Privacy policies

Data controller

For all purposes, the following companies will be responsible for the data: Internaut S.A.S, identified with Nit. 901.463.593 - 0, located at Calle 18 No. 31-28 in Bucaramanga, Colombia.

1. Objective

THE CONTROLLER is a company dedicated to information technology activities, computer services activities, and computer systems development activities as the data controller, and recognizes the importance of the security, privacy, and confidentiality of personal data of its employees, clients, suppliers, and in general, of all its stakeholders with respect to whom it processes personal information. For this purpose, it has created this policy for the processing of personal data (hereinafter the "Data Processing Policy") which will regulate the information and data that is collected, stored, and/or managed by THE CONTROLLER.

2. Definitions

The concepts presented below are the result of the provisions of Law 1581 of 2012 and Article 15 of the Colombian Political Constitution. In case the law is modified or replaced in these aspects, its meaning will be that indicated in the current legal norms.

Authorization: Prior, express, and informed consent of the Data Subject to carry out the Processing of personal data.

- **Database:** Organized set of personal data that is subject to Processing.
- **Personal data:** Any information related to or that can be associated with one or more identified or identifiable natural persons.
- **Data Processor:** Natural or legal person, public or private, that, by itself or in association with others, carries out the Processing of personal data on behalf of the Data Controller.
- **Data Controller:** Natural or legal person, public or private, that, by itself or in association with others, decides on the database and/or the Processing of the data. In this case, the company INTERNAUT S.A.S.
- **Data Subject:** Natural person whose personal data is subject to Processing.
- **Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation, or deletion.

- **Personal Data Protection Area/Privacy Officer:** Responsible within the Company, in charge of monitoring, controlling and promoting the application of the Personal Data Protection Policy.
- **INTERNAUT S.A.S:** Legally constituted company in Colombia that creates information technology products.
- **Joinnexus:** Remote team interaction platform developed by the company INTERNAUT S.A.S.

3. Legal framework applicable to data processing

In accordance with this Data Processing Policy, the following normative references and procedures/guidelines issued by THE CONTROLLER for the processing of personal data will apply: Statutory Law 1581 of 2012 and Regulatory Decree 1377 of 2013 incorporated into Decree 1074 of 2015, Title V of the Single Circular of the Superintendence of Industry and Commerce, and other related and complementary norms.

- Colombian Political Constitution.
- Law 1581 of 2012.
- Decree 1377 of 2013, incorporated into the Unique Decree 1074 of 2015.
- Regulatory Decrees.
- Circular 002 of 2015 of the Superintendence of Industry and Commerce.
- Applicable jurisprudence.
- Title V of the Single Circular of the Superintendence of Industry and Commerce.
- Other legal norms may be created in the future and are applicable.

4. Principles applicable to data processing

The processing of personal data carried out in connection with this Treatment Policy must strictly comply with the following principles:

- **Legality**: The processing must comply with the provisions of Statutory Law 1581 of 2012.
- **Purpose**: The purpose of the processing must be legitimate, temporary and informed to the data subject.
- **Freedom**: Data may only be processed with the prior, express, informed, and self-determined consent of the data subject or by legal or judicial mandate.
- **Truth or quality**: The information must be truthful, complete, accurate, updated, verifiable, and understandable.
- **Transparency**: The data subject's right to request information from the controller about their data at any time and without restrictions must be guaranteed.

- **Restricted access and circulation:** The processing may only be carried out by persons authorized by the data subject or by persons provided for by law.
- **Security**: The information must be handled with the necessary measures to provide security to the records and prevent their alteration, loss, consultation, unauthorized or fraudulent use or access.
- **Confidentiality**: Personal data that is not of a public nature is confidential and may only be provided in the terms of the Law. Anyone involved in the processing of the information must guarantee its confidential nature.

5. Purpose of the processing

As the data controller, THE RESPONSIBLE has various databases, which will be processed for one or more of the following purposes:

A. Administrative and accounting management.

a. Managing the collected data to administer account statements to each of these suppliers or customers.
b. Administration and formalization of commercial agreements and contracts with the Company's suppliers and service providers, and support for external and internal audits.
c. Reporting annually to the National Tax and Customs Directorate (DIAN), complying with the Company's legal obligations.
d. Recording and supporting financial and accounting information in the Company's software, in order to monitor transactions made.
e. Administration of contracts for third parties that provide services to the Company, such as lessors, security, and legal, among others.
f. Managing billing processes and managing the collection process associated with the expiration of payment terms granted in the Company's billing, in order to support payments within the internal accounting and serve as support for external and internal audits.

B. Commercial management, suppliers, and contractors.

a. Managing the link between customers and suppliers to facilitate the internal management of the Company's accounting, administrative, and financial processes.
b. Maintaining commercial relationships and future negotiations with suppliers and contractors from different areas of the Company.
c. Advertising of commercial promotions.
d. Advertising and commercial prospecting through the sending of emails or messages through applications to customers with information on promotions and follow-up of the curriculum plan.

C. Human Resources and Occupational Health.

a. Promote verification and evaluation procedures for candidates in selection processes in order to fill vacancies offered by the Company.
b. Perform and verify the results of comprehensive security studies for Company candidates as a prerequisite for employment.
c. Control and monitoring of the formalization of the employment of Company workers.
d. Control and monitoring of active and inactive personnel of the Company for statistical purposes.
e. Control and monitoring of temporary workers during the execution of their employment contract with the Company.
f. Verify the payroll of Company workers in order to report labor changes with an impact on payroll calculation, collection, and payment.
g. Manage the occupational health and safety management system to mitigate risks and ensure proper management of incidents or events during different work activities.
h. Promote the development of well-being activities, action plans, provisions, and the integral development of the worker in their work environment.
i. Control and monitoring of the reporting of risks that occur in the Company in order to identify unsafe areas and develop action plans to mitigate risks.
j. Control and monitoring of absenteeism of Company workers for statistical purposes.
k. Administer the occupational health and safety management system to monitor the medical examinations of workers upon entry and retirement.

D. Technology and security.

a. Promote control of the Company's computer and technological systems in order to manage user accounts, software licenses, and technical support.
b. Ensure the security of personal and financial information of organizations, their personnel, our providers, and collaborators, and at the same time have the broad and sufficient information that allows us to provide them with the best service.

6. Sensitive Personal Data Processing

According to Law 1581 of 2012, sensitive personal data is "those that affect the privacy of the Owner or whose misuse may generate discrimination, such as those

that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social organizations, human rights organizations or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sexual life, and biometric data." Within them, data of minors are also recognized.

While the RESPONSIBLE PARTY under normal platform operation conditions will not request sensitive data, in the event that it is collected, the RESPONSIBLE PARTY will strictly observe the limitations and legal obligations regarding sensitive data. Therefore, if sensitive data processing is carried out, the RESPONSIBLE PARTY will ensure:

6.1. Obtain express consent from the Owner.

6.2. Inform the Owner that, since it is sensitive data, they are not obliged to authorize its processing.

6.3. Explicitly and in advance inform the Owner which data will be subject to processing and the purpose of the processing.

Processing of Minors' Data

The platform is intended for users over 18 years of age. Persons under 18 years of age cannot use or register on the platform. While the RESPONSIBLE PARTY cannot absolutely control whether minors obtain unauthorized access to the Services, access may be canceled without notice if the Company considers that the services are being used by a minor.

7. Rights that the data subject is entitled to

- To know, update, and rectify their personal data that are being processed by the RESPONSIBLE or the data processors.
- To request proof of the authorization granted to the RESPONSIBLE, except when expressly exempted as a requirement for processing.
- To be informed by the RESPONSIBLE upon request, regarding the use given to their personal data.
- To revoke the authorization and/or request the deletion of the data when the processing does not respect constitutional and legal principles, rights, and guarantees.
- To file complaints with the Superintendence of Industry and Commerce for breaches of the provisions of Law 1581 of 2012.
- To be aware of our Personal Data Processing Policy, and the substantial changes that may occur therein.

- To access and know free of charge the personal data that are subject to the processing according to the provisions of the law, in the processing of personal data.
- Other rights granted by current legal norms.

8. Company's duties as data controller

A. Ensure that the data subject can fully and effectively exercise their right to habeas data at all times;
B. Request and keep a copy of the authorization granted by the data subject, under the conditions provided for in this law;
C. Properly inform the data subject about the purpose of the data collection and the rights granted to them by virtue of the authorization granted;
D. Keep the information under the necessary security conditions to prevent its alteration, loss, consultation, unauthorized or fraudulent use or access;
E. Ensure that the information provided to the data processor is truthful, complete, accurate, up-to-date, verifiable, and understandable;
F. Update the information by promptly informing the data processor of any changes regarding the data previously provided, and take any other measures necessary to keep the information provided up-to-date;
G. Rectify the information when it is incorrect and communicate the relevant information to the data processor;
H. Provide the data processor, where appropriate, only with data whose processing is previously authorized in accordance with the provisions of this law;
I. Require the data processor to respect the security and privacy conditions of the data subject's information at all times;
J. Process inquiries and complaints made in accordance with the terms set forth in this law;
K. Adopt an internal manual of policies and procedures to ensure compliance with this law, especially for the handling of inquiries and complaints;
L. Inform the data processor when certain information is in dispute by the data subject, once a complaint has been filed and the respective process has not yet been completed;
M. Provide the data subject, upon request, with information on the use made of their data;
N. Inform the data protection authority of security breaches and risks in the administration of the data subjects' information;
O. Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.

9. Transmitting and international transfer of data

When sending or transferring data to another country, it will be necessary to obtain the authorization of the data subject whose information is being transferred. In this sense, before sending personal data to another country, those who are obliged to comply with this policy must verify that they have the prior, express and unequivocal authorization of the data subject that allows for the transmission of their personal data. Notwithstanding the foregoing, THE RESPONSIBLE PARTY may transmit personal data internationally with the authorization of the data subjects, when they are transmitted to International Processors. This transfer of personal data will only be made to third parties with whom THE RESPONSIBLE PARTY has a contractual, commercial and/or legal relationship, aimed at carrying out some of the functions related to payment collection, safeguarding information, or outsourcing our customer service systems.

10. Security of data

Our platform has all the required licensing in all aspects of software development, infrastructure, and third-party tools. We have the necessary licensing levels that adapt to the needs of each situation, with support from manufacturers and experts.

This also applies to access to data from our customers, suppliers, and collaborators. As these accesses are protected by audit concepts and are only granted through controlled access tools such as VPNs or proprietary tools that control and audit access.

Similarly, access to information by our collaborators is protected by filters and security levels that guarantee restriction based on roles and responsibilities. And a detailed record is kept of any queries or modifications to the data with audit data responding to who, when, and what was done.

11. Authorization for Data Processing

The consent and authorization of the data subject is a constitutional and legal requirement that must be met by the persons responsible for the processing of personal data. The consent must meet the following requirements:

Prior: The authorization must be given by the data subject prior to any type of processing of personal data.

Express: The authorization must be granted unequivocally, clearly, and specifically.

Informed: The data subject must clearly understand for what purposes their personal data will be processed and the purposes that may arise from the processing.

All users of the Joinnexus platform must register and authorize the processing of personal data in order to use the services offered. Therefore, on the platform, when registering for the first time, there is a box that says "Privacy Policy and Processing of Personal Data" which must be read and accepted in order to continue using the services of **INTERNAUT S.A.S.**

12. Procedure for submitting claims, inquiries, and complaints.

THE RESPONSIBLE PARTY will have the following procedures for addressing questions, complaints, inquiries, claims, and suggestions presented by the Data Subjects, in accordance with the provisions of Law 1521 of 2012:

Inquiries

The data subject or their legal representative will make inquiries through written communication or by email, in which they:

1. Identify themselves, including their name and identification number.
2. Clearly and expressly specify the reason for the inquiry.
3. Provide legitimate interest with supporting documentation.
4. Indicate the physical or electronic address to which a response to the request can be sent.
5. If the request is incomplete, the interested party will be required to rectify the deficiencies within five (5) days following the receipt of the claim. If two (2) months have elapsed since the date of the requirement and the requester has not submitted the requested information, it will be deemed that they have withdrawn their request.

In accordance with Article 14 of Law 1581 of 2012, "The inquiry will be addressed within a maximum of ten (10) business days from the date of receipt. If it is not possible to address it within this period, the interested party will be informed, stating the reasons for the delay and indicating the date on which their inquiry will be resolved, which in no case may exceed five (5) business days following the expiration of the initial term."

Claims

The data subject, their legal representative, or any other person with a legitimate interest who considers that the information contained in a database must be corrected, updated, deleted, or that authorization granted for its processing must be revoked, or when they detect a presumed breach of any of the duties contained in Law 1581 of 2012, may submit a timely claim to the responsible area, either physically or electronically. In accordance with Article 15 of Law 1581 of 2012, such a claim will be admissible once the following requirements are met:

1. The claim must: i) include the identity of the claimant, stating their name and identification number; ii) clearly and expressly specify the reason for the claim; iii) provide legitimate interest with supporting documentation; and iv) indicate the physical or electronic address to which the response to the request should be sent. If the claim is found to be incomplete, "the interested party will be required to rectify the deficiencies within five (5) days following its receipt. If two (2) months have elapsed since the date of the requirement and the requester has not submitted the requested information, it will be deemed that they have withdrawn their claim."
2. If THE RESPONSIBLE PARTY is not competent to resolve the claim, they will transfer it to the appropriate party within a maximum period of two (2) business days and inform the interested party of the situation.
3. "Once the complete claim has been received, a note will be included in the database stating 'claim in process' and the reason for it, within a period not exceeding two (2) business days. This note must be maintained until the claim is resolved."

"The maximum period for addressing the claim will be fifteen (15) business days from the day following its receipt. If it is not possible to address it within this period, the interested party will be informed of the reasons for the delay and the date on which their claim will be resolved, which in no case may exceed eight (8) business days following the expiration of the initial term."

The request to delete information and the revocation of the authorization will not proceed when the Data Subject has a legal or contractual obligation to remain in the database with THE RESPONSIBLE PARTY.

The data subject may only file a complaint with the Superintendency of Industry and Commerce once they have exhausted the procedure for inquiries or claims before Internaut S.A.S, in accordance with the aforementioned procedure.

13. Attention to inquiries and complaints

The RESPONSIBLE has an area in charge of attending and resolving inquiries and complaints from data subjects or authorized persons. Data subjects may submit their inquiries and complaints through the following channels:

- Email: hello@joinnexus.io
- Whatsapp: +57 312 5256655

14. Third-party links

The RESPONSIBLE, on its website or through social networks, may make links to third-party addresses available to its users. In this case, INTERNAUT S.A.S is not responsible for the privacy practices of those other websites or those who manage them, and the RESPONSIBLE expressly exempts itself from any responsibility for the actions of these third parties. In the event that a customer, user, or merchant is providing the RESPONSIBLE with information about a third party through any means, the user declares to have all the authorizations from the data subject, including the purposes for which it is being shared, and in that sense, the RESPONSIBLE will not assume any responsibility for the use that the customer gives to the data in accordance with the purposes indicated in this policy.

15. Attention to inquiries and complaints

The RESPONSIBLE has an area in charge of attending and resolving inquiries and complaints from data subjects or authorized persons. Data subjects may submit their inquiries and complaints through the following channels:

- Email: hello@joinnexus.io
- WhatsApp: +57 312 5256655

16. Modifications to the policy

The RESPONSIBLE reserves the right to modify the privacy policy of personal information at any time. For this purpose, a notice will be posted on the website or through the mechanism enabled by the RESPONSIBLE 10 business days prior to its implementation and during the validity of the policy. In the event that data subjects or their representatives do not agree with the new policies for handling personal information, they may request the removal of their information through the aforementioned means. However, data cannot be requested to be removed while a relationship of any kind with the RESPONSIBLE is maintained.

17. Validity of databases

Personal Data that is stored, used, or transmitted will remain in the databases of the RESPONSIBLE party for as long as necessary to fulfill the purposes set out in this policy or for the Company to comply with its legal obligations.

However, the information will be reviewed every year to verify the accuracy of the data and the purpose of continuing its processing.

If necessary, the RESPONSIBLE party reserves the right to unilaterally modify this Policy.