

PRIVACY POLICY - RABIT
DECEMBER/2021

We at **BLU APPS** – a company from United States having its registered office at 7345 W SAND LAKE ROAD, STE 210 OFFICE 8073, ORLANDO, FL 32819, registered with the Trade and Companies Registry of United States under number 38-4180245 (henceforth “**BLU**”) - understand the importance of your privacy and are committed to protect your rights as a data subject. You have the right to know how we collect, use, disclose and process your personal information.

In order to use our services through **RABIT** (or, the “App”), you will need to share some personal information with us. Therefore, we have created this Privacy Policy to explain in plain English how we operate by the best international practices regarding data protection and cybersecurity.

We will clarify how we take care of your personal data through the following topics:

- 1. Key Definitions**
- 2. Our role as a Data Controller**
- 3. What Data We May Collect From You**
- 4. Purposes and Legal Basis for Personal Data Processing**
- 5. Retention of Personal Data**
- 6. How We Protect Personal Data**
- 7. Sharing of Personal Data**
- 8. Rights of the Data Subject**
- 9. Updates to this Privacy Policy**
- 10. Questions and Contact Information**
- 11. Dispute Resolution**

Specifically, this Policy applies to **BLU**’s the collection, use, storage, transfer or other processing activities of information associated with our mobile application **RABIT** in order to offer an online habit tracker solution.

We clarify that this Policy is a complementary document to **RABIT’s Terms and Conditions of Use** and, therefore, it must be interpreted in conjunction with the aforementioned document, which describes the rules of use and the responsibilities of Users in the use of **RABIT**. Thus, if you have registered to use **RABIT**’s services, this Privacy Policy applies to your personal data processed on that occasion. The

use of **RABIT** implies acceptance of this Privacy. If you do not agree with this document, we kindly ask that you do not provide us with your personal data and do not use our app and services in general.

For readability, we have divided this Policy into two columns — our official policy, which is legally binding; and a "simple" version, which is not legally binding.

1. Key definitions:

For your better understanding of this Policy, we have adopted the following definitions:

- I. **Personal Data:** any information relating to an identified or identifiable natural person. An identified/identifiable natural person is one who can be identified, directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- II. **Special categories of personal data:** personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and genetic data, biometric data processed for the purpose of uniquely identifying a natural person, or data concerning health, a natural person's sex life or sexual orientation.
- III. **Data subject:** any living individual who is the subject of personal data held by an organization.
- IV. **Processing of data:** any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
- V. **Data controller:** natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
- VI. **Data processor:** a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
- VII. **Subprocessor:** a natural or legal person appointed by or on behalf of Processor to process Personal Data on its behalf.
- VIII. **Data Protection Officer ("DPO"):** natural or legal person appointed by the Controllers and Processors to act as a communication channel between the Controller, data subjects, the Data Protection Authorities and third parties in general.
- IX. **User:** a natural person who shares its personal information with us while using **RABIT**.

2. Our role as a Data Controller

In other words,

The Data Controller has the decision-making power and defines the purposes of personal data processing. Hence, **BLU** is the Data Controller of your Personal Data collected while using **RABIT**.

3. What Data We May Collect from You

We may collect the following personal data from our Users in order to provide our services:

- First and last name
- Nickname
- E-mail
- Birthday
- Location
- Time zone
- Photos uploaded
- Personal information related to your habits

Our Users may voluntarily provide additional personal data when contacting us through our support channels.

Please, be aware that **RABIT**'s functionalities depend on integration with third party services, applications and software, therefore, we cannot be held responsible for any breaches of the terms of use and/or regulations of these third parties or for any treatment of data carried out by these third parties.

3.1. Sensitive Personal Data

We do not intentionally collect sensitive personal data. However, it is possible that you choose to voluntarily share sensitive personal data, such as health appointments and habits, for example. On those occasions, sharing personal data implies acceptance of the conditions contained in this Policy, granting your free and unambiguous consent to the processing of your sensitive personal data for the purposes set forth herein.

BLU is the Data Controller of your Personal Data when you use **RABIT**.

In other words,

When you use **RABIT**, we collect your name, nickname, e-mail, birthday, location, time zone and uploaded photos. Additional personal data may be voluntarily shared by our Users through our support channels. Be aware that our application depends on software developed by third parties, but we cannot be held responsible for non-compliant practices taken by those third parties.

In other words,

We do not collect sensitive data intentionally, but the User may share this kind of information voluntarily. In that case, the user automatically consents to **RABIT**'s Terms and Policy.

3.2. Information Relating to Children

RABIT is not directed to children under age 13 and we do not knowingly collect Personal Information from children under the age of 13. Children under 13 should not provide their Personal Information to us through our Platform, to support channel, or in writing. If we identify that Personal Information belonging to anyone under the age of 13 is stored by us without any parental consent, we may immediately delete such information and refrain from using it for any purpose.

4. Purposes and legitimate basis for Personal Data Processing

The processing of personal data carried out by **RABIT** will always have the goal of achieving legitimate, specific, explicit and duly informed purposes based on lawful bases. We may process your personal information in order to:

- Provide our services.
- Generate a personal profile about you to make future visits to the App more personalized.
- Monitor and analyze usage and trends to improve your experience with the App.
- Notify you of updates to the App.
- Request feedback and contact you about your use of the App.
- To improve our product.

We will also require you to link either your iTunes Account, ApplePay Account or Google Play Account with our App if you wish to purchase one of our Premium subscriptions. However, this does not give us access to your credit card or banking information, as it is only needed to process your purchases/subscriptions.

We may use your personal data to register, identify and communicate with Users and to enable functionalities

In other words,

We may delete any personal data of persons under the age of 13 that is identified in our database without authorization from the respective legal guardian.

In other words,

We process your personal data to fulfill the following purposes:

- (a) Ensure the use of **RABIT** in a safe and personalized way.
- (b) Improve your experience on the App and ensure the security of the services.
- (c) So we can communicate with you, whether for informational or commercial purposes;
- (d) Customize and communicate offers and services.
- (e) Comply with legal and regulatory obligations, credit protection or for the regular exercise of rights in judicial, administrative or arbitration proceedings.

We take care of your data in accordance with the following bases:

- (a) to perform a contract or during preliminary procedures for a contract.
- (b) there is a legitimate interest, whether ours, you or a third party.
- (c) we are in our regular exercise of rights during any dispute.

of the App, which may include processing payments, solving problems and developing our operating system, among other treatments directly linked to our services. Likewise, for security purposes, we may use your personal data to prevent frauds through our App.

(d) to comply with legal or regulatory obligations.

(e) for credit protection.

Occasionally, personal data may be processed to meet our legitimate interests, such as to promote our services. We may also use your personal information to identify your profile, track your habits, customize offers and to create strategies related to **RABIT** or use your personal data to send you information about **RABIT** news and offers.

We may also use your personal data for auditing purposes, promotions, communication with Users, analysis for service improvement, research, development, statistics and identification of trends inherent to the use of our services. When possible, this analysis will be stored in an anonymized form that cannot be traced to you or any other individual, always preserving the rights and guarantees of the data subjects.

We reserve the right to process your personal data to comply with any legal or regulatory obligation, protection of credit, or for the exercise of our vested rights in judicial, administrative or arbitration proceedings, for the entire period necessary to do so.

We may eventually process your personal data for purposes other than those described above. In that case, you will be notified in advance and, if necessary, in order to consent to such operation.

We process personal data always respecting the principles of adequacy and necessity.

We take care of your data in accordance with the following bases:

- a) For the performance of services, products and other contracts or preliminary.
- b) In pursuit of the legitimate interest of the Data Controller or third parties, e.g. in case of commercial communications, promotion of our activities and products and to improve the services provided by **BLU**.
- c) For the regular exercise of rights in judicial, administrative or arbitration proceedings, e.g. in cases of storage of your information for the periods provided for by law.
- d) Compliance with any legal or regulatory obligation.
- e) For protection of credit, e.g., in cases of data processing for security and improvement of services, which includes protection against fraud in the use of **RABIT**.

5. Retention of Personal Data

The Personal Data handled by us will be deleted when it is no longer needed for the purposes for which it was collected and in accordance with the legal deadlines

The Personal Data collected and controlled by **RABIT** is stored by Google Drive. After the established period and legal requirement, the personal data will be deleted using safe disposal methods or will be submitted to an anonymization process.

If requested by the data subject, the data may be deleted before the deadline internally established. However, the data requested to be deleted may need to be retained by **BLU** due to an exercise of rights, legal compliance, court order, fraud prevention, credit protection and other legitimate interests - and if this is the case, you will be notified and we will provide the reasoning.

In other words,

We store your information through Google Drive. We will safely delete this information as soon as we no longer need it. You can request this deletion to be done before that, but we may still need this data for some reason (in this case, we will inform you about the impossibility of deletion and why). In addition, we may also delete your information at any time.

Finally, it is important to emphasize that, to the extent permitted or required by law, we may delete your personal information at any time for our own criteria of non-compliance, not having, on our part, the duty to retain it.

6. How We Protect Personal Data

We use systems and procedures that meet reasonable standards of precaution and care, considering the technically and economically reasonable possibilities of technology applicable to the internet - such as the use of firewall and data encryption - to protect your personal data against unauthorized access, among other measures.

We will not intentionally disclose your personal data and we are not responsible for the actions of Users, including cases of negligence that may expose personal data. For this reason, we recommend the use of antivirus, information security procedures and other measures necessary to maintain the security of your personal data.

You acknowledge that there is no possibility of total security in the worldwide computer network, especially regarding criminal intrusions into secure data networks by hackers, among other scenarios of security incidents. Despite this, we are committed to taking reasonable steps to protect and prevent unauthorized access to your data. However, we cannot be sanctioned for the acts of those who may obtain unauthorized access to your data.

We make no warranty – either express or implied - that we will prevent unauthorized access to your personal data.

In the event of any security incidents that lead to the exposure or unauthorized access to your personal data,

In other words,

We protect your personal data both with technology (through firewalls and encryption, for example) and with the training of our employees.

However, you acknowledge that it is impossible for us to guarantee total security on the world wide web. We will take all possible security measures to prevent a security incident, but if it does happen, we cannot be sanctioned for unauthorized access to your personal data. Furthermore, if a security incident occur, you will be promptly notified and we will comply with all legal and regulatory obligations.

we will publish an informational notice and/or send you an email informing the circumstances of the occurrence.

7. Sharing of Personal Data

In order to fulfill the purposes described in this Privacy Policy, we may share your personal data with other data processing agents. The sharing of personal data will always be carried out in compliance with the principles of good faith, purpose limitation, lawfulness, fairness, and transparency, data minimization, accuracy, storage limitation, integrity, confidentiality, accountability, security, prevention and non-discrimination.

We may internally share your personal data with people whose role within **BLU** requires access to it. The usage of Operators and/or third-party services may also lead to the sharing of your personal data, such as the use of cloud storage services and payment intermediation.

During data processing, we may share your personal data in a different manner from those described above, if we have your express consent to do so.

7.1. Judicial or Administrative Authorities

The personal data processed, and the activities recorded by us may be shared with competent judicial or administrative authorities, whenever there is a legal determination, a request by an administrative authority or a court order to comply with the law, governmental process, legal process or regulation. We also may use your personal data as a defense against legal claims or assert legal rights; or to prevent, detect or investigate illegal activity, fraud, abuse, violation to our terms, or threats to the security of our services or the safety of any person.

In other words,

We may share your personal data in order to fulfill the processing purposes indicated in this Policy. This sharing can be done: (i) with our Operators; (ii) with authorities, when there is a legal obligation, request for administrative authority or court order; (iii) internationally, to enable the use of the platform; (iv) internally with our employees; (v) with third parties to improve your experience while using the platform. We may occasionally share your data differently, but we will seek your express consent in order to do so.

7.2. International Data Transfer

We may transfer your personal data to countries other than the country in which the data was originally collected for the purposes described in this Privacy Policy. For example, if you are located outside Brazil, we may transfer your personal information to Brazilian territory. The countries to which we transfer personal information may not have the same data protection laws as the country in which you initially provided the information. When we transfer personal information across borders, we consider a variety of requirements that may apply to such transfers.

Any data sharing will always be performed within the limits and purposes of the treatments described in this Policy. Furthermore, international data transfer is possible when using third-party software and/or servers that store data outside the country.

7.3. Sharing of Personal Data with Third Parties

In order to provide our services, the use of data sub processors, business partners and third-party services may lead to the sharing of personal data that we process. Your personal data may be shared with payment providers and service providers that may be used by **RABIT**, such as law firms, accounting firms, etc.

We also may use external service providers to manage our App or social networks and create associated infrastructure, to carry out auditing or to provide legal services.

Among the third-party processors and services that we hire or otherwise use to provide our services, we highlight:

- Google Drive ("cloud" data storage tool);

- Firebase (sending push notifications);
- Firebase (sending emails).

8. Rights of the Data Subject

We respect your rights as a data subject and we guarantee that you can request at any time:

I. Confirmation of data processing: confirmation of the existence of processing of your personal data.

II. Data access: access to your personal data processed by us.

III. Data correction: correction of your incomplete, inaccurate or outdated personal data.

IV. Anonymization, blocking and deletion of data: the anonymization, blocking or deletion of your personal data deemed unnecessary, excessive or treated in breach of the applicable law.

V. Data portability: the portability of personal data to another service or product provider, upon express request, in accordance with the regulations of the national authority, observing commercial and industrial secrets.

VI. Opposition to the processing of data: the interruption of the processing and elimination of your personal data processed with your consent, if you object to the processing, its purpose or the way in which it is being carried out. The treatment will be stopped, and the data eliminated - except in the cases where the treatment was carried out under a legal basis other than consent.

VII. Data sharing information: information regarding which public and private entities we share data with.

VIII. Consent information: information regarding the possibility of not providing certain consents and the consequences of denial.

IX. Withdrawal of consent: you may withdraw your expression of consent.

In other words,

We will guarantee the following rights:

I. Confirm that we are processing your data.

II. Access your data being processed by us.

III. Fix your data.

IV. Require anonymization, block or erase of your data from our database.

V. Take your data to another service provider, in a portable manner.

VI. Demand the interruption of the processing and elimination of your data.

VII. Require information about who we are sharing your data with.

VIII. Require information about what happens if you do not agree with a certain treatment of your data.

IX. withdraw your consent and what will be the consequence of that is the case.

For us to be able to grant your rights, it is necessary that you keep us informed of any changes to your personal data. If we are unable to comply with your request immediately, we will keep you fully informed.

We request that you inform us of any changes to your personal data, so that your data is updated and correctly stored with us. In case of impossibility of immediate adoption of the measures indicated above, we will send a reply to indicate the factual or legal reasons that prevent their immediate adoption.

9. Updates to this Privacy Policy

We reserve the right to edit or update this Policy at any time, in order to guarantee your privacy and commitment to transparency in the processes for collecting and processing your personal data. Modifications may occur when there is a change in the data collected, treatments carried out or purposes, when required by Data Protection Authorities or other competent body, or as a result of questions or suggestions from you.

The new version of the Privacy Policy will take effect immediately upon its posting on the App. If you do not agree with any of the amendments to the Privacy Policy, you must cease using **RABIT**'s services and may request the interruption of the processing of your personal data within the contractual and legally possible and reasonable limits.

In other words,

We may update this Policy later.

10. Questions and Contact Information

If you have any questions about the Privacy Policy or if you want to have more information about the processing of your personal data, you can contact our Data Protection Officer through the email bluebookoficial@gmail.com.