Privacy Policy

Updated: Feb 27, 2024

We appreciate your trust in our products and services. In order to provide the Rainflower mobile application, website, mobile application, and through the services we provide (collectively, the website, application, and services referred to as our "App"), and continue to make them better, the company Zephyr Technologies, LLC. (further referred to as “the Company”, "we," "us," or "our") collects information from you. “You” refers to you as a user or visitor of the App (referred to as “You” or “User”).

This Privacy Policy explains how the Company collects, stores, uses, transfers, and discloses your information.

From time to time, we may revise this Privacy Policy. Any changes to this Privacy Policy will be effective immediately on posting the updated Privacy Policy unless otherwise stated or as required by applicable law (for example, a different form of notice and your opt-in or opt-out consent, etc.). By continuing to use our App, you agree to the revised Privacy Policy to the fullest extent permitted by applicable law.

Information to be Collected and Method of Collection

Personal information items to be collected by the Company are as follows:

Personal Data (or Data)

The Company may collect the information directly provided by the users.

1. Webpage contact service

- Email address and message contents
- Method of collection: webpage

2. Online payment service

- Name, address, telephone number, and email address
- Payment information including account number and card number
- Information of bid, purchase and sales
- Method of collection: mobile application

The Company may collect information in the course that the users use the service provided by the Company.

1. Equipment Information

- Equipment identifier, operation system, hardware version, equipment set-up and telephone number.
- Method of collection: mobile application

2. Log information

- Log data, use time, App page information.
- Method of collection: mobile application

The Company agrees that it will obtain consent from the users, if the Company desires to use the information other than those expressly stated in this Policy.

The Company uses the collected information of users for app analytics, to improve existing services and help future development of new services

Sharing collected information

Except for the following cases, the Company will not share personal information with a 3rd party:

- when the Company shares the information with its affiliates, partners and service providers
- when the users consent the sharing in advance
- when the sharing is required by the laws
    - if required to be disclosed by the laws and regulations; or
    - if required to be disclosed by the investigative agencies for detecting crimes in accordance with the procedure and method as prescribed in the laws and regulations

Period for retention and use of personal information

In principle, the Company destructs personal information of users without delay when: the purpose of its collection and use has been achieved; the legal or management needs are satisfied; or users request: Provided that, if it is required to retain the information by relevant laws and regulations, the Company will retain member information for certain period as designated by relevant laws and regulations.

- Record regarding contract or withdrawal of subscription: 5 years (The Act on Consumer Protection in Electronic Commerce)
- Record on payment and supply of goods: 5 years (The Act on Consumer Protection in Electronic Commerce)

- Record on consumer complaint or dispute treatment: 3 years (The Act on Consumer Protection in Electronic Commerce)
- Record on collection/process, and use of credit information: 3 years (The Act on Use and Protection of Credit Information)
- Record on sign/advertisement: 6 months(The Act on Consumer Protection in Electronic Commerce)
    - Log record of users such as internet/data detecting the place of user connection: 3 months (The Protection of Communications Secrets Act)
- Other data for checking communication facts: 12 months (The Protection of Communications Secrets Act)

Procedure and method of destruction of personal information

In principle, the Company destructs the information immediately after the purposes of its collection and use have been achieved without delay: Provided that, if any information is to be retained as required by relevant laws and regulations, the Company retain it for the period as required by those laws and regulations before destruction and, in such event, the personal information which is stored and managed separately will never be used for other purposes. The Company destructs: hard copies of personal information by shredding with a pulverizer or incinerating it; and deletes personal information stored in the form of electric file by using technological methods making that information not restored.

Cookies and Similar Technologies

The Company and its service providers may use first and third party Cookies and Other Tracking Technologies, including web beacons, to manage our Sites and our services and collect analytics about how you use them. The Company and its service providers may collect information about whether you open or click any links in the knowledge, research or event communications that we send to you. The information provided throughout this Privacy Policy about cookies also applies to these other tracking technologies. Please refer to our Cookie Policy for more details regarding our use of Cookies and Other Tracking Technologies.
The users have an option for cookie installation. So, they may either allow all cookies by setting options in the web browser, make each cookie checked whenever it is saved, or refuses all cookies to be saved: Provided that, if the user rejects the installation of cookies, it may be difficult for that user to use the parts of services provided by the Company.

Users’ Right to Access

The users or their legal representatives, as main agents of the information, may exercise the following options regarding the collection, use and sharing of personal information by the Company:

- exercise right to access to personal information;
- make corrections or deletions;
- make temporary suspension of treatment of personal information; or
- request the withdrawal of their consent provided before

If, in order to exercise the above options, you, as an user, use the menu of 'amendment of member information of webpage or contact the Company by using representative telephone or sending a document or e-mails, or using telephone to the responsible department (or person in charge of management of personal information), the Company will take measures without delay: Provided that the Company may reject the request of you only to the extent that there exists either proper cause as prescribed in the laws or equivalent cause.

Security

The Company regards the security of personal information of users as very important. The Company constructs the following security measures to protect the users' personal information from any unauthorized access, release, use or modification by the Personal Information protection Act.

- Establish and implement an internal privacy management plan. Establish an internal personal information management plan, containing matters in relation to the composition and operation of the privacy organization, such as the designation of privacy personnel, and inspect whether the internal management plan is implemented effectively each year. Provide education and training for staffs treating personal information.
- Actions are undertaken to control access to and restrict the right to access personal information. In order to prevent illegal access to personal information, The Company has established the standards for granting, modifying, and canceling access rights to the personal information processing system, and runs an intrusion prevention system and intrusion detection system. Employees that handle personal information are kept to a minimum, thereby reducing the risk of personal information leakage.
- Actions are taken to store personal information access records and prevent any forgery and tampering. The personal information handler stores and manages access records for the personal information processing system, periodically inspects access records to prevent any misuse, abuse, loss, forgery, and tampering of personal information, and safely stores the relevant access records so that they are not forged , stolen, or lost. Utilize security servers for transmitting encryption of personal information. Take measures of encryption for confidential information.
- The Company installs and renews security programs for personal information. The Company frequently backs up data to offset risk of any damage to personal information, and uses the latest antivirus software to prevent leakage or damage of users' personal information.

- The Company enforces physical actions to keep personal information safe. In order to prevent leakage or damage of members' personal information caused by hacking or computer viruses, The Company installs systems in areas with restricted access from the outside, and establishes and operates access control procedures.

Mobile Application Privacy Policy

What information does the Application obtain and how is it used?

The Application does not provide an option to create an account therefore, the Company does not store nor have access to your entries and data. Your data are stored only locally on your device and all calculations are done on your device as well. The Company can obtain your email address when you request support via email or customer support contact form. The Company only uses your email only to contact you to provide support, feedback or important information.

Analytics

The application does NOT collect any usage or crash reporting data without your consent.
If you've agreed to data collection, the application collects some usage data that are essential for us to deliver our services, to understand your needs, and to improve our services. Such as app launches, taps, clicks, scrolling information, in-app purchases, screen visits, session durations, or other information about how you interact with our app. This data is anonymized and aggregated from all users who gave us collection consent. If you've agreed to data collection, the application also collects crashes and performance reports so the Company can improve the stability and performance of our app.
The application does NOT collect any user-generated content. Such as your name, surname, email, or anything you type within the app.

Media

You can optionally attach photos, videos, or audio to your entry. Your media are stored locally on your phone in our app's storage. The Company does not have access to your media. Your media are never sent with the analytics data.

Android

The Company use the following third-party services for our Android app:
Google Analytics for Firebase (Google Inc.)

- This service helps us to collect and analyze usage data in order to understand usage patterns and to improve our Android app.
- Data collected: various usage and device data such as cookies, unique device identifiers, Android Advertising ID, Firebase installation IDs, Analytics App Instance IDs, usage data, anonymized IP addresses, session durations, device models, operating systems, geography, in-app purchases, first launches, app opens, app updates
- Data retention: 2 months

Firebase Crashlytics (Google Inc.)

- This service helps us to identify crashes and errors in our app. It helps us to improve the reliability and stability of our Android app.
- Data collected: Crashlytics Installation UUIDs, crash traces, device models, geography, operating systems
- Data retention: 90 days

iOS

The Company use the following third-party services for our iOS app:
Google Analytics for Firebase (Google Inc.)

- This service helps us to collect and analyze usage data in order to understand usage patterns and to improve our iOS app.
- Data collected: various usage data, Firebase installation IDs, Analytics App Instance IDs, anonymized IP addresses, session durations, device models, operating systems, geography, in -app purchases, first launches, app opens, app updates
- Data retention: 2 months

Firebase Crashlytics (Google Inc.)

- This service helps us to identify crashes and errors in our app. It helps us to improve the reliability and stability of our iOS app.
- Data collected: Crashlytics Installation UUIDs, crash traces, device models, geography, operating systems
- Data retention: 90 days

Advertising

Advertising helps us to keep our app free. The premium version of our app does not serve any ads. The premium version also does not initialize or call any AdMob method.
Ad content is NOT based on your entries or notes. The Company does not share your data with the ads providers.
The iOS version of our app does not show third party ads. The free version of our Android app uses the following service:
AdMob (AdMob Google Inc.)
The Company use AdMob to display ad banners and other advertisements possibly based on your interests. AdMob uses cookies to identify users and they may use the behavioral retargeting technique, ie displaying ads tailored to your interests and behavior, including those detected outside our app. For example, if you've previously visited e-shop selling shoes you might see more ads promoting shoes or shoe shops.
Google's advertising requirements can be summed up by Google's Advertising Principles https://www.google.com/policies/privacy/partners/. They are put in place to provide a positive experience for users.
Personal data collected: Cookies, Google Advertiser ID
If you do not want to see personalized ads based on your interests you might opt-out by using this link. Please note that you will see the same amount of ads but the ads will be less relevant to you.