable natural persons (data subjects).
Non-personal information: Data other than personal information that cannot be directly linked to any specific individual, such as occupation, language, zip code, area code, serial number, URL, and automatically recorded browse data, product and unique product identifier of your mobile device, video contents without personal information, country/region and time zone of the connected product, geographical location, identifier of mobile network operator, device software platform, and hardware information, etc.
De-identification: The process by which personal information is processed to make it possible to identify a specific individual without the use of additional information.
Anonymization: The process by which personal information is processed to make it impossible to identify a specific individual and cannot be restored.

(3) How we collect and use your personal information

1. Sign up for a UNV-Link User account
a. When you sign up for an account, you need to provide your password and email address/mobile phone number. The above information is collected to meet the on-line registration system requirements of relevant laws and regulations in various region. You can provide non-essential personal information such as username according to your own needs.
b. If you only need to use the browsing service, you do not need to sign up for an account and provide the above information.
2. **When you log in to our app for the first time**, we will collect the following information of you and take appropriate control measures:

Information collected	**Control method**	**Purpose**
Model of your mobile phone	For the first-time use, a pop-up window will	

Operating system and version of your mobile phone	appear to notify you. When the collection method, contents, or purposes are changed, we will notify you of the changes and ask for your permission.	To determine the push service

3. Permission description

When you use our app, we will need you to authorize us certain permissions in your mobile phone. If you refuse such permissions, you will be unable to use the relevant functions, but it will not affect your normal use of other functions of the app. For information about permissions that we ask for, refer to the table below. Please note that we ask for the permissions only when you use the relevant functions. You may disable these permissions in the system settings of your mobile phone. If you choose to disable certain permissions, we will no longer collect or use the related personal information, and we will not be able to provide the services associated with those permissions.

a. Sensitive Permissions

Permission	**Application scenario**	**Function**
ACCESS_FINE_LOCATION access precise location	Add Wi-Fi device; initialize JPush service	Obtain Wi-Fi information to connect device to network; network connection request from Aurora server to ensure stable and continuous JPush service
CAMERA camera	Read QR code to add device; retrieve device password; face import function	Use camera to read QR code to obtain device information to add device or retrieve password; import face information to device
RECORD_AUDIO microphone	Device audio intercom and doorbell intercom; access control device video call; set custom alarm sound	Two-way audio between user and device; answer video call from access control devices; record custom alarm sound as an alarm-triggered action
READ_EXTERNAL_STORAGE read external storage	Read QR code to add device, retrieve device password; face import function	Used to scan QR code in album to add device or import face information into device
WRITE_EXTERNAL_STORAGE write to external storage	Import snapshots or videos into system album	Download snapshots or videos to system album

b. Common Permissions

Permission	**Application scenario**	**Function**
ACCESS_NETWORK_STATE obtain network status	When app is running	Used to obtain network status information to improve video communication efficiency
ACCESS_WIFI_STATE obtain Wi-Fi information	When app is running	Used to obtain network status information to improve video communication efficiency

INTERNET connect to network	When app is running	For Internet connection using SIM card
CHANGE_NETWORK_STATE change network status	When app is running	Update device status after network changes
CHANGE_WIFI_STATE change Wi-Fi status	When app is running	Update device status after network changes
RECEIVE_BOOT_COMPLETED automatic startup at system boot	When app is running	Used for Android persistent connection
SYSTEM_ALERT_WINDOW display on top of other apps	When a dialog box opens	Request for floating box permission to display a pop-up dialog box in the system
VIBRATE control device vibration	When using the push service	Used for vibration reminder when the mobile phone receives a notification message from push service such as Mi Push
DISABLE_KEYGUARD allow app to disable keyboard guard when it is not safe	When on-screen keyboard is opened	Allow app to disable keyboard lock
WAKE_LOCK prevent mobile phone from going into sleep status	When video is playing	Used for video playing to prevent mobile phone screen from going to sleep
FLASHLIGHT control flashlight	When scanning QR code	Control flashlight to scan QR code to connect smart device in low-light environment
MODIFY_AUDIO_SETTINGS change audio settings	Device audio intercom or doorbell intercom	Used for audio settings when having two-way audio with device or doorbell
BATTERY_STATS	When app is running	Used for data processing before shutdown due to low battery
MOUNT_UNMOUNT_FILESYSTEMS	When saving or reading video tutorial or configuration file	Permission to read files in SD card
C2D_MESSAGE	When initializing the push service	Used to receive notification messages
RECEIVE_USER_PRESENT	When initializing the push service	Used to wake up the screen or unblock radio when receiving alarm notifications
DOWNLOAD_WITHOUT_NOTIFICATION	Download upgrade file, configuration file or tutorial video	Used for file download
com.coloros.mcs.permission.SEND_MCS_MESSAGE	When initializing the push service	Used for message push service on OPPO mobile phones
com.heytap.mcs.permission.SEND_MCS_MESSAGE	When initializing push service	Used for message push service on OPPO mobile phones
com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	When initializing push service	Used for message push service on OPPO mobile phones

com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	When initializing push service	Used for message push service on OPPO mobile phones
USE_FULL_SCREEN_INTENT	When initializing push service	Full screen notification, tap doorbell notification in background
PROCESS_PUSH_MSG	When initializing push service	Used for message push service on Huawei mobile phones
MIPUSH_RECEIVE	When initializing push service	Used for message push service on Xiaomi mobile phones
JPUSH_MESSAGE	When initializing push service	Used for the JPush message push service
BLUETOOTH connect to Bluetooth device	When app is running	Used to connect to a paired Bluetooth device and achieve audio adaptation to the Bluetooth device
BLUETOOTH_ADMIN discover and pair with Bluetooth device	When app is running	Used to connect to a paired Bluetooth device and achieve audio adaptation to the Bluetooth device
SENSOR_SERVICE light sensor; accelerometer sensor	1.When scanning QR code 2.When using the shake function	1.Used to prompt user to turn on flashlight when scanning QR code in low-light environment 2.Used to obtain the shake status and open the advertising app
OTIFICATION_SERVICE notification service	When using notification service	Used to display or clear notifications in the bar
WINDOW_SERVICE window service	When obtaining window size	Used to fit the window size in the app screen
INPUT_METHOD_SERVICE soft keyboard	When using soft keyboard	Used to display soft keyboard when entering mobile phone number, username, password, etc.
POWER_SERVICE power status	When local video is playing	Used to wake up the screen when local video is playing
CLIPBOARD_SERVICE clipboard information service	When copying share links	Used to copy share links

4. Video information
   When you use our service to save video related contents, such as video clips, live video streams, images (user contents), message notifications, etc., we will collect video images captured by your camera and push video images to you so you can save the contents that you need. Such information is necessary for the function. If you refuse to provide such information, you will not be able to save the contents you need.
5. Message push
   When you use the message notification function, we need to collect the unique feature value of your client (such as the unique value generated based on your device's IMEI, Android ID, or UDID) and the language of your mobile

phone. The purpose is to provide precise alarm message notification in the language you prefer.

Such information is necessary for the function. **If you refuse to provide such information, you will not be able to use the alarm subscription function, but it will not affect your normal use of other functions.** You can choose to turn off the function and clear information about the unique feature value of your client.

6. Device adding

   When you use device adding functions, we may need to collect the serial number, register code, password, model, MAC address of your device, and Wi-Fi information (read Wi-Fi's BSSID) of your client. The purpose is to configure network on your device and bind your device. Such information is necessary for the function. **If you refuse to provide such information, you will not be able to add your device.**

7. Connecting device to cloud

   When you use our device connection service, **to ensure your normal use of our service, we will collect information including the model, UDID, IP address, MAC address, software version, network connection method and type, latitude and longitude (if applicable), and operation records of your device.** Such information is necessary for the service. **If you refuse to provide such information, you may not be able to connect your device to cloud.**

8. Live view

   When you use the live view function, we will collect the serial number, IP address, port number, and video stream information of your device in order to provide you with live streams of your device. **Such information is necessary for the function. If you refuse to provide such information, you will not be able to use the live view function, but it will not affect your normal use of other functions.**

9. Cloud storage

   The cloud storage service is free or prepaid. It does not support return, exchange or account change after purchase. The service is only for lawful and legitimate purposes, and you should ensure that you do not use the service for any illegal or infringing activities, and assume full responsibility independently and completely for the purchase and use of the service.

   When you use the cloud storage function, we may need to collect the device serial number, cloud storage order information, and video stream information. The purpose is to save the video of your device to the cloud. **Such information is necessary for the function. If you refuse to provide such information, you will not be able to use the cloud storage function, but it will not affect your normal use of other functions.**

10. Information that you provide proactively when using our service

    When you use analysis, comparison functions and alarm service based on user benchmark information (including face/human body recognition, license

plate/vehicle recognition, attendance management, fingerprint unlocking, if applicable to your device), you need to enter the benchmark information such as **face images, license plate information, attendance personnel information, fingerprints** into the system in advance. **Such information is necessary for the service. If you refuse to provide such information, you will not be able to use the relevant analysis, comparison functions and alarm service, but it will not affect your normal use of other functions.**

11. Device sharing

    When you use the device sharing function, we need to collect certain information in order to implement the sharing, including the device serial number, your nickname, and the usernames with which you want to share the device. **Such information is necessary for the function. If you refuse to provide such information, you will not be able to use the device sharing function, but it will not affect your normal use of other functions. The sharing function is active only when you use it; it is not permanently active.**

12. Customer service

    When you need our support and contact us through email, telephone or our customer support tools, we need to collect information including **your name, phone number or email address, enterprise or organization, device usage, device serial number, device account, and SIM card number** during the process of communication. The purpose is to verify your product and identity and provide precise service support. If you refuse to provide such information, we will not be able to provide support services to you.

13. In other possible scenarios, we will also collect your personal information, including:
    a. When you contact us by telephone, we collect call recordings to promptly analyze interactions and effectively respond to your requests, ensuring high-quality after-sales support.
    b. In situations where you need to sign a certificate to authorize remote access, we will collect your manual signature or company seal.
    c. <u>If you report a device failure and need to return the device to us for inspection and repair, you need to provide your receiving address. If the returned device contains your private data, you need to back up the data and format the storage before returning the device.</u>
    d. When you forget your device password and need to regenerate it, you can get a temporary password by scanning the QR code if you bind an email or mobile phone number. If you haven't bound your email or mobile phone number, please call our customer service hotline (+86 18768170822) to get help.

14. In order to offer better user experience and prevent misoperation, we will collect industry-standard non-personal information (see the definition in Chapter 2). Such information does not infringe on user privacy and user rights. If you have any concerns about the security and privacy settings of

your mobile device, please adjust the settings by referring to the documentation of your mobile service provider or mobile device manufacturer. These actions include but are not limited to:

a. We may record adjustments that you make to your product through the services that we provide, and we will store the collected non-personal information with the information directly collected by the product.
b. We also use cookies, web beacons, pixel tags, and other technologies to record and store your settings, and to collect non-personal information such as log data and device data. To work with other information, ensure proper operation, better understand and resolve your issues, help us improve our products and services, and provide you with a more seamless browsing experience, we store small data files called cookies on your mobile device. Cookies typically contain identifiers, website names, and some numbers and characters. We can only access cookies provided by our company. You can refuse the collection of cookies by declining the use of cookies in your browser settings. For detailed instructions on how to adjust your browser settings, please visit the relevant settings page for your browser. In addition to cookies, we also use web beacons, pixel tags, etc. Web beacons are often transparent images embedded in web pages or emails. Pixel tags in emails allow us to determine whether emails are opened. If you do not want us to track your activities in this way, you can opt out of our mailing list at any time.
c. When you use audio recording or media streaming functions of our product, we may record and transmit videos and/or audios from the product, with your permission. This may include taking snapshot images and attaching part of snapshot images and analysis data to email notifications.

(4) Sharing, transfer and disclosure of personal information

1. Sharing of information
   When we provide you with certain services, we need to share your personal information with authorized partners, carefully selected service providers, or national regulatory agencies, only for legal, justified, necessary, specific, and definitive purposes, and only share the information necessary for us to provide services. The organization that shares your personal information has no right to use the shared personal information for any other purposes irrelevant to our products or services. For companies, organizations, and individuals with whom we share personal information, we will sign strict data protection agreements with them, demanding them to process personal information as per our instructions, this privacy policy, and any other relevant confidentiality and security measures.

2. Transfer of information
   We will not transfer your personal information to any other companies, organizations or individuals, except in the following situations:
   a. After obtaining your explicit consent.
   b. When it involves mergers, divisions, dissolutions, acquisitions, asset transfers, asset reorganizations, or bankruptcy liquidations, and if it involves the transfer of your personal information, we will demand the new company or organization that holds your personal information to continue to be bound by this personal information protection policy; otherwise, we will demand the company or organization to re-seek authorization and consent from you.
3. Disclosure of information
   In principle, we do not disclose your personal information to the public. We will disclose it only under the following circumstances:
   a. After obtaining your explicit consent.
   b. Please understand, in accordance with applicable laws, we can disclose your personal information without your consent under the following circumstances:
      - When it is directly related to national security and defense security.
      - When it is directly related to public safety, public health, and significant public interests.
      - When it is directly related to criminal investigation, prosecution, trial, and verdict.
      - When it is necessary to safeguard significant legitimate rights such as life, property of the personal information subject or other individuals but it is difficult to obtain your consent.
      - When the personal information collected is disclosed to the public by yourself.
      - When the personal information is collected from information that has been disclosed lawfully, such as from lawful news reports, government-disclosed information, etc.
      - When it is necessary for signing a contract according to your requirements.
      - When it is necessary for maintaining the safe and stable operation of the provided products or services, such as detecting and handling product or service failures.
      - When required for academic research institutions conducting statistics or academic research based on public interest, and when providing academic research or descriptive results, the personal information included in the results is de-identified.
      - When required by applicable laws and regulations and government orders of the country where the business is operated, as well as legal procedures of law enforcement agencies, regulatory agencies, and court of law, or other applicable legal procedures and subpoenas.

(5) Storage and protection of personal information

1. Storage of personal information
   Wherever you use our services, we will transmit and process your information globally with the help of our own facilities and through service providers or partners. Since our company operates worldwide, we may transfer your personal information to our global affiliates for the purposes described in this privacy policy. For example, if you request customer service from us, our colleagues in China may access certain information to assist you, regardless of your location. We do so in compliance with applicable laws, in particular, we ensure that all transfers comply with your local data protection laws. You hereby consent to these data transfers and have the right to know the safeguards we've implemented for these transfers.
   Currently, we have data centers in North America (USA), the Asia-Pacific region (Singapore, Vietnam), and Europe (Germany). The laws, regulations, and standards of the country in which your information is stored or processed may be different from those of your own country. You have understood that the risks under applicable data protection laws are different and we may transfer to and store your personal information at our overseas facilities. However, this does not change any of our commitments to safeguard your personal information in accordance with this Privacy Policy.
   Unless explicitly permitted by law or by you, we will retain your personal information only for the length of time required for the purposes bound by this privacy policy. During the period that you use our products or receive our services, we will continuously keep your personal information for you, and we will delete or anonymize your personal information after the service period has expired. If you cancel your account or proactively delete your personal information, we will delete or anonymize your personal information within 48 hours after receiving your request, unless otherwise stated in law or agreement.
2. Security protection of personal information
   We are committed to safeguarding your information security and have a dedicated team responsible for the research, development and application of a variety of security technologies and programs. We use data encryption and access control mechanisms to establish internal control systems to ensure only the authorized personnel can access your personal information, to publicize security and privacy protection requirements to the related personnel, and to publicize protection measures such as the information security protection system to all the staff. At the same time, we have been granted information security management system certification (ISO27001 international standard), and will regularly hire independent third-party organizations to evaluate our information security management system. Through these rigorous measures, we try our best to protect your information from unauthorized access, use and disclosure. **However, please understand that in the**

Internet industry, due to the limits of current technologies and all kinds of possible malicious attack methods, even if we do everything that we can to strengthen our security measures, it is impossible to guarantee 100% security of information. Please be aware, the systems and communication networks that you use while using our products and/or services may encounter security issues due to factors that are beyond our control. Therefore, we strongly recommend that you take proactive measures to safeguard the security of your personal information, such as using complex passwords, changing your password regularly, and not disclosing your account passwords and related personal information to others.

We have established dedicated management systems, procedures and organizations to safeguard information security. We strictly limit the scope of people who have access to the information, demand their compliance with confidentiality obligations, and conduct audits regularly.

In the event of a security incident such as personal information leakage, we will initiate an emergency plan to prevent the expansion of the security incident and promptly inform you in the form of push notifications, announcements, etc.

(6) Your rights

1. Access your personal information. You can tap Me > Profile photo or information bar to access the personal information you provided.
2. Correct your personal information. You have the right to update your personal information at any time. You can also correct your personal information after finding the information collected and stored by us is incorrect. You can correct or change your username, password, email address or mobile phone number in Me > Profile photo or information bar.
3. Delete your personal information. You can delete the personal information online by yourself or contact us (wangchen.hz@gmail.com or +86 18768170822) to delete it for you. We will delete or anonymize your personal information after the minimum retention period required by the applicable laws and regulations.
4. Revoke authorization. You can disable permissions on your mobile phone as needed (including access to your location, phone, album, camera, microphone, and notification).

   After you withdraw consent or authorization, we may not be able to provide the related services, but it does not affect us handling your personal information based on your previous consent or authorization.
5. Cancel your account. You can tap Me > My profile photo or information bar to cancel your account.

   After you cancel your account, unless otherwise provided by laws and regulations, we will stop providing services to you, keep your personal information for the length of time stated in this agreement, and then anonymize your personal information.

6. If you cannot access, correct, delete your personal information, or withdraw consent using the above ways, you can contact us by sending an e-mail to wangchen.hz@gmail.com or by calling customer service at +86 18768170822. We will respond within fifteen working days after verifying your identity. We reserve the right to decline requests that are unreasonably repetitive, require excessive technical efforts, pose risks to other's legitimate rights, or are otherwise highly impractical.
7. Notwithstanding the above agreements, in accordance with relevant laws, regulations, and national standards, we may be unable to respond to your requests in the following circumstances:
   - When it is related our fulfillment of obligations as stipulated by laws and regulations.
   - When it is directly related to national security and defense security.
   - When it is directly related to public safety, public health, and significant public interests.
   - When it is related to our fulfillment of obligations as stipulated by laws and regulations.
   - When it is directly related to criminal investigation, prosecution, trial, and verdict.
   - Where there is sufficient evidence indicating that you have subjective malice or abuse of rights.
   - When it is necessary to safeguard significant legitimate rights such as life, property of the personal information subject or other individuals but it is difficult to obtain your consent.
   - When responding to your request would result in serious harm to the legitimate rights and interests of you or other individuals or organizations.
   - When involving trade secrets.

(7) Third-party services

Our products and/or services may be connected to or linked to websites or other services provided by the third party, for example, when you use the share function to share some of your information to third-party services. These functions may collect your information (including your log information) in order to operate properly. We will only share your information for legitimate, necessary, and specific purposes. For third-party service providers with whom we share information, we demand them to fulfill confidentiality obligations and take corresponding security measures.

In order to achieve the purposes stated in this policy, we may connect SDK or other similar applications provided by third-party service providers, and share with them certain information about you that we collect in accordance with this policy, so as to provide better customer service and user experience. At present, the third-party service providers we connect include the following types:

1. Used for notification push function, including the push function provided by mobile phone manufacturers.

2. Used for obtaining your device location, collecting device information and log information with your consent.
3. Used for third-party authorization services to share relevant contents with third-party products, etc.
4. Used for services related to account security, product reinforcement, including data encryption, data decryption, etc.

Such third-party services are operated by the relevant third party; your using their services or providing information to them are subject to the terms of service/or privacy protection statements of the corresponding third party (not this policy). For information about third-party services that we are currently using, please refer to the table below.

Third-party SDK	**Description**
JPush	Operator: Shenzhen Hexun Huagu Information Technology Co. Ltd.
	Function: Push notifications
	Application scenario: Provide notification push service. When you use the push service of the APP, JPush SDK needs to use the auto-launch function so that you can receive messages (such as alarms) pushed by the app when it is closed or running in the background. At the certain frequency, the app will start automatically or start the third-party app after being wakened by the system.
	Scope of collected personal information Device parameters and system information (device type, device model, system version, and related hardware information), device identifiers (IMEI, IDFA, Android ID, GID, MAC, OAID, VAID, AAID, IMSI, MEID, UAID, SN, ICCID, SIM information), network information (IP address, Wi-Fi information, base station information, DNS address, DNCP address, SSID, BSSID) and location information, app list and active status information (application crash information, notification switch status, app application list and active status, app application page information, app function event related information), push information logs
	Purpose of collecting personal information Device parameters and system information: used to identify user's device type, device model, system version, etc., to ensure accurate message delivery Device identifier: used to identify user uniquely and ensure accurate delivery of push messages Network information and location information: used to improve network connection requests from SDK to JPush server to ensure stable and continuous service and realize the push function

	App list and active status information: used to save battery and data traffic for user
	Required sensitive permissions: storage, location
	Privacy policy: https://www.jiguang.cn/license/privacy
Baidu Speech Synthesis	Operator: Beijing Baidu Netcom Science Technology Co., Ltd.
	Function: Text-to-speech conversion
	Application scenario: Custom alarm sound for device
	Scope of collected personal information: network status, Wi-Fi status, device model, operating system, permission to read/write external storage.
	Privacy policy: https://ai.baidu.com/ai-doc/REFERENCE/Jkdyl0v3v
Agora RTC SDK	Operator: Shanghai Zhaoyan Network Technology Co., Ltd.
	Function: Real-time audio and video service
	Application scenario: When playing audio and video
	Permission access: (Optional) Microphone permission, camera permission, Bluetooth permission
	Sharing method: SDK native collection
	Scope of collected personal information Device brand, model, operation system, CPU information, memory utilization, battery information, screen resolution, IP address, network access methods and types, use ID in channel, sensor information (orientation sensor)
	Purpose of collected personal information: Test access and connectivity of audio, video, network, etc., provide compatibility and troubleshooting for different devices, provide screen adaptation
	Privacy policy: https://www.agora.io/en/privacy-policy/
Agora RTM SDK	Operator: Shanghai Zhaoyan Network Technology Co., Ltd.
	Function: Provide real-time messaging
	Application scenario: When signaling transmitting audio and video
	Sharing method: SDK native collection
	Scope of collected personal information Device brand, model, operation system, memory utilization, IP address, network access method and type, user ID in channel
	Purpose of collected personal information: Test access and connectivity of audio, video, network, etc., provide compatibility and troubleshooting for different devices
	Privacy policy: https://www.agora.io/en/privacy-policy/

(8) Privacy of minors

We do not provide any of our services to minors under 14 years of age (or equivalent minimum age set by the relevant jurisdiction). If we find any account associated with or registered by a minor under 14 years of age (or equivalent minimum age set by the relevant jurisdiction), we will immediately delete the relevant account information. If we find that we have collected personal information of minors without prior verifiable parental consent, we will try to delete the relevant data as soon as possible.
If you are the parent or guardian of a minor under the age of 14 (or equivalent minimum age set by the relevant jurisdiction), and you believe that your minor has disclosed her/his personal information to us, please contact us immediately through your local Bresee service phone number or e-mail address. Parents or guardians of minors who are under 14 years of age (or equivalent minimum age set by the relevant jurisdiction) can check and ask us delete the minor's personal information and prohibit us from using it. In cases where we collect personal information of minors with the consent of the parents/guardians, we will only use or publicly disclose the information when permitted by law, expressly allowed by the parents or guardians, or when necessary to protect the minors.

(9) Contact us

The registered address of Jinan Boguan Intelligent Technology Co., Ltd. is 20th Floor, Building 2, Import and Export Enterprises Comprehensive Service Center and Ancillary Facilities Project, Gangxi Road No. 1 Entrepreneurship Base, Suncun District, Jinan, China (Shandong) Pilot Free Trade Zone，China.
We have set up a dedicated department to protect your personal information. If you have any questions, comments or suggestions regarding this privacy policy or your personal information, please contact us via the following methods:

- Email: wangchen.hz@gmail.com
- Tel: +86 18768170822
- Mailing address: 20th Floor, Building 2, Import and Export Enterprises Comprehensive Service Center and Ancillary Facilities Project, Gangxi Road No. 1 Entrepreneurship Base, Suncun District, Jinan, China (Shandong) Pilot Free Trade Zone，China.

We will process your inquiry or request within fifteen working days after verifying your identity.

(10) Revisions to privacy policy

This privacy policy is subject to revisions from time to time, and such revisions shall constitute a part of this privacy policy. When the terms of this policy are changed, we will show you the changed policy in the form of push notifications, pop-up windows or other reasonable means when you log in and upgrade the

version. Please note that we will collect, use and store your personal information according to the updated policy only after you click the Agree button in the pop-up window.

(11) Others

Any disputes regarding this policy or our handling of your personal information can be submitted to courts of competent jurisdiction in Hangzhou City, Zhejiang Province, China.