Privacy Policy (Umeng+)

# Privacy Policy

Umeng Tongxin (Beijing) Technology Co., Ltd. and Beijing Ruixun Lingtong Technology Co., Ltd. (hereinafter collectively referred to as "We", "Us" or "[Umeng+]", with the registered address at Suite 701-26, 7/F, No. 2, Haidian East 3rd Street, Haidian District, Beijing) pay high attention to the protection of personal information. When you use the services provided by the [Umeng+] platform (hereinafter referred to as "[Umeng+] Services"), we will collect and use the personal information of you and your end users ("End Users of Your Product" or "Terminal Users of Your Products", the same below) in accordance with this Privacy Policy. We hope to introduce to you clearly how we process personal information of you and your end users through this Privacy Policy, so we recommend that you read this Privacy Policy in its entirety to help you understand how you maintain your privacy.

This Privacy Policy is applicable to various services provided by [Umeng+], and you shall visit the [Umeng+] platform and use the services provided by [Umeng+], including but not limited to the website, SDKs, APIs, plug-ins , components, code, tools, and continuously innovative products and services provided by us, subject to this Privacy Policy.

If you use one or several services provided by [Umeng+] and having its or their own privacy policy, the privacy policy corresponding to such service(s) and this Privacy Policy shall jointly form a complete [Umeng+] privacy policy. If you allow us to share the said information with a third-party website, we shall also be subject to the third-party website's terms of service and privacy policy at the same time.

It should be specially noted that a third party displays, links or repackages our services and then provides products and services for you as an information controller in compliance with the third party's privacy policy, and we cannot understand or control the purpose of its information collection and use. Please access or use its services with caution until you have viewed and accepted its privacy policy.

If you provide services in an EU member state, the special provisions of this Privacy Policy regarding the EU shall apply to you.

Before using [Umeng+] products or services, please be sure to read and thoroughly understand this Policy, especially the provisions underlined in bold, which you should read carefully, and you shall use the relevant products or services after confirming your full understanding and consent of such terms. If you have any questions about this Privacy Policy, you can contact us through the contact method published by [Umeng+] (Umeng_Legal@service.umeng.com). If you do not agree with the terms of this Privacy Policy, you shall stop using the [Umeng+] service.

This Privacy Policy will help you understand the followings:

## I. How we collect and use the personal information of you and your end users

We collect information in order to perform the service you choose in a better, superior and more accurate manner. We collect information as follows:

### 1. Information that you provide for us

When you activate the [Umeng+] service and use the relevant services provided by [Umeng+], you shall fill in, submit or access the relevant information, including your contact number, e-mail address, corporate information, product information, promotion channels, Application name, and other related data.

When you conduct corporate certification, we may also require you to provide the information such as business license, uniform social credit code, business name, operating period, location, detailed address, and your certified Alipay account number.

We collect such information to provide you with better services. For this purpose, we will use your information for the following purposes:

(1) Provide you with various[Umeng+] services, and maintaining and improving these services.

(2) We may use your personal information to prevent, detect, and investigate fraud, infringement, endangering, illegal use or violation of the agreements, policies or rules with us or with [Umeng+] affiliates, in order to protect the legitimate rights and interests of you, other users, or us or [Umeng+] affiliates.

(3) Contacting you to solve the problem.

(4) Other purposes permitted by you.

### 2. Information collected during your use of the services

(1) Umeng + SDK service

Ø Collection of personal information fields:

| SDK Type | SDK Personal Information Field | Purpose | Data Protection Method |
|---|---|---|---|
| U-App statistical analysis service | Device location and rough location: IMEI/MAC/Android ID/IDFA/OpenUDID/GUID/SIM card IMSI/IP | 1. Provide SDK service based on devices<br>2. Provide regional data reports based on IPs | 1. Adopt SSL protocol encryption and HTTPS transmission encryption technology to ensure security<br>2. Take encryption, de-identification and other security measures for desensitization |
| U-Push message push service | | | |
| U-Share social sharing service | | | |
| U-Link smart hyperlink service | | | |
| U-APM application performance monitoring service | | | |
| U-Mini Mini Program statistics service | Mini Program user's account nickname/avatar, gender/region/language set by such user in the Mini Program account, as well as such user's device model/brand, operating system and system version number, resolution, etc. | Used to provide the Mini Program statistical analysis services | |

Collection of personal information fields

Ø Use of personal information permissions:

| S/N | Permission Name | Involved Product | Function Description |
|---|---|---|---|
| 1 | READ_PHONE_STATE | U-APP statistical analysis service<br>U-Push message push service | Obtain the IMEI of the user equipment, and uniquely identify the user through the IMEI in order to provide services. |
| 2 | ACCESS_COARSE_LOCATION | U-Share social sharing<br>U-Verify smart authentication service<br>U-APM application crash monitoring service<br>U-Link intelligent hyperlink service | By obtaining location information, it provides the developer with anti-fraud functions and eliminates fraudulent devices: at the same time, it corrects users' geographical distribution data to make report data more accurate. This permission is optional. |
| 3 | ACCESS_FINE_LOCATION | | |
| 4 | WRITE_EXTERNAL STORAGE | U-Push message push service | Used to save device-related information to ensure the accuracy of the unique identification of the device, so as to accurately push messages to the target device. |
| | | U-Share social sharing | To be used when large images/multiple images or large files are shared between different apps. |
| 5 | READ_EXTERNAL_STORAGE | U-Share social sharing | To be used when large images/multiple images or large files are shared between different apps. |

Use of personal information permissions

Note:

1. Only the use of personal information permissions is disclosed in the aforesaid form. For details of the scope of personal information permissions, please refer to the Network Security Practice Guidelines - Application and Use Specifications for Personal-Information-Related System Permissions in Mobile Internet Applications issued by the National Information Security Standardization Technical Committee.

2. It should be specially noted that the precise location permission (ACCESS_FINE_LOCATION) has been removed in the latest versions of various SDKs, and the WRITE_EXTERNAL_STORAGE permission has also been removed in U-Push V6.4.0 and above. We recommend that you upgrade to the latest SDK as soon as possible.

Ø Other non-personal information data

In addition to the aforesaid personal information, the SDK service will collect the following non-personal data according to the different dimensions provided by the service: SDK/API/JS code version, browser, Internet service provider, platform, timestamp, application version, application distribution channel, device model, sensor parameters, terminal manufacturer, the operating system version of terminal device, language location, time zone and network status (WiFi, etc.), hard disk, CPU, battery use, etc.

(3) Visit and browse the [Umeng+] website

During your use of our services, in order to identify abnormal account status, abnormal device status, and understand and/or optimize product adaptability, we may automatically collect your usage and store it as web log information. When you use the [Umeng+] service or visit the websites involving the [Umeng+] platform, [Umeng+] will automatically receive and record the information on your browser and computer, including but not limited to your data such as IP address, browser type, language used, date and time of access, hardware and software feature information, and web page records that you require. If you visit a mobile webpage and use the [Umeng+] service, [Umeng+] may read information related to your location and mobile device, including but not limited to device model, device identification code, operating system, resolution, telecom operator, etc.

(4) Others

In addition to the aforesaid information, we may also collect your other information reasonably necessary to provide services and improve service quality, including the relevant information that you provide when you contact our customer service team, and the reply information that you send to us when you participate in the questionnaire, and the relevant information that we collect when you interact with [Umeng+] affiliates and [Umeng+] partners. At the same time, in order to improve the security of your use of the [Umeng+] service, and to more accurately prevent phishing website fraud and Trojan horse viruses, we may judge and determine whether your account is at risk based on some of your network use habits and the information about your commonly used software, and may record some URLs that we deem risky. Please be noted that individual 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 use it in combination with personal information, then such non-personal information will be deemed as personal information during the combined use, unless authorized by you or otherwise provided by laws and regulations, and we will anonymize and de-identify such information.

3. How we use the information that we collect

Based on the data legally collected by us through the [Umeng+] data service, we will process the crowd data and build a data intelligence platform in accordance with the industry-leading data security technologies such as de-identification, anonymization and pseudonymization. Such platform provides you with data services by means of data plus intelligent engine services. For example, it can classify end users with common characteristics and preferences, and provide crow grouping management and crowd labeling services to help you optimize delivery and improve marketing effects. We guarantee not to leak or violate the privacy of your end users.

On the premise that a specific individual cannot be re-identified after being processed through security technologies such as strict de-identification, we analyze and mine the collected data through an algorithmic model, without giving further notice to you and obtaining your consent. We will take technical measures and other necessary measures to process such information, to conduct aggregated and anonymous group analysis and research in the form of unidentifiable or reversed personal information, and may also use machine learning technology or model algorithm training to provide relevant institutions with forecasting services in anti-fraud , risk control audit or other reasonable scenarios based on the authorization between users and credit reporting agencies (such as Baihang Credit, Park Road Credit), licensed financial institutions or other institutions. Under no circumstance will we disclose, transfer, impart or license any personal information to any third party for use without the authorization of the users.

4. How you use Umeng+SDK services in compliance with applicable laws and regulations

In order to guarantee the compliance of your app with applicable laws and regulations, you must take the following three steps to ensure that your use of Umeng+SDK services complies with current laws, regulations or regulatory requirements:

1. Please be sure that you have upgraded the Umeng+SDK to the latest version that meets the new regulatory regulations. Various latest SDK versions can be downloaded at the following link: https://developer.umeng.com/sdk

2. Please be sure to inform users to use the Umeng SDK in the Privacy Policy. The reference terms are as follows:

Name of Used SDK: Umeng SDK

Service Type: Please fill out this item according to the SDK function, such as statistical analysis

Type of Personal Information Collected: device information (IMEI/MAC/Android ID/IDFA/OpenUDID/GUID/SIM card IMSI/geographical location, etc.)

Privacy Policy Link: https://www.umeng.com/page/policy

In order to ensure the legal compliance of your app, you must ensure that you use Umeng+SDK services in accordance with current laws, regulations or regulatory requirements, and you must complete the following three steps:

1. Please make sure that you have upgraded the Umeng+SDK to the latest version that meets the new regulatory regulations. Various latest SDK download links: https://developer.umeng.com/sdk

2. Please be sure to inform users of the use of Umeng SDK in the "Privacy Policy". The reference terms are as follows:

Use SDK name: Umeng SDK

Service Type: Please fill in according to the SDK function, such as statistical analysis

Type of personal information collected: device information (IMEI/MAC/Android ID/IDFA/OpenUDID/GUID/SIM card IMSI/geographical location, etc.)

Privacy Policy Link: https://www.umeng.com/page/policy

3. Please be sure to perform delayed initialization configuration to ensure that the user authorizes the Privacy Policy before initializing the Umeng SDK.

Various SDK delay initialization link: https://developer.umeng.com/docs/147377/detail/184328

Please be sure to use the Umeng+SDK service in compliance with applicable laws and regulations based on the aforesaid prompts. If you fail to do so, the risks arising therefrom and losses sustained by Umeng+ as a result shall be borne by you.

II. How we use cookies and web Beacons

In order to make you obtain easier access experience, when you visit the [Umeng+] platform or use the services provided by [Umeng+], we may identify you through small data files so as to help you save the steps of repeatedly enter registration information, or help you determine the security of your account. These data files may be cookies, flash cookies, or other local storage provided by your browser or associated application (hereinafter collectively referred to as "Cookies").

Please understand that some of our services can only be achieved through the use of Cookies. If your browser or browser add-ons allow, you can activate your browser's settings options, select privacy settings, check "Do Not Track", or disable Cookies, so that your data will not be tracked by us. Web pages often contain some electronic images (called "Single-pixel GIF Files" or "Web Beacon"), and the use of Web Beacon can help the website count users who browse the web or access certain cookies. We will collect the information of your web browsing activities through the Web Beacon, such as the address of the webpage that you visit, the address of the referring page

you previously visited, the time you stay on the webpage, your browsing environment, display settings, etc.

III. How we share, transfer, and disclose to the public the personal information of you and your end users

1. Sharing

We are obligated to keep your information confidential and will not sell or lease to any third party the information of you and your end users for achieving such third party' s marketing or illegal purposes. We will not share the personal information of your end users with any third party except where:

(1)We have obtained prior consent or authorization from the subject of personal information rights.

(2)Such sharing is conducted in accordance with the provisions of laws and regulations or the requirements of administrative or judicial bodies.

(3) If your end user is an eligible intellectual property complainant and has filed a complaint, you shall disclose it to the respondent at the request of the respondent, so that both parties can deal with possible disputes over rights.

(4) We cannot provide services or deal with controversies or disputes between your end users and others unless we can share the information of your end users.

(5) Sharing with advertisers, media and other partners. We will cooperate with such partners to use the handled and processed desensitization data in various forms for various purposes, including optimizing advertising delivery and improving marketing effects. We will provide such partners with data about targeting crowd strategies or advertising effects of the advertiser's ads, but will not provide any personal identity information about your end users. We sign strict non-disclosure agreements with our partners sharing such information, requiring them to process and use data through taking strict data security measures in accordance with our Privacy Policy.

(6) We share your personal information with [Umeng+] affiliates subject to applicable laws and regulations.

2. Transfer

We will not transfer the personal information of your end users to any third party except where:

(1) We have obtained the consent of your end users.

(2) In case of merger, acquisition or liquidation upon bankruptcy involving the transfer of personal information, we will require new companies and organizations holding the personal information of your end users to continue to be bound by this Privacy Policy, otherwise we will

require such companies or organization to seek authorization and consent from your end users once again.

3. Public disclosure

We will only publicly disclose the personal information of your end users in the following circumstances:

(1) We have obtained the express consent of you or your end users;

(2) Disclosure according to law: We may publicly disclose the personal information of you or your end users as required by law, legal proceedings, lawsuits or competent government authorities.

(3) In an emergency, such public disclosure is reasonably judged to protect the important legitimate rights and interests of us, our customers, end users or others.

IV. How we protect the personal information of you and your end users

In order to protect the security of the information of you and your end users, we will try our best to take reasonable security measures in terms of physical, electronic and management aspects to protect your information in accordance with general industry standards, and make our best reasonable efforts to prevent the information of you and your end users from being leaked, damaged or lost. The data exchanged between your browser and the server is protected by SSL protocol encryption; we provide safe browsing on the website through the HTTPS protocol; we will use encryption technology to improve the security of personal information; we will use trusted protection mechanisms to prevent personal information from being maliciously attacked; we will deploy the access control mechanisms to make efforts to ensure that only authorized personnel can access personal information; and we will have security and privacy protection training courses to enhance employees' awareness of the importance of protecting personal information.

We have an industry-leading data security management system with the data as the core and around the life cycle of the data, and establish a compliance system in accordance with relevant laws and regulations, various standards, etc., and enhance the security of the whole system from organizational construction, system design, personnel management, product technology, and other aspects in multiple dimensions.

The information collected by us is saved in a secure operating environment that is not open to the public. To prevent unauthorized access to your information, we store it on a server protected by firewalls and possibly encrypted. However, no system is absolutely secure, please understand that there is no "perfect security measure" on the information network. Even we have made best efforts, it may be possible that we can eradicate unlawful access to the personal information of you and your end users. Furthermore, we may be blinded by unreliable, misleading or illegal information because of our inability to judge whether the representations by others are true or not.

In case of a personal information security incident, we will, as required by applicable laws and regulations, inform you or your end users of the followings: the basic situation and possible impact

of the security incident, the disposal measures we have taken or will take, recommendations for you and your end users to conduct self-prevention and mitigation of risk, remedies available to you and your end users, and so on. We will notify you and your end users of the relevant situation of such incident by email, letter, telephone, push notice, etc. When it is difficult to inform the subjects of personal information one by one, we will publish an announcement in a reasonable and effective way. At the same time, we will also report on the handling of personal information security incidents as required by the relevant regulatory authorities.

We will take reasonable and practicable measures to try to avoid collecting irrelevant personal information. We will only retain the personal information of you and your end users during the period required for achieving the purposes described in this Policy, unless such retention is mandatorily required by law. Our criteria for judging the aforesaid period include the following:

1. Completing the service purpose related to you, maintaining the corresponding service and business records, and responding to your possible business needs;

2. Guaranteeing the security and quality of the services that we provide for you;

3. Whether you give consent to a longer retention period;

4. Whether there is any other special agreement on the retention period.

After your personal information is kept beyond the retention period, we will delete or anonymize your personal information as required by applicable laws.

V. How we manage the personal information of you and your end users

You may access and manage your information as follows:

1.Query, correct and supplement your information. We will endeavour to enable you to review, correct or supplement the information you have stored with us. For review, correction or supplement purpose, please visit our website and log in to your account to so operate. If the exercise of a certain right cannot be performed on the account page, you can contact us through the contact information in this Policy, and we will assist you in conducting the corresponding operation.

2. Account de-registration and deletion of your personal information.

If you do not want to continue to use our products, you may submit the application for de-registration of your account to us through the work order system (the specific path is to log in to your account, click on the customer service work order, and select legal issue consultation and other types of rights consultation so as to give work order feedback), and we will usually respond to your application needs within 15 working days, provided that for the security of your account, we will identify your identity, verify and process your application, and we will require you to submit sufficient and valid identity information. After the account is de-registered, we will no longer provide you with services. If you want us to delete your personal information, you may also submit to us an application for the deletion of your personal information.

3. Obtaining a copy of personal information.

You have the right to obtain a copy of your basic personal data through sending us a request. In case of technical feasibility, such as data interface matching, we may also directly transmit a copy of your personal information to a third party designated by you upon your request.

If your end users need to obtain a copy of their personal information, they can initiate a request to us, and we will return the copy of their personal information after we verify their identity.

VI. How do we process the information of minors

We highly value the protection of personal information of minors. If your application is developed for minors, please take necessary measures to ensure that the registration and use thereof by your end users have obtained the consent of their guardians. At the same time, you shall fulfill the corresponding disclosure obligations in your privacy policy. Please be noted that, as an app designed for minors, you also need to comply with the review standards and guidelines for the apps for minors in the app market, so as not to affect the launching or normal operation of your app.

Subject to the existing technology and business model, it is difficult for us to actively identify the information of minors. If the guardian of a minor finds that the personal information of the minor has been collected without authorization, the relevant guardian may notify us to delete it. If we find the aforesaid circumstance on our own, we will also take the initiative to delete such personal information.

VII. Scope of application of SDK services and globalization statement

Our SDK provides services for developers in the territory of China, and we will store your data in the territory of China. In order to prevent you from violating local regulatory requirements due to your ignorance of the relevant regulations and policies of the country or region where your end users are located on data protection, we strongly recommend that you only use the [Umeng+] service on the mainland of the People's Republic of China. If you apply for using the [Umeng+] service outside the mainland of the People's Republic of China, the information and data about your end users processed by us as entrusted will be transmitted to a server in Singapore or Germany. You may be suspected of violating the relevant provisions of the current Chinese laws and regulations on cross-border transmission, and you shall bear the corresponding risks and consequences arising therefrom. We strongly recommend that you consult local professionals to ensure that such cross-border transmission complies with local regulatory requirements, especially when the cross-border transmission involves countries or regions such as Russia, India, the European Union, the United States, etc., please pay attention to the relevant regulations of such countries and regions on the supervision and administration of personal information. You need to bear all the risks that may arise independently. If [Umeng+] sustains any losses as a result, you are liable for damages in full to us. If you provide services in the European Union, our business may require us to transfer the personal data of your end users to countries or regions other than the European Union. The aforesaid countries or regions may offer a different level of data protection than EU countries. As the entrusted processor of the personal data of your end users,

we will take appropriate measures to ensure our performance of the confidentiality obligations and to ensure the enforcement of the measures such as standard contract terms.

VIII. How to update this Privacy Policy

We may adjust or change this Privacy Policy as appropriate. Any updates to this Privacy Policy will be posted on the [Umeng+] website by marking the update time. Unless otherwise mandatorily prescribed by applicable laws, regulations or regulatory requirements, the adjusted or changed content will take effect 7 days of notification or announcement. We shall not restrict your rights hereunder without your express consent. For material changes, we will also provide you with more prominent notice (including notifying you through public notice on the website or the homepage of the client or even provide you with pop-up prompts).

Material Changes referred to herein include, but are not limited to:

1. Our service model has undergone a material change, such as the purpose of processing user information, the method for the use of user information, etc.

2. We have undergone a material change in terms of control, organizational structure, etc., such as the change in owners resulting from business adjustments, merger and acquisition upon bankruptcy, etc.

3. The main objects of personal information sharing, transfer or public disclosure have changed.

4. There are material changes in your rights to participate in the processing of personal information and the manner in which such rights are exercised;

5. There are changes to our responsible department in charge of the security of user information, contact information and complaint channels.

6. The personal information security impact assessment report indicates that there is a high risk.

IX. How to contact us

If you have any questions, suggestions or complaints about this Privacy Policy, please raise them through the work order system (the specific path is to log in to your account, click on the customer service work order, and select legal consultation so as to give work order feedback). We will respond within 15 working days of receipt of an inquiry.

We have also set up a dedicated department for personal information protection, you can contact it through (Umeng_Legal@service.umeng.com), the work order system or the place located at 30/F, Jinhui Building, Building 6, Wangjing East Park, Chaoyang District, Beijing, China.

If you are not satisfied with our response, especially if you believe that our processing of personal information has prejudiced your legitimate rights and interests, you may also seek a

solution by bringing a suit to a court of competent jurisdiction of the place where the defendant is domiciled.