Shanghai Yanding Information Technology Co., Ltd. Privacy Policy

Welcome to the website and services of Shanghai Yanding Information Technology Co., Ltd.!

Shanghai Yanding Information Technology Co., Ltd. (hereinafter referred to as "we" or "Yanding") always regards the protection of personal information as a core corporate responsibility, strictly complies with laws and regulations such as the "Personal Information Protection Law of the People's Republic of China" and the "Data Security Law of the People's Republic of China", as well as relevant national standards and industry norms. We are well aware of the importance of personal information to user rights and interests, and therefore adopt both technical and management measures to ensure the legality, transparency, and security of data processing activities.

This "Privacy Policy" aims to clearly explain to you:

1. How we collect, use, store, share, and protect your personal information;
2. Your rights and how to exercise them in personal information processing activities;
3. Our special protection measures for minors' information;
4. Policy updates and user communication mechanisms.

Please be sure to read the full text of this policy carefully, especially the **key terms marked in bold or underlined**. If you have any questions about the policy content, you can contact us through the contact information at the end. **Using our products or services indicates that you have fully understood and agreed to all contents of this policy.**

We promise to always follow the "**Principle of Minimum Necessity**", only collecting personal information necessary to achieve service functions and avoiding excessive collection. You can flexibly manage the authorization scope of personal information through setting options. Refusing to provide non-essential information will not affect your use of basic services.

Table of Contents

1. About Us

1.1. Company Introduction

Shanghai Yanding Information Technology Co., Ltd. (hereinafter referred to as "Yanding" or "we") is a technical service entity with independent research and development capabilities. The core team is composed of professionals in the field of [data security and privacy protection]. Relying on the technical resources and compliance experience of affiliated enterprises, we are committed to providing users with safe and reliable products and services. If you need to contact us, please refer to Chapter 10 "**Contact Information**" of this policy.

1.2. Policy Scope of Application

(1) This "Privacy Policy" applies to all products and services provided by Yanding and its affiliated enterprises (hereinafter collectively referred to as "we"), including but not limited to:

① Services provided through clients such as websites, mobile applications, and mini-programs;

② Innovative services developed based on new technology forms such as artificial intelligence and the Internet of Things.

(2) Applicable Objects: This policy mainly governs the **data processing** relationship between us and users who use the products and services.

(3) Special Situation Explanations:

① **Separate Statements for Sub-services**: If a specific product or service (such as a specific functional module) has a separate privacy policy, that policy is a special agreement and takes precedence over this policy; contents not covered shall still be governed by this policy.

② **Third-Party Service Boundaries**: When you access third-party platforms (such as partners' applications, open platform interfaces, etc.) through our services, the processing of relevant personal information will be carried out by the third party according to its privacy policy. You need to assess the risks of third-party services yourself. We do not bear joint liability for the data processing activities of third parties.

③ **Minimum Coverage Principle**: This policy only regulates service scenarios directly provided by us. If you use personal information for purposes not agreed upon in this policy (such as reselling or sharing it with other users on your own), the relevant risks shall be borne by you.

2. Personal Information Processing Principles

2.1. Principle of Legitimacy, Justification, and Necessity

We promise to always follow the following principles when processing your personal information:

(1) **Legality**: All data processing activities are strictly carried out in accordance with laws and regulations such as the "Personal Information Protection Law of the People's Republic of China" and the "Data Security Law of the People's Republic of China", ensuring that the processing purposes and methods have a legal basis.

(2) **Justification**: Information is collected only for legitimate purposes such as providing you with products/services, optimizing user experience, or fulfilling legal obligations, and obtaining data by fraudulent, coercive, or other illegitimate means is prohibited.

(3) **Necessity**: Only information necessary to achieve specific functions is collected (e.g., mobile phone number for identity verification, location permission for map navigation). Data collection beyond the necessary scope is prohibited.

2.2. Principle of Minimization and Transparency

To protect your right to know and control, we take the following measures:

(1) **Data Minimization**:

Collection Scope: Strictly limited to core fields necessary to achieve service functions;

Storage Period: Immediately deleted or anonymized after exceeding the retention period required for services and business.

(2) **Process Transparency**:

Clearly disclose data types, usage scenarios, and third-party sharing scope in the privacy policy;

Notify you in real time of the direct impact of data processing through interactive prompts (such as permission request pop-ups).

(3) **Dynamic Optimization Mechanism**:

Regularly review the necessity of data processing activities and eliminate unnecessary links;

Adopt privacy-enhancing technologies to reduce data exposure risks and explain improvement measures through version updates.

3. **How We Collect and Use Your Information**

3.1. Information Collection Methods

We will collect your personal information in the following two ways:

(1) User Active Submission

① Account Registration and Service Use

You may need to provide some basic information, such as: [Basic information for personal real-name authentication (name, ID number, etc.), company basic information (company name, business registration information, etc.), phone number, email address and other relevant basic information].

② Product Services and Test Analysis

During use, due to data analysis needs, you may actively upload content such as [corresponding text, pictures, audio, video, or other files] for testing, research, or development.

To ensure the accuracy of analysis results, we extract information from the test images you upload for use as test data for product optimization and iteration. The relevant algorithms are only used to provide test analysis services and result feedback, optimize product functions, and technical improvements. We will not extract personal or company-related information unrelated to the analysis.

③ Problem Feedback and Complaint Handling

When you provide feedback, suggestions, complaints, or request customer support, you may need to provide relevant information such as [problem description, appeal content, and contact information].

(2) Technical Data Acquisition

① Device and System Information

We will automatically collect your device information through technical means, such as device model, operating system version, unique device identifier, etc.

② Usage Behavior Records

The server automatically records your usage, including access time, IP address, etc.

③ Location Confirmation

If you use location-based services, we will collect your location information.

④ Behavior Analysis Technology

We may use Cookies and similar technologies to understand your usage habits in order to provide more personalized services.

3.2. Information Use Types and Purposes

(1) Authorization Items and Permission Content

Item	Permission Content
Microphone Permission	When you send voice messages or use your voice as the reply voice or call voice corresponding to our service, we will request your microphone permission.
Camera and Gallery Access Permission	When you actively take photos, we will request your authorization for camera permission.
Location Information Permission	When you use location-based services, we will request you to grant location information permission.

If you refuse authorization, you will not be able to use the corresponding functions related to it, but it will not affect your continued use of other functions in the application.

(2) Collected Information Types and Usage Purposes

Information Category	Example Content	Collection Purpose
User Identity Identification Information	Contact number, email, other identity or basic information, etc.	Account registration, login verification, service notifications...
Information Generated During Use	Text conversations, voice records, taken or uploaded pictures/videos, etc.	Testing, analysis, report generation...
Device and Log Information	MAC address, system version, access time, etc.	Security protection, service anomaly monitoring, performance optimization...

3.3. Basic Service Functions Provided When Using Information

(1) Basic Service Support

① **Account Verification and Access Control**

During registration and login, you need to complete real-name authentication through your mobile phone number and SMS verification code. This number will be used as the main contact channel for service notifications (such as policy revisions, system maintenance reminders).

If you register through a mini-program/App, you can choose the "Quick Login" method in cooperation with communication operators. After your authorization, we will use the mobile phone number bound to the device to complete verification without repeatedly entering a dynamic password.

Support for third-party account (e.g., WeChat) login requires obtaining public information (such

as avatar, nickname) after your consent for account association and service login. If registration fields are missing, we will supplement the collection of necessary information.

② **Dialogue Service Interaction**

Function Implementation: The text, voice, images, and files you input will be used for the core functions of the service.

Temporary Data Call: When you paste content from the system clipboard into the dialog box, we will temporarily call clipboard data to achieve functional interaction.

③ Service Continuity Guarantee

To maintain service stability, we may use non-communication data, including:

System logs (access timestamp, IP address, device model);

Technical identifiers (anonymized IMEI identifier, Android ID, operating system version);

Runtime environment data (language settings, product version number).

(2) Value-Added Service Provision

① Voice Service Enhancement

Voice reply and call functions require the collection of biometric data (voiceprint information), which is only used to generate personalized voice responses. If you refuse authorization, the relevant functions will be unavailable.

② Service Optimization Mechanism

User Behavior Analysis: Your operation data such as likes, feedback, and sharing, after being processed by privacy-enhancing technologies, is used to optimize interaction design and model training.

Historical Dialogue Utilization: Anonymized historical dialogue data can be used for model iteration. You can delete such data at any time through settings.

3.4. User Warnings and Statutory Exceptions

(1) User Responsibility Warning

① Sensitive Information Upload Risk: Please do not submit inappropriate information containing third-party personal information (such as others' contact information, ID numbers, photos, etc.) or other confidential information. **Before submitting, you need to ensure that you have obtained legal authorization to avoid unintentionally leaking others' privacy or infringing upon their legitimate rights and interests. If your own actions infringe upon the rights and interests of others, legal liability arising from violative content shall be borne by you.**

② **Scenarios Where Consent is Not Required by Law**: In the following circumstances, we will process your information in compliance with the relevant provisions of the "Personal Information Protection Law of the People's Republic of China".

◆ Necessary Scenarios for Contract Performance: When you enter into or perform a contract with us (e.g., order delivery, after-sales service response, etc.), we may need to process your relevant information.

◆ Fulfillment of Legal Obligations: When we need to fulfill legal duties (including but not limited to cooperating with judicial authorities' investigations, responding to national security directives, and other legal duties), we may need to process your relevant information.

◆ Public Interest Emergency Events: In emergency situations (including but not limited to public health emergencies, conducting news reporting or public opinion supervision for public interest, etc.), in order to protect your or others' life, health, and property safety, we may need to process

your personal information.

◆ Reasonable Use of Publicly Available Information: If you have already disclosed certain personal information, or this information has been lawfully made public, we may process this information within a reasonable scope.
◆ Specially Authorized Situations by Law: Other circumstances stipulated by laws and regulations.

4. Use of Cookies and Similar Technologies
During your use of our products, we will use Cookies and similar technologies to provide you with more customized and comprehensive services.

4.1. Technical Purpose Description
We will use Cookies and similar technologies to achieve the following functions:
(1) **Personal Preference Settings**: We will store your configuration choices in the interface (such as language preference, theme mode) to avoid repeated settings affecting operational efficiency.
(2) **Service Optimization and Analysis**: We will collect anonymous data to help us understand user behavior patterns to improve website functionality and service quality.
(3) **Security Protection Mechanism**: We will identify and prevent potential security threats, block malicious attacks, and protect your account security.

4.2. User Rights Protection
(1) We assure you: We promise to use technical tools only for the purposes mentioned above, and will not use Cookies and similar technologies for data analysis or behavior tracking unrelated to business functions.
(2) We respect your rights: You can manage or disable Cookies according to your needs. Most browsers allow you to manage Cookies directly in the settings. You can choose to accept all Cookies, only accept certain types of Cookies, or completely reject all Cookies. If you wish to delete stored Cookies, you can also do this through your browser's settings options. Please note that disabling certain Cookies may seriously affect your user experience.

5. **Entrusted Processing, Sharing, Transfer, and Public Disclosure of Personal Information**

5.1. Entrusted Processing
We may entrust **third-party service providers (such as technical support parties) to process** your personal information for technical services such as data analysis, system maintenance, and technical support.
The entrusted party will process your relevant information according to the following rules; for legal, legitimate, necessary, and clear purposes; only access personal information necessary to perform their duties; adopt industry-standard security technical measures; strictly comply with our instructions and the provisions of this policy; not use information beyond the agreed processing purpose.

5.2. Sharing

We may share your personal information with cooperation partners (including related parties and third parties) only when we have obtained your express consent, or as required by law where your consent is not necessary—this is to ensure the normal functionality of features such as the Software Development Kit (SDK).
Sharing activities will strictly follow the principle of minimum necessity.

5.3. Transfer
We may transfer your personal information only when we have obtained your express consent, or as required by law where your consent is not necessary—and such transfers shall occur in scenarios involving mergers, acquisitions, or asset transfers. We will require the new holder of your personal information to continue fulfilling the obligations under this Policy; if the new holder is unable to meet such requirements, we will re-obtain your authorization and consent.
Transfers will only be conducted within the scope permitted by law.

5.4. Public Disclosure
Except in cases where we have obtained your explicit consent or where it is not required by law to obtain your consent, we will not publicly disclose your personal information.

5.5. Exceptions to Prior Authorization for Entrusted Processing, Sharing, Transfer, and Public Disclosure of Personal Information
In the following circumstances, entrusted processing, sharing, transferring, or publicly disclosing your personal information does not require prior authorized consent from you:
(1) Necessary Scenarios for Contract Performance: When you enter into or perform a contract with us (e.g., order delivery, after-sales service response, etc.), we may need to process your relevant information.
(2) Fulfillment of Legal Obligations: When we need to fulfill legal duties (including but not limited to cooperating with judicial authorities' investigations, responding to national security directives, and other legal duties), we may need to process your relevant information.
(3) Public Interest Emergency Events: In emergency situations (including but not limited to public health emergencies, conducting news reporting or public opinion supervision for public interest, etc.), in order to protect your or others' life, health, and property safety, we may need to process your personal information.
(4) Reasonable Use of Publicly Available Information: If you have already disclosed certain personal information, or this information has been lawfully made public, we may process this information within a reasonable scope.
(5) Specially Authorized Situations by Law: Other circumstances stipulated by laws and regulations.

6. Storage and Security of Personal Information

6.1. Information Security Safeguards
To better maintain personal information security, we will **avoid excessive collection of user information as much as possible** and **adopt technical and organizational measures not lower**

than the general industry standards to protect your personal information from unauthorized access, public disclosure, use, modification, damage, or loss, including but not limited to:

(1) **Data Encryption**: We will use advanced encryption algorithms to encrypt your relevant information at various stages of using your personal information, such as collection, storage, transmission, testing, and analysis, to ensure that even if the data is obtained by an unauthorized third party, it cannot be parsed to reveal the user's actual situation.

(2) **Data Transmission Security**: We will use advanced encryption technology to provide reliable security for communication between you and the server, ensuring that data is not intercepted or tampered with by unauthorized third parties during transmission.

(3) **System Security Protection**: We will regularly conduct security checks on servers and systems, and patch and optimize vulnerabilities to prevent you from being hacked or infected by viruses while using our products or services.

(4) **Institutional Guarantees**: We will establish strict institutional norms to ensure information security when users use products or services, such as regularly training and educating company employees on personal information protection to ensure all staff fully understand its importance; strictly restricting company employees' access permissions to user information and data, only allowing specific employees to access relevant data when business requires; supervising and assessing employees who access user personal information, and handling improper behavior promptly.

(5) **Data Backup**: We will regularly back up users' personal information and data, and store backup data in different geographical locations to reduce the risk of data loss due to emergencies or force majeure.

(6) **Data Leakage Early Warning**: We have established a real-time monitoring system to monitor abnormal data and leakage situations. Once signs of data leakage are detected, we will immediately take measures to block the leakage, find the cause, and formulate comprehensive improvement measures.

6.2. Sensitive Information Processing

Before collecting and using your sensitive personal information, we will clearly explain the processing purpose, method, and scope to you, obtain your separate consent, and adopt stricter security and confidentiality measures.

6.3. User Security Recommendations

It is particularly important to remind you that given the objective limitations of technical protection and management systems, absolute security for internet

data transmission and storage cannot be achieved. Once leaked, some sensitive information may have impacts that are difficult to completely eliminate.

Although we have implemented multiple security protections and continuously optimized management mechanisms, we still cannot promise to completely eliminate risks. Therefore, we solemnly urge you to jointly **strengthen the security safeguards. Do not implement the following behaviors: handing over personal accounts to others for use; providing SMS/dynamic verification codes to others; uploading core sensitive materials such as ID photos, bank card information, etc., in unnecessary scenarios; other high-risk operations**.

6.4. Emergency Response Plan

We have established a cybersecurity emergency response mechanism. In the unfortunate event of a security incident such as a data breach, the disposal process will be immediately activated to strive to contain the impact and prevent further spread.
Following the incident, we will promptly disseminate the event overview, potential risks, and the current progress of disposal measures through channels such as phone calls and push notifications at the earliest opportunity. Should large-scale information leakage make individual notification difficult, we will adopt reasonable and effective methods to inform users through official announcements. Simultaneously, we will report the incident details to regulatory authorities in accordance with the law, cooperate with investigations, and strictly pursue the legal liability of relevant entities

7. Your Rights and Choices

7.1. Right to Know and Decide
You have the right to **know and decide about the processing of your personal information, and can restrict, refuse, or withdraw authorization** (unless otherwise provided by law). You can withdraw your consent at any time. The specific operations are as follows:
(1) Understand the processing rules by reading this policy and independently choose whether to authorize. If further explanation is needed, you can contact us.
(2) If you do not agree with our necessary information processing for providing services, please suspend using the relevant functions.
(3) Adjust the authorization scope through system permission settings or in-app options. After withdrawing part of the authorization, the corresponding information will stop being processed (which may affect some functions, but does not affect previously completed processing behaviors). If you need to completely terminate authorization, you can cancel your account.

7.2. Other Rights
We provide you with the right to control and choose regarding our collection, use, and sharing of your information. According to applicable laws and regulations, you have the right to control and choose your personal information based on your actual needs. Specific rights include:
(1) The right to access, copy, correct, supplement, and delete;
(2) The right to change your authorization scope or withdraw your authorization;
(3) The right to cancel your account;
(4) The right to complain or report;
(5) Other rights enjoyed according to legal provisions.
You can contact us via the hotline【021-50275618】or email【sales@yanding.com】to exercise the above control and choice rights, or to feedback any problems you encounter during the exercise of your rights.

8. Protection of Minors

8.1. Service Target and Protection Principle

This service is mainly aimed at adults with full civil capacity, but we always place the protection of minors' personal information and privacy in an important position.

8.2. Technical Limitations and Guardianship Responsibility

Limited by technical conditions and legal norms, it is difficult for us to accurately identify the identity of minors during registration and use. Given the complexity of the online environment and the limitations of minors' risk judgment ability, we call on guardians and the platform to work together to build a clean cyberspace. It is recommended to take measures including but not limited to: strengthening information protection awareness, guiding the compliant use of AI technology, and strengthening supervision and communication.

If you find that we output inappropriate content in our products and services, please notify us as soon as possible.

8.3. Prerequisite for Use by Minors

If you are a user under the age of 18, you must obtain the explicit consent of your parents or guardians before using this service.

8.4. Special Agreement for Child Users

If you are a child user under the age of 14 (hereinafter referred to as "Child"), you need to use this service under the full supervision of your parents or guardians and obtain their written authorization.

8.5. Guardian Obligations

If you are the guardian of a child user, you must first read and agree to this policy, assist in completing the registration process, and ensure that the minor's use behavior complies with this agreement and legal provisions.

8.6. Lawful Processing of Minors' Information

We strictly follow the provisions of relevant national laws and regulations to strictly protect the personal information of minors. We only process minors' information under the following circumstances: within the scope permitted by law; with the explicit consent of parents or other guardians; based on the necessity of protecting the rights and interests of minors, etc.

If you are the guardian of a minor user and find that we have processed the minor's personal information without authorization, please contact us. We will verify and take appropriate action as soon as possible.

9. **Policy Updates and Rules**

9.1. Dynamic Optimization and Updates

To continuously improve service quality and compliance management, we will periodically adjust and improve this policy.

9.2. Notification of Major Updates

For major revisions involving core content, we will notify you through prominent methods such

as SMS and pop-up prompts.

9.3. Update Consent Rules

If you have questions or objections to the updated content, please suspend using the service after the revision takes effect. If you continue to use it, it will be deemed that you have fully known and agreed to the updated content.

10. Contact Information

10.1. Multi-Channel Contact Methods

Based on the principle of minimizing personal information processing, when you have any questions or suggestions about our policies, products, or services, you can contact us through the following methods:

(1) General inquiries or suggestions: Submit through the [Feedback within the product];

(2) Complaints, reports, or dispute handling: Send an email to 【sales@yanding.com】.

10.2. Infringement Complaint Material Requirements

When you need to complain due to infringement of your legitimate rights and interests, we need you to submit: **valid identity proof, contact information, a written request, and preliminary evidence constituting the infringement.**

We will process your request as soon as possible after verifying your identity and reply within fifteen working days.

10.3. Legal Document Service Address

【Room 701, Building 5, No. 3000 Longdong Avenue, Pudong New Area, Shanghai】