Privacy Policy

Welcome to PersonalGO!

PersonalGO is an Application developed to connect Trainees and Personal Trainers, providing personalized workout tracking. The application enables connections between Trainees and professionals based on their preferences and needs, offering tools for the creation and management of customized training programs. Additionally, PersonalGO allows for detailed recording of workout data, enabling continuous monitoring of each user's individual progress and development.

We dedicate our best efforts to ensure that our website and application ("Application") are the ideal solution for you.

To enable us to improve our Application and provide our services, PersonalGO processes personal data. Recognizing the importance of your privacy, we have prepared this Policy so that you, our User (and the general public), can understand: (i) how we process personal data; (ii) what security measures we apply to keep your data protected and secure; (iii) what your rights are under the Brazilian General Data Protection Law; and (iv) how you can contact us to exercise those rights.

The use of the Application is not intended for children or adolescents. Therefore, do not register or use the Application if you are not at least 18 (eighteen) years old. The registration of minors or individuals with limited legal capacity (including individuals under 18 years of age) must be carried out by their legal guardians.

Key Definitions:
Many of the terms used in this Privacy Policy ("Policy") are provided for under Law No. 13.709/2018, known as the Brazilian General Data Protection Law ("LGPD"). To facilitate your understanding and reading, we present in this glossary the main terms we use.

a. **Application:** The digital interface (software) through which Users access the services and functionalities of the Application. The Application is the means by which Personal Trainers and Trainees interact and use the tools provided by PersonalGO.

b. **Database:** A structured set of data, including personal data, established in one or multiple locations, in electronic or physical format.

c. **Legal Bases:** The legal bases that legitimize, i.e., allow the processing of personal data.

d. **Controller:** A natural or legal person, whether public or private, who is responsible for decisions regarding the processing of personal data. In this case, the Controller of the Personal Data entered into the Application will be the Contracting Party, who holds the license to the Application.

e. **Data Subject:** The natural person to whom the personal data being processed refers.

f. **Personal Data:** Information that identifies a natural person (i.e., an individual), either directly—such as name or CPF number—or indirectly, such as address or financial data.

g. **PersonalGO or Platform:** A digital platform that provides a complete environment for connection and interaction between Personal Trainers and Trainees for the provision of health, wellness, and personalized training services. The Application includes the set of technological tools, systems, and resources available to both Personal Trainers and Trainees, accessible via the mobile Application.

h. **Personal Trainer:** A physical education professional registered in the Application to provide personalized training services to Trainees.

i. **Processor:** A natural or legal person, whether public or private, who processes personal data on behalf of the Controller. In this case, PersonalGO acts as a Processor with respect to the personal data entered by its Users into the Application.

j. **Services:** The services offered by our Application, as described in these Terms of Use.

k. **Sensitive Personal Data:** Data concerning racial or ethnic origin, religious beliefs, political opinions, membership in a union or organization of a religious, philosophical, or political nature, data related to health or sexual life, genetic or biometric data, when linked to a natural person.

l. **Trainees:** A user of the Application who uses the Platform to engage in physical activities, either independently or with the technical support of a Personal Trainer. This term includes both individuals who hire services from professionals on the Platform and those who choose to manage their workout routines autonomously.

m. **Terms of Use:** The document that establishes the rights and obligations related to the use of the Application.

n. **Processing:** Any operation carried out with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, deletion, evaluation or control of information, modification, communication, transfer, dissemination, or extraction.

o. **User:** Any person who registers and uses PersonalGO's services, including Personal Trainers and Trainees.

p. **We/Us:** The legal entity indicated in item 1.1 of these Terms.

If you would like to learn more about the Brazilian General Data Protection Law, you can access it by clicking here. If you have any questions about any concept in this Policy and wish to learn more, you may contact us to clarify any doubts using the contact information provided in the summary table.

1. General terms

1.1 PersonalGO (PERSONALGO - DESENVOLVIMENTO DE SOFTWARE LTDA., a legal entity registered under CNPJ No. 54.249.128/0001-12, with its registered office at Rua Assis Bueno, 46/601, Botafogo, Rio de Janeiro/RJ, ZIP Code: 22280-080) considers the use of personal data to be a matter of utmost importance and seriousness. For this reason, this Policy has been prepared to communicate practices related to the processing of personal data, particularly regarding the collection, use, and processing of information provided by Users through the Application.

1.2 By using the PersonalGO Application, the User authorizes the processing of personal data and agrees to be bound to PersonalGO. If you do not accept the practices and policies described in this document, you will not be permitted to use the Application.

1.3 PersonalGO operates in accordance with Brazilian law, complying, including but not limited to, the provisions of Law No. 12.965/2014 ("Marco Civil da Internet"), Law No. 13.709/2018, and any other applicable regulations that may be enacted.

1.4 In case of questions or suggestions regarding the Privacy Policy of the Application, the User may contact the Data Protection Officer ("DPO") at the email address: gabriel.delarocha@personalgo.app.

1.5 This Policy describes which personal data may be processed from Users while using the Application's services, how such information may be used, and the precautions taken to prevent unauthorized access or use of such information.

2. Personal Data and Sensitive Personal Data Processed

2.1 PersonalGO may process the following information and/or personal data and sensitive personal data of Trainees:

a) Email address;
b) Name;
c) Phone number;
d) Date of birth;
e) Photo;
f) Gender;
g) Additional health information, such as diagnosed medical conditions, weight, body fat percentage, and height; and
h) Body images (temporary storage).

2.2 PersonalGO may process the following optional information and/or personal data of Personal Trainers:

a) Email address;
b) Name;
c) Phone number;
d) Date of birth;
e) Official personal identification number;
f) Professional qualification information (valid registration with a professional council, certificates or proof of training related to the activity, as well as any other documents required to demonstrate technical qualification);
g) Professional profile information (years of experience, areas of specialization, service conditions, and modes of service delivery).

2.3 PersonalGO may also collect, store, and use the following information:

a) Records of any communication, such as file submissions or information uploaded to the Application, including those exchanged between Users;
b) Details of visits to the Application and the features accessed by Users;

c) Information about the access device used, including, for example, hardware model, operating system and version, file names and versions generated or managed by Users, preferred language, unique device identifier, advertising identifiers, serial number, and network information;
d) Access log information (including device IP address, date, and time), browsing characteristics, and browsing method; and
e) Preference data regarding how Users interact with the Application and chosen settings. In some cases, pixel tags and similar technologies are used to create and maintain unique identifiers.
f) Images and voice of Personal Trainers and Trainees who have subscribed to the Premium Plan ("Premium Users") contained in videos voluntarily submitted to the Application for the purpose of creating their personal exercise library.

2.3.1. By submitting videos to the Application, Premium Users acknowledge and agree that their image and voice may be stored and viewed by Trainees to whom the videos are sent, as well as by PersonalGO, exclusively for monitoring purposes and to enhance the platform experience.

2.3.2. The submission of videos by Premium Users does not imply an automatic assignment of image and voice rights to PersonalGO or third parties, but rather a license granted to PersonalGO for use in accordance with the functionalities of the platform. Responsibility for the content of the videos and for sharing them with Users who submitted them.

2.3.3. PersonalGO will not sell, distribute, or use the videos for purposes other than the operation of the Application without the express authorization of Premium Users. However, PersonalGO may process videos for organizational purposes, such as categorization and indexing of information related to exercises (muscles worked, equipment used, among others).

2.4 If the Trainee is under 18 (eighteen) years of age, registration for access to the Application shall only occur through registration performed by the Trainee's Legal Guardian. In other words, it will always be linked to a person fully capable of performing civil acts.

2.5. The personal data of children and adolescents are always processed considering their best interests, in accordance with Article 14 of the LGPD.

3. How PersonalGO Uses the Data Processed

3.1 By agreeing to this Policy, Users consent to PersonalGO processing the data collected through the Application for the purpose of:

a) identifying and registering Users in the Application and providing services to Users;

b) informing Users about changes to services, sending newsletters, special offers, and notifications of interest to the User;

c) contacting and notifying Users regarding changes in the Application or its policies and terms of use, when necessary;

d) ensuring that the content of the Application is presented in the most efficient manner to adapt the User experience, providing personalized, relevant, and effective service;

e) helping to make general improvements to the Application;

f) ensuring that the Application complies with all applicable data protection regulations and standards;

g) sending newsletters and informational emails;

h) conducting marketing campaigns and sending advertisements through the contact channels provided;

i) performing billing for services provided, when applicable;

j) conducting and supporting scientific research aimed at promoting public health studies, using anonymized data and respecting appropriate ethical standards related to such studies and research;

k) detecting and combating fraud, abuse, spam, illegal activities, and protecting access accounts.

3.2 The personal data processed by PersonalGO are framed under the following purposes and legal bases:

TYPE	DATA PROCESSED	PURPOSE	LEGAL BASIS
Trainee Data	Email address; Name; Phone number; Date of birth.	User identification and registration in the Application.	Performance of contract (art. 7, V, of the LGPD)
	Email address; Phone number.	Notifications, communication, and marketing campaigns	Consent for marketing activities and performance of contract for communication (art. 7, I and V, of the LGPD)
	Photo*; Gender*; and additional health information, such as diagnosed medical conditions, weight, body fat percentage, and height* * will only be collected if there is the Trainee's express interest, as this is optional data.	Personalized service.	Consent (art. 7, I and art. 11, I, of the LGPD)

	Body images captured during scanning by Artificial Intelligence	Personalized service.	Consent (art. 7, I and art. 11, I, of the LGPD)
Personal Trainer Data	Email address; Name; Phone number; Date of birth; and CPF (Brazilian Individual Taxpayer Number).	User identification and registration in the Application.	Performance of contract (art. 7, V, of the LGPD).
	Professional qualification information*	The documentary record is used for purposes of security, audit, oversight, or accountability.	Cumprimento de obrigação legal ou regulatória (art. 7º, II) LGPD

3.3. PersonalGO does not provide medical, clinical, nutritional, physiotherapy, or any other professional health services. The information, metrics, and analyses made available on the Platform or obtained through its technological resources are for informational purposes only and do not replace professional evaluation, diagnosis, or treatment. The User is responsible for ensuring that their health conditions allow for the practice of physical activities and should seek guidance from qualified professionals in case of doubts or specific needs.

4. Compartilhamento dos dados pessoais tratados

4.1 PersonalGO does not disclose to third parties any personal data provided by Users through the PersonalGO Application, except in the following cases:

a) With Personal Trainers who have an approved connection by the Trainee, and solely with respect to the information relevant to the provision of such service;
b) Sharing of information such as phone numbers between Users with an approved connection, to enable communication between them outside the Application, provided it is consented to by both parties and conducted through external services such as WhatsApp. PersonalGO does not have access to any communication conducted outside its Application environment, nor does it store the content of messages exchanged between Users outside the platform;
c) Cases in which PersonalGO is required to disclose or share the processed personal data to comply with a court order, or for the purposes of fraud prevention or other crimes, as well as in response to information requests from a competent authority, where we believe the disclosure is consistent with or required under applicable laws, regulations, or legal processes;

d) To protect the rights, property, or safety of PersonalGO and the Application;
e) With law enforcement agencies and/or government authorities, if it is believed that their actions are inconsistent with the provisions of our terms of use, or to protect the rights, property, or safety of PersonalGO, its Users, or others;
f) Upon the User's own action, when choosing to connect with other Users;
g) If, upon prior notice, the User agrees to share their data;
h) With third parties such as affiliates, subcontractors, and/or partners, for statistical reports created from anonymized data that do not reveal the identity of data subjects; and
i) In cases of partial or total sale of the business or its assets, or as part of any business reorganization or restructuring, merger, spin-off, or incorporation, whereby PersonalGO may share Users' information with third parties involved in such transactions, taking the necessary measures to ensure that privacy rights continue to be protected in accordance with this Policy.

4.2 PersonalGO also shares personal data with third-party business partners to enable the functionalities of the Application, as well as to store and back up information (e.g., storing data in the cloud on utilized servers).

4.2.1 These partners, in accordance with the LGPD, are processors or sub-processors of personal data who, by definition, must process personal data solely in accordance with the purposes set forth in this Policy. That is, partners may not use personal data in other ways or for purposes other than those provided for herein.

4.2.2 Whenever establishing a partnership, PersonalGO carefully assesses its business partners to determine whether those involved in data processing follow security standards deemed appropriate by PersonalGO for handling your information. Additionally, whenever possible, PersonalGO establishes specific contractual clauses to protect the confidentiality of your personal data.

4.3 PersonalGO may transfer or store Users' personal data on servers located outside the country of residence of the data subject, including in countries that may not offer the same level of personal data protection required by the User's local laws. These transfers may occur, for example, when we use cloud services, technology tools, or partners located abroad.

4.3.1 When we carry out international transfers, we ensure that appropriate safeguards are implemented to protect personal data, including, where required by law, the execution of Standard Contractual Clauses approved by the European Commission or other legally recognized mechanisms under applicable legislation.

5. Data Collection by Advertisers

5.1. The PersonalGO Application displays advertisements provided by advertising partners, such as Google AdMob, to maintain free access and offer a more personalized experience to Users. These partners may automatically collect certain user data during interaction with the ads, for example, language, IP address, device type, operating system, and data about the User's interaction with the ads.

5.2. The data may be used to personalize the displayed advertisements, measure the effectiveness of advertising campaigns, and offer more relevant content to the User. This use is always carried out through an automated and anonymized process, without manual analysis or direct disclosure of data to advertising partners. For more information about how Google AdMob

processes this data, please consult their Privacy Policy. Additionally, Users have the right to set appropriate ad preferences for their profile by accessing Google's ad preferences manager

5.3. By using the PersonalGO Application, the User acknowledges and accepts that the displayed advertisements may be targeted based on the information mentioned above. For further details or questions, please contact our privacy team through the channels indicated in this Policy.

6. Body Composition Assessment Using Artificial Intelligence

6.1. PersonalGO, in partnership with Shaped 3D LTDA, a company registered under CNPJ No. 42.909.293/0001-74 ("Shaped"), offers its Trainee Users the functionality of body composition assessment using artificial intelligence. This functionality allows Trainees to obtain body metrics through the capture and analysis of two images of their bodies and, if they wish, to integrate the history of assessments carried out with Shaped into the PersonalGO application. For further details on how data is processed by Shaped, please refer to their Terms of Use and Privacy Policy available at the following links: shaped.com.br/docs/terms_and_conditions/ e https://shaped.com.br/docs/privacy_policy/.

6.2. To use this functionality, the following data may be processed:

a) Data collected by Shaped: (i) Number of successful scans performed (without storage of images or body metrics).

b) Data processed by PersonalGO: (i) Body images captured by the Trainee (used exclusively for processing and not stored); (ii) Body images captured by the Trainee (used exclusively for processing and not stored); and (iii) History of body metrics processed by Shaped, integrated into the application with the Trainee's authorization.

6.2.1. Body images captured for this functionality will be temporarily stored by PersonalGO after collection, exclusively to allow technical reviews or reanalysis at the User's request. Once the temporary storage period ends, as provided in item 10.4, the images will be permanently and securely deleted, except where there is a pending review request.

6.3. The data processed under this functionality have the following purposes:

a) To enable body assessments directly in the PersonalGO application using advanced artificial intelligence technology;

b) To record and manage the Trainee's history of body measurements, if authorized;

c) To offer a personalized and enhanced workout tracking experience.

6.4. The processing of data related to this functionality is based on the following legal basis:

a) The Data Subject's consent, under Article 7, I, and Article 11, I, of the LGPD, for the collection and use of body images and metrics;

b) Performance of contract, under Article 7, V, of the LGPD, for the provision of personalized services in the application.

6.5. PersonalGO uses the Shaped API to technically process body images exclusively for the analysis and calculation of body metrics through artificial intelligence, without such images being stored either by Shaped or by PersonalGO. Shaped, in accordance with its privacy policy, agrees to: (i) Process the images securely and immediately without storing them; and (ii) Return to the PersonalGO application the data derived from the processing, such as measurements and body composition. Thus, PersonalGO will act as the Controller of the data stored in the application, while Shaped will act as the Processor for the technical processing of images and generation of body metric.

6.6. The images captured for this functionality will not be stored by Shaped and will be processed in real time and discarded immediately after analysis. The derived body metrics will be stored by PersonalGO in a secure environment, subject to the information security policies described in this Policy. The storage of photos by the Trainee will be optional and exclusively accessible to the Trainee.

6.7. To access the body assessment functionality, the Trainee must provide explicit consent, which can be revoked at any time through PersonalGO's contact channels. The Data Subject may also request the deletion of their data, as described in item 8 of this Policy.

6.8. For questions, requests, or the exercise of rights related to this functionality, the Trainee may contact PersonalGO's Data Protection Officer (DPO) at gabriel.delarocha@personalgo.app, or Shaped's DPO at contato@shaped.com.br.

7. Access and Correction of Personal Data

7.1. The User has the right to access their personal data processed by PersonalGO, as provided under the LGPD, by contacting the Data Protection Officer (DPO) via email at gabriel.delarocha@personalgo.app. The request will be responded to during business hours, Monday to Friday, from 8:00 a.m. to 8:00 p.m. (Brasília time, UTC-3), within fifteen (15) days, and the response may be sent by email or letter, in accordance with Article 9 of the LGPD, to ensure the following rights:

a) Right to confirmation of processing: the right to request confirmation of whether their personal data is being processed, including clear information about the source of the data, the absence of records, the criteria used, and the purpose of the processing.

b) Right of access: the right to be informed and request access to personal data processed by PersonalGO.

c) Right to rectification: the right to request that PersonalGO amend or update their personal data when it is incorrect or incomplete.

d) Right to erasure: the right to request the deletion of their personal data, or, if not possible (due to mandatory retention required by law), to have it maintained in an inactive database for the period established by law.

e) Right to data portability: the right to request the transfer of their personal data for use by third-party services.

f) Right to review of automated decisions: the right to request a review of decisions made solely through automated processing.

g) Right to object: the right to object to the processing of their personal data in certain situations, especially when the processing is based on legitimate interests or legal obligations.

h) Right to restriction of processing: the right to request the restriction of processing of their personal data in cases where the accuracy of the data is contested, where the User objects to the processing, or in other circumstances provided by law.

i) Right to withdraw consent: the right to revoke previously given consent at any time, through express manifestation, without affecting the lawfulness of the processing carried out prior to withdrawal.

j) Right to non-discrimination: the right not to suffer any form of discrimination or unequal treatment for exercising any rights related to the protection of their personal data.

k) Right to lodge a complaint with competent authorities: the right to lodge a complaint with the Brazilian National Data Protection Authority (ANPD) or other data protection authorities in accordance with applicable laws in their jurisdiction of residence.

7.2. The User has the right to request the deletion of their personal data stored in the Application at any time, except in cases where there is a legal obligation or court order requiring the retention of such data, under Articles 18, VI, and 16, I, of the LGPD. However, certain data may be maintained in anonymized form, as established in item 8 of this Policy, without any possibility of identifying the User, for the exclusive use of the controller, and prohibited from being accessed by third parties, under Article 16, IV, of the LGPD, including:

7.2.1. Data retained for all Users: (i) Gender; (ii) Age range; (iii) Indication of invitation relationships between users (whether invited and invitations sent); (iv) Connections made on the platform; (v) Record of acceptance of the Terms of Use and Privacy Policy during the period of activity; (vi) Type of profile (Trainee or personal trainer); (vii) State of the provided area code; (viii) Statistical data related to the number, dates, and duration of platform access;

7.2.2. Data retained for Trainees: (i) Declared objective; (ii) Self-declared level of proficiency; (iii) Desired training frequency; (iv) Registration date; (v) Information about free trial period and/or active subscription; (vi) Weight, height, and body fat index; (vii) History of created and executed workouts, including exercises, weights, repetitions, and workout dates;

7.2.3. Data retained for Personal Trainers: (i) Years of experience; (ii) Declared specialties; (iii) Hourly rate charged; (iv) Preference for in-person or online services; (v) History of training programs created and executed.

7.3. Data maintained in anonymized form will be used exclusively for statistical analysis, improvement of the User experience on the platform, development of new features, and market research studies, without any possibility of reidentification or use that violates the rights and individual freedoms of Users.

7.4. The User is responsible for keeping their information up to date. In the event of inaccuracies, PersonalGO may update or delete the information, except in cases where retention is necessary for legitimate business or legal purposes.

7.5. PersonalGO takes necessary security measures to protect Users' personal data and to safeguard it against loss, misuse, unauthorized access, disclosure, alteration, or destruction.

7.6. Users are also responsible for taking appropriate measures to protect their passwords, usernames, and other special access features to their personal account in the Application.

8. Updates to This Privacy Policy

8.1. PersonalGO may update this Policy from time to time. The use of processed information is subject to the Privacy Policy in effect at the time. If PersonalGO makes changes to how it processes personal data, Users will be notified by email.

8.2. Minor adjustments to this Policy may occur that do not significantly affect the way PersonalGO processes personal data, and therefore, such changes may not require individual notification.

9. Communication

9.1. By registering, Users agree that PersonalGO may send them emails containing notifications, advertisements, updates about the services, and important information regarding the use of the Application that may require their attention.

9.1.1. When receiving an email on behalf of PersonalGO, Users will have the option to opt out of receiving further emails by using the opt-out feature or by submitting a request via email.

9.2. PersonalGO takes necessary precautions to avoid the unsolicited sending of notifications.

9.3. The highest level of confidentiality is ensured in the handling of data such as email lists during PersonalGO's regular administrative tasks.

10. Retention and Storage of Personal Data

10.1. The LGPD does not establish a specific period for retaining personal data. However, it requires that storage be carried out for a reasonable period. PersonalGO will retain Users' data for as long as the User's account remains active.

10.2. The storage of personal data is carried out for a period considered appropriate based on applicable Brazilian law, as follows:

a) Six (6) months for records of Application activities, as provided under Article 15 of the Brazilian Internet Civil Framework (Marco Civil da Internet);

b) Five (5) years for information related to the processing of personal data, as this is the period during which PersonalGO may be subject to audits and/or legal claims.

10.2.1. In cases where data retention is required, the data subject will be informed of the impossibility of deletion, if such deletion is requested, and the data shall not be used for purposes other than those outlined in this section.

10.3. Retention includes personal data related to user registration and usage, as well as interaction records and associated information, which we retain for a period of six (6) years from either: (i) the date the User's account is cancelled; or (ii) the date the data subject (when not a User of the Application) provides their personal data through contact forms or similar means.

10.3.1. It is important to note, however, that in the event of ongoing administrative or judicial proceedings, regulatory oversight, or audits, PersonalGO may extend the afore mentioned retention period until the conclusion of the respective procedure.

10.4. In the case of personal data storage related to Clause 6, body images captured during the scanning process may be stored for up to forty-eight (48) hours after collection, exclusively to allow technical reviews or verifications. After this period, the images will be permanently deleted unless there is a pending review request.

11. Personal Data Security

11.1. Users' personal data and all information in the Application are stored and transmitted securely, and only employees authorized by PersonalGO may access personal information, being strictly bound by duties of confidentiality and a rigorous commitment to privacy, as provided in this Policy.

11.2. PersonalGO adopts appropriate technical and organizational measures to protect personal data against unauthorized access, loss, destruction, alteration, or improper disclosure, in compliance with the Brazilian General Data Protection Law (LGPD), the European Union General Data Protection Regulation (GDPR), the UK GDPR, the CCPA/CPRA, and other applicable laws. Such measures include, but are not limited to, access controls, encryption, monitoring, internal security policies, and periodic employee training.

11.3. All interactions conducted by PersonalGO are subject to data backups, monitoring tools, security policies, employee access controls, and up-to-date security software.

11.4. If PersonalGO becomes aware of any security breach within its own systems or those of its hosting providers, including intrusions, data leaks, or any other information security incident, it will notify the competent authorities and any affected Users about such breach and will provide as many details as possible regarding the nature, extent of the breach, and compromised data, within a reasonable timeframe, in accordance with Article 48, § 1, of the LGPD.

12. Security of Personal Data Processing

12.1. Personal data from your account and all Application information are securely stored and transmitted. Only employees authorized by PersonalGO have access to your personal data and are strictly bound by confidentiality obligations, professional secrecy, and a rigorous respect for privacy, in accordance with this Policy and applicable regulations.

12.2. Personal data are transmitted and stored on servers hosted by DigitalOcean, headquartered in the United States. All interactions carried out in the Application, including those relating to the transfer and sharing of information with public authorities, are subject to data backups, monitoring tools, security policies, and employee access controls, utilizing up-to-date security software.

12.2.1. Users retain all their rights over personal data, including the right to access, correct, delete, or request additional information about how their data is processed, even when such data

is stored or processed outside Brazil. To exercise these rights, Users may contact PersonalGO through the channels indicated in this Policy.

12.3. Since your data must be stored in locations compliant with Brazilian law (see Article 33 of the LGPD), PersonalGO informs and guarantees that the international server used meets the requirements established under the aforementioned legal provision.

12.4. If PersonalGO becomes aware of any security breach either within its own systems or those of its hosting providers, including intrusions, data leaks, or any other information security incident, it will notify the competent authorities and any affected Users about such breach and provide as many details as possible regarding the nature, extent of the breach, and compromised data, within a reasonable timeframe, in accordance with Article 48, § 1, of the LGPD.

13. Our Official Contact Channels

13.1. In case of questions or suggestions regarding the Privacy Policy or any other information related to this document, Users may request support via email from the Data Protection Officer (DPO), Gabriel Ferreira de La Rocha, at the email address gabriel.delarocha@personalgo.app.

13.2. Users residing in the European Union, the European Economic Area, the United Kingdom, or other international jurisdictions may contact PersonalGO for any matters related to privacy rights or the use of the Platform via email at gabriel.delarocha@personalgo.app, in Portuguese or English. If applicable, PersonalGO may appoint local representatives in such jurisdictions to comply with legal requirements, which will be informed in a future update of this Privacy Policy.

13.3. The support service hours are from 9:00 a.m. to 6:00 p.m., Brasília time (GMT-3). Our support team aims not only to resolve possible issues quickly and efficiently but also to seek an amicable solution.

14. General Provisions

14.1. PersonalGO does not use cookies in its Application. However, PersonalGO may adopt other technologies and mechanisms to store local data when strictly necessary for the proper functioning of the Application and to enhance the User's experience, always respecting legal guidelines and privacy rights. Such mechanisms are intended to ensure the operability of the Application and provide smoother and more personalized navigation without compromising the security and confidentiality of User information.

14.2. Users will be liable to indemnify PersonalGO for all costs and damages it may incur as a result of any violation of this Privacy Policy caused by them.

14.3. PersonalGO fully cooperates with any authorities or courts requesting disclosure of the identity or location of any person who has posted any material in the Application that violates the provisions of this Privacy Policy.

14.4. This Privacy Policy is governed by Brazilian law, with the courts of the Judicial District of Rio de Janeiro established as the competent forum to settle any disputes arising from this Policy, to the exclusion of any other forum, however privileged it may be or may become. Nonetheless, priority should always be given to attempts at resolution through conciliation or mediation.

14.5. If PersonalGO becomes subject to the obligation set forth in Article 27 of the General Data Protection Regulation (GDPR) of the European Union, it will appoint a representative established

in the European Union or the United Kingdom to act as its point of contact for authorities and data subjects, which will be disclosed in a future update of this Privacy Policy.

14.6. This Privacy Policy addresses only the processing of personal data provided to the platform. If the User discloses their information to third-party websites, different rules may apply to the use of their information.