

TO HELP YOU UNDERSTAND WHAT WE DO WITH YOUR INFORMATION

We have made every effort to explain clearly and simply what personal data we will need from you and what we will do with each of them. Below, we've highlighted the most important points, which can also be read in full detail in our Privacy Notice.

Additionally, we are always available to answer any questions you may have through the Support Tab within the GAIO system or via WhatsApp at +1 (346) 589-7667.

For specific inquiries about User personal data, we have a dedicated channel: lgpd@gaiodataos.com.

1. Who is responsible for data processing?

We are operators of the personal data entered into our system, even by users of GaiO Free. In other words, we simply provide the technology for decisions to be made by our clients.

We do not have control over the data that users enter into the solution or their outcomes. This means that the user is the data controller and is responsible for making relevant decisions regarding the processing.

We are the controllers of personal data related to our customers in some specific activities, such as sales and marketing. This means that once you choose to use our services, we will request some information and make decisions to provide the best possible service.

2. How will we ensure the security of your data?

GAIO is very concerned about the security of its users' personal data. Therefore, we are committed to keeping the data provided on the platform in a secure environment, considering the scale of the processing, through technical measures compatible with international standards and encouraging the use of good practices. This includes a risk analysis of information security and the implementation of effective and widespread Information Security Policies.

To ensure your information is stored in a secure environment, the platform uses trusted servers with restricted access. The use of this server may involve an international transfer of your personal data to the country where the server is located, the United States.

We emphasize that for GaiO Enterprise plan users, the system is installed on the user's machine, and the database and infrastructure are the user's own. It is the user's exclusive responsibility to implement all security measures.

3. What data do you need to provide to use our platform?

For registration and use of GAIO services, the following information will be required:

- **Free User:** Email, Username, and Password (Registration Data)
- **Teams or Business User:** Email, Username, and Password (Registration Data), and payment details.
- **Enterprise User:** Email, Username, and Password (Registration Data), essential contract data, and payment details.

4. For what purposes do we use your personal data?

All your data is processed for specific purposes and in accordance with the General Data Protection Law of Brazil. We may process this information for:

- Identification
- Platform usage
- Payment processing, for paid plans
- Providing our service
- Offering support and customer service
- Sending sales and marketing communications
- Offering our services or products

To better understand what we do with the information, we have provided a table in our Privacy Notice.

5. With whom do we share your personal data?

We will not share your data with third parties, except in the cases mentioned in the Privacy Notice, with the legal consent of the data subject, or by court order or legal determination.

6. Will your access logs be collected?

When you access our platform, we collect your access logs, meaning a set of information related to the date and time you use a specific internet application from a certain IP address. This information will be kept confidential by GAIO in a controlled and secure environment for a minimum period of 06 (six) months, in accordance with Law No. 12.965/2014 and Article 7, II, of Law No. 13.709/18.

7. Will personal data be collected indirectly?

In addition to access logs, we may also collect some information indirectly, in accordance with our Cookie Policy.

8. Will communication records be stored?

We will store and monitor the conversations you have with us through our communication channels, as this will improve your service, make it more efficient, and be used as evidence/proof of the service provided.

9. What are your rights?

Even if you have already provided us with your personal data, you have the full right at any time to: confirm the existence of data processing; access your data; correct your data; anonymize your data; block or delete unnecessary, excessive data, or data processed in non-compliance with the law; request data portability to another provider; delete data, except those required by law; obtain information on who the controller has shared your data with; obtain information about the possibility of not providing consent and the consequences of refusal; and withdraw and revoke your consent.

10. What is the content of the Privacy Notice?

The Privacy Notice is divided as follows to facilitate access to the information:

- a. Date of Availability of the Text;
- b. Explanation of Technical Terms or Foreign Language Terms;
- c. Data Processing Agents;
- d. Information Security;
- e. Data Collection;
- f. Processing of Personal Data;
- g. Cancellation of the Platform, Access Accounts, and Data Deletion;
- h. Rights of the Data Subject;
- i. Changes to the Privacy Notice;
- j. Communication Channel Regarding Privacy;
- k. Contact About General Matters.

GAIO

PRIVACY NOTICE

Before accessing the GAIIO platform, it is important that you read, understand, and freely, unambiguously, and informedly accept this Privacy Notice.

This platform, which includes both free and paid SaaS versions, is owned, maintained, and operated by GAIIO INNOTECH LTDA, CNPJ No. 28.575.989/0001-80, with its headquarters at Rua José Elias, 71, Sala 201, Bairro Jardim Karaiba, ZIP Code 38.411-201, Uberlândia – MG.

This document aims to provide information regarding the collection, use, processing, and storage of data provided by Users and is in accordance with Law No. 12.965/2014 (Internet Civil Framework) and Law No. 13.709/18 (General Data Protection Law).

1. DATE OF AVAILABILITY OF THE TEXT

1.1. This document was drafted and made available on 02/10/2025.

2. EXPLANATION OF TECHNICAL TERMS OR FOREIGN LANGUAGE TERMS

2.1. Below are the meanings of technical terms and terms in English:

- **Controller:** A natural or legal person, public or private, who makes decisions regarding the processing of personal data.
- **Cookies:** Small text files stored on a user's computer that can be retrieved by the website that sent them during browsing. They are primarily used to identify and store information about visitors.
- **Encryption:** A set of principles and techniques for encoding text, making it unintelligible to those who do not have access to the agreed-upon conventions.
- **Personal data:** Information related to an identified or identifiable natural person.
- **Sensitive personal data:** Personal data concerning racial or ethnic origin, religious beliefs, political opinions, membership in a union or religious, philosophical, or political organization, data regarding health or sexual life, genetic or biometric data, when linked to a natural person.
- **Data Protection Officer:** A person appointed by the controller and operator to act as a communication channel between the controller, data subjects, and the National Data Protection Authority (ANPD).
- **IP (Internet Protocol):** A unique identifier for each computer connected to a network.

- **Operator:** A natural or legal person, public or private, who processes personal data on behalf of the controller.
- **Data processing:** Any operation performed with personal data, such as collection, production, receipt, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, deletion, assessment, modification, communication, transfer, dissemination, or extraction.

2.2. Types of Users of the platform:

- **User:** A person who registers on the platform and may use the free version of Gaio or subscribe to paid plans (Teams, Business, and Enterprise).
- **Administrator User:** A person who registers on the platform and has access to the permission environment, able to make definitions such as: developer permission user, final user who does not access development, or restricting access to a specific application by a group of people.

3. DATA PROCESSING AGENTS AND INFORMATION SECURITY

3.1. We are operators of the personal data entered into our system, even by users of Gaio Free. That is, we only provide the technology for decisions to be made by our clients.

3.1.1. We do not control the data that users enter into the solution or their results. This means that the user is the controller of the data and responsible for making relevant decisions about the processing.

3.1.2. The user is fully responsible for determining the purposes of the data to be processed through the platform and for defining the most appropriate legal grounds for such processing.

3.1.3. The user is fully responsible for informing the data subjects in advance about the sharing of data with GAIO and must not include any data or information in the platform without the knowledge and/or specific consent (when applicable) of the data subject and/or their legal representative. Similarly, the user will be responsible for deleting the personal data they enter into the platform while the account is active and must directly address the requests from data subjects, so that GAIO will only follow their instructions when applicable and necessary.

3.1.4. Thus, the parties agree to respect and act in accordance with the obligations imposed on data processing agents by Law No. 13.709/2018, responding solely for their actions, with the possibility of a right of recourse by the innocent party in cases

of non-compliance and penalties, including judicial penalties and those imposed by the National Data Protection Authority (ANPD).

3.2. We are the controllers of personal data related to our clients in some specific activities, such as sales and marketing. That is, once you choose to use our services, we will request some information and make decisions in order to provide our service in the best possible way.

3.3. Some sub-processors are necessary for the platform to be available. Therefore, they will have access to user data for the following purposes:

3.3.1. **Azure:** Since personal data is stored on its servers, in cases where it is not the GaiO Enterprise plan, which is stored on the user's own database.

3.3.2. **Azure:** Since they are responsible for hosting the platform, in cases where it is not the GaiO Enterprise plan, which is hosted on the user's own infrastructure.

3.3.3. **Stripe:** Since they are responsible for processing payments, in the case of paid plans.

3.4. Our contracts always prioritize the secure processing of user information. Therefore, once these companies have access to this data, they will become responsible for the security, processing, and proper sharing of this information, and cannot disclose it for other purposes, in non-compliance with the applicable law or this Privacy Notice, under the penalty of responding to all punishments, especially civil, criminal, and those imposed by the National Data Protection Authority.

3.5. **International Transfer:** The servers used by GAIO, which are equipped with mechanisms to ensure the security of your data, are located outside Brazil, specifically in the United States, and are used for GAIO to perform its service adequately, as determined by Article 33, IX, of Law No. 13.709/18.

4. INFORMATION SECURITY

4.1. GAIO is highly concerned with the security of your personal data. Therefore, we implement all the measures suggested by the National Data Protection Authority (ANPD) in its Guideline for Small-Scale Data Processing Agents, which includes a variety of technologies and security procedures to help protect your information.

4.1.1. Additionally, we have effective measures and controls in place to prevent or reduce information security risks, with an approach focused on the principles of the matter, to prevent, detect, respond, and recover quickly from a threat to protect the confidentiality, integrity, and availability of technological assets and information.

4.2. All access records, which are a set of information regarding the date and time of use of a certain internet application from a specific IP address, will be kept by GAIO under confidentiality, in a controlled and secure environment, for a minimum period of 06 (six) months, as per Law No. 12.965/2014 and Article 7, II, of Law No. 13.709/18.

4.3. GAIO is committed to preserving the stability, security, and functionality of the platform through technical measures that comply with international standards and by encouraging the use of good practices. However, no service available on the internet can guarantee complete protection against illegal breaches. In cases where unauthorized third parties unlawfully breach the system, GAIO will do its best to identify the responsible party, but it will not be held liable for damages caused by such breaches.

4.4. We emphasize that in the Gaio Enterprise plan, the system is installed on the user's machine, and the database and infrastructure are the user's responsibility, meaning it is their exclusive responsibility to implement all necessary security measures.

4.5. The user must be responsible and declare themselves as exclusively responsible for all actions, as well as for all information and the accuracy of the content they enter into the platform.

5. DATA COLLECTION

5.1. To register and use GAIO's services, the following information will be required:

- **Free User:** Email, Username, and Password (Registration Data)
- **Teams or Business User:** Email, Username, and Password (Registration Data) and payment details.
- **Enterprise User:** Email, Username, and Password (Registration Data), essential contractual information, and payment details.

5.2. **Contact History:** GAIO stores information about all interactions previously conducted between users through the platform, such as in the support tab, to improve your service, make it more efficient, and use it as evidence/verification of the service.

5.3. **Information Collected Indirectly:** In addition to access records, we may also collect certain information indirectly, in accordance with our Cookie Policy.

6. PERSONAL DATA PROCESSING

6.1. By accepting this Privacy Notice, the User understands that the collection and processing of the personal data listed below are necessary for the execution of the contract with GAIIO, as detailed below.

Personal Data Type	Legal Basis	Purpose
User	Necessary for the execution of the contract or preliminary procedures related to a contract of which the data subject is a part, at the request of the data subject (Art. 7, V, Law No. 13.709/2018).	Used for identifying the User. This is essential data for contacting the User to address requests and provide targeted responses. It is also used to avoid duplication in registrations and prevent fraud.
E-mail	a) Necessary for the execution of the contract or preliminary procedures related to a contract of which the data subject is a part, at the request of the data subject (Art. 7, V, Law No. 13.709/2018).	a) Used to validate registration on the platform, as well as a means of communication with the User for contacts and interactions throughout the platform usage journey.

	<p>b) Necessary to fulfill the legitimate interests of the controller or a third party (Art. 7, IX, Law No. 13.709/2018).</p>	<p>b) Used for sending marketing emails, news, classifieds, and newsletters.</p>
<p>Payment Data</p>	<p>Necessary for the execution of the contract or preliminary procedures related to a contract of which the data subject is a part, at the request of the data subject (Art. 7, V, Law No. 13.709/2018).</p>	<p>Used for processing payments in cases of paid plans.</p>
<p>IP (Internet Protocol), Location, Referring Source, Browser Type, Visit Duration, Pages Visited</p>	<p>Compliance with legal or regulatory obligations by the controller (Art. 7, II, Law No. 13.709/2018).</p>	<p>Compliance with Article 15 of Law No. 12.965/2014, which imposes on GAIO the obligation to maintain access logs to internet applications, under confidentiality, in a controlled and secure environment for 6 (six) months.</p>
<p>Full Name</p>	<p>Necessary for the execution of the contract or preliminary procedures related to a contract of which the data subject is a part, at the request of the data subject (Art. 7, V, Law No. 13.709/2018).</p>	<p>Used for formal identification of the User, ensuring proper association of registration data and preventing fraud. Essential for the issuance of documents, contracts, and official communications.</p>

7. CANCELLATION OF THE PLATFORM, ACCOUNT ACCESS, AND DATA DELETION

7.1. Cancellation of Access Accounts by GAIO: GAIO may, at its sole discretion, block, restrict, disable, or prevent any User from accessing the platform if inappropriate conduct is detected.

7.2. Cancellation of Services by the User:

7.2.1. Free Gaio: The User may cancel the service at any time without restrictions through the "Delete Account" feature on the platform. No penalty fee will be charged.

7.2.2. Teams or Business Plan: These are monthly subscription plans. The User may cancel at any time. No refunds will be made for amounts paid for the month, and access to services will remain until the end of the payment period.

7.2.3. Enterprise Plan: The terms for cancellation, both without cause and with cause, will be specified in a specific contract.

7.3. When the purpose of data processing ends, or upon request via the email lgpd@gaiodataos.com, the User's data will be deleted immediately and permanently, except for data that must be retained by law or regulation, data necessary for the regular exercise of rights in judicial, administrative, or arbitral proceedings (such as access logs), which will be kept confidential in a controlled and secure environment, according to Law No. 12.965/2014 and based on Article 7, II, of Law No. 13.709/18.

7.3.1. It is emphasized that in cases where the User is the data controller, they are responsible for performing the necessary deletions.

8. RIGHTS OF THE DATA SUBJECT

8.1. The data subject has the right to request from the controller, at any time, in relation to the data processed by them:

8.1.1. Confirmation of the existence of data processing. **8.1.2.** Access to the data. **8.1.3.** Correction of incomplete, inaccurate, or outdated data. **8.1.4.** Anonymization, blocking, or deletion of unnecessary, excessive, or improperly processed data, in accordance with Law No. 13.709/2018. **8.1.5.** Portability of the data to another service or product provider, upon express request, in accordance with the regulations of the national authority, considering commercial and industrial secrecy. **8.1.6.** Deletion of data processed with the consent of the data subject, except in the cases provided for

in Law No. 13.709/2018. 8.1.7. Information about the public and private entities with which the controller shared the data. 8.1.8. Information on the possibility of not providing consent and the consequences of refusal. 8.1.9. Revocation of consent.

8.2. If GAIIO receives a request to exercise rights from a data subject where it is the data processor, the User, as the data controller, will be responsible for directly addressing the data subject's request.

9. CHANGES TO THE PRIVACY NOTICE

9.1. GAIIO may unilaterally add and/or modify any clause contained in this Privacy Notice. The updated version will apply to the use of the platform starting from its publication. Continued access or use of the platform after the disclosure will confirm the validity of the new Privacy Notice by the Users.

9.2. If the change made requires the User's consent, the option to freely, unequivocally, and informedly accept the new text or reject it will be presented.

9.3. If the User does not agree with the change, they may refuse to provide consent for specific actions or may terminate their relationship with GAIIO entirely. However, this termination does not exempt the User from fulfilling all obligations assumed under previous versions of the Privacy Notice.

10. PRIVACY COMMUNICATION CHANNEL

10.1. GAIIO designates Mr. Guilherme Tomaz De Freitas Mariano as the Data Protection Officer (DPO), with the email address lgpd@gaiodataos.com, in accordance with Article 41 of the General Data Protection Law, to accept complaints and communications from data subjects and the National Data Protection Authority, provide clarifications, and take necessary actions.

10.2. GAIIO has a specific document regulating the license of use, rights, duties, guarantees, and general provisions: the Terms of Use. All these documents are inseparably integrated into this Privacy Notice.

11. CONTACT FOR GENERAL MATTERS

11.1. GAIIO provides the following channels to receive all communications that Users may wish to make: through the Support Tab within the GAIIO system and via WhatsApp +1 (346) 589-7667.