DATA PROCESSING POLICY
PROLIBU TECH S.A.S.

1. General Information of the Company

PROLIBU TECH S.A.S. (the "Company"), TIN [901.268.824-1], a company incorporated and existing under the laws of the Republic of Colombia, with domicile in Bogota D.C, with main offices at the address [Cra 9 # 115-06 / Piso 17 Of. 01] of Bogotá D.C, phone number (57- 311-5213448), is a company devoted to the protection of privacy, integrity, security and confidentiality of all identifying, contact, sensitive and biometric data, and all other data related or that may be related to one or several certain or ascertainable natural persons (the "Personal Data") such as its customers, providers, employees, contractors, be they potential or current, and, in general, all Holders registered in the Company's database, information that it has access to and which it processes while developing its business activity, which is developing IT systems (planning, analysis, design, programming, tests) and, in general, IT consulting and administration activities of IT installations.

The company carries out its Personal Data Processing through activities that include their recollection, storage, management, processing, creation of databases, circulation, segmenting, transfer, transmission and/or use.

This Data Processing Policy required by Decree 1074 of 2015 (the "Policy"), has the purpose of informing the Holders of their legal rights regarding their Personal Data, making known the mechanisms and procedures to make them effective , to make known who within the Company is in charge of tending to the inquiries, questions, claims and complaints and, finally, to make known the purposes and Processing to which the Personal Data will be subjected in the development of the Company's business activities.

2. Scope of this Policy

This Policy will apply to all Personal Data Processing carried out in the territory of the Republic of Colombia by the Company through its employees and, where applicable, by those third parties that reach an agreement with the company to perform all or part of any activity relating or related to the Personal Data Processing for which the Company is a Responsible Party (as defined further below).

The Policy will also apply to third parties with whom the company eventually signs Transmission Contracts (as defined further below), so that such third parties are aware of the obligations that will apply to them, the purposes they must submit to and the security and confidentiality standards that they must adopt when Processing data on behalf of the Company.

3. Main definitions

The most relevant terms of this Policy are defined below:

Term	Definition
Authorization	It is the prior, express and informed consent of the Holder to perform Data Processing.
Authorized Party	It is the Company and all the people who by virtue of the Authorization and this Policy, have the legitimate right to perform Processing.
Notice of Privacy	It is the verbal or written communication generated by the Responsible Party, addressed to the Holder, by means of which they are informed about the existence of the Policy, the way to access it, their rights and the purposes of Processing.
Database	It refers the organized set of Personal Data that are subject to Processing, whatever its form, storage, organization and access.
Personal Data	It is any piece of information of any kind, linked to or that can be associated with one or more certain or ascertainable natural persons.
Public Data	It means the Personal Data qualified as such according to the mandates of the law or the Political Constitution and that which is not semi-private, private or sensitive. The data related to the marital status of individuals, their profession or trade, their status as a merchant or public servant and those that can be obtained without any reservation, among others, are public. By its nature, public data may be contained in public registries, public documents, official gazettes and bulletins, duly enforced court rulings that are not subject to confidentiality, among others.
Sensitive Data	It is the Personal Data that could affect the privacy of the Holder or whose improper use could generate discrimination, such as those that reveal union affiliations, racial or ethnic origin, political orientation, religious, moral or philosophical convictions, membership to unions, social or human rights organization or those that promote the interests of any political party or that guarantee the rights and guarantees of political parties of the opposition, as well as data related to health, sexual life, and biometric data.
Party in Charge	It is the natural or legal person, public or private, that by itself or in association with others, performs Processing on behalf of the Responsible Party.
Capacity	It is the capacity that the company grants to third parties expressly and in writing by means of a contract or document that takes its place, in compliance with the applicable Law, to carry out Processing, turning such third parties into Parties in Charge.
Party with Legitimate Right	It refers to those who can exercise the rights of the Holder, such as the Holder when proving their identity by the means at their disposal, the successors who prove that status, the representative and/or attorneys showing a power of attorney or evidence of legal representation and those who have the right by stipulation in favor of a third party or for a

third party.

Law	It is Law 1581 of 2012, Decree 1074, Sentence C-748 of 2011, and the case law of the Constitutional Court related to personal data that sets precedents, and any regulation issued by the government regulating the legal precepts, that are in force at the time Processing by the Company begins, as may be amended from time to time and when such amendment applies to Processing carried out by the Company.
Manual	It is the document that contains the policies and procedures to guarantee adequate compliance with the Law.
Policy	It is this document, establishing the data processing policy required by Decree 1074, which also contains the directives and guidelines in relation to the protection of personal data, and which includes, among other things, (i) full identification of the Responsible Party (name, business name, domicile, address, email and telephone number); (ii) the forms of Data Processing; (iii) the purposes to which they are subject; (iv) the Rights of the Holders; (v) the procedures for inquiries, claims and complaints and to exercise the rights of the Holders, and (vi) the person or agency in charge of tending to all the inquiries of the Holders.
Responsible Party	It is any person whose Personal Data Processing activities are subject to compliance with this Policy, as they perform decision-making activities on databases that contain Personal Data.
Holder	It is the natural person to whom the Personal Data refers–such data may be stored in a Database–and who is the subject of the right to habeas data.
Transfer	It is Processing that involves sending the information or Personal Data to a recipient, who is a Responsible Party and is located outside or within the country. In the Transfer, the recipient will act as Responsible Party and will not be subject to the terms and conditions of this Policy.
Transmission	It is Processing that involves the communication of Personal Data within or outside the territory of the Republic of Colombia when it has the purpose of carrying out Processing by the Party in Charge on behalf of the Responsible Party. In the Transmission, the recipient will act as Party in Charge and will be subject to the Policy and the terms established in the Transmission Contract.
Processing	It is any systematic operation and procedure, whether it is electronic or not, that allows the collection, conservation, ordering, storage, modification, linking, use, circulation, evaluation, blocking, destruction and, in general, processing of Personal Data, as well as its delivery to third parties through communications, inquiries, interconnections, assignments, data messages.

4. Principles

In all Processing carried out by the Company as Responsible Party, and by its Parties in Charge and/or third parties that receive Transmission of the Personal Data, the principles established in the Law and in this Policy will be complied with, in order to guarantee the habeas data right of the Holders. These principles are:

Principle	Description
Restricted Access	The Company may not make Personal Data available for access through the Internet or other means of communication, unless technical and security measures are established that allow access to be controlled and restricted only to Authorized parties. Personal Data may not be available on the internet or other means of dissemination or mass communication, unless access is technically controllable to provide restricted knowledge only to Holders or Authorized third parties or unless the information is public.
Restricted Circulation	Personal Data can only be Processed by company staff who have Authorization to do so, in accordance with the provisions of such authorization, or those who within their functions are in charge of carrying out such activities. Personal Data may not be delivered to third parties, within or outside the territory of the Republic of Colombia, without the Authorization or without the signing of a contract, in the event that there is Transmission.
Confidentiality	Processing must be subject to strict confidentiality requirements and, therefore, the people involved in it must keep the data confidential, even after the relation that gave rise to the Processing has ended.
Consent	Processing requires Authorization, by any means that may be subject to subsequent inquiries, including through unequivocal conduct as established by Decree 1074.
Sensitive Data and Diligence	Sensitive Data that is collected in the development of the Company's activities must be processed with the utmost diligence to preserve its integrity, restricted access and security.
Purpose	All Processing activities must obey the legitimate purposes mentioned in this Policy, which must be notified to the Holder when obtaining their authorization.
Integrity	Personal Data submitted to Processing must be true, complete, accurate, updated, verifiable and understandable. When it is in possession of partial, incomplete, fractioned or misleading Personal Data, the Company must refrain from Processing them or request the Holder to complete or correct the information. The Company shall make its best efforts to maintain the integrity of the Personal Data contained in its Databases and the veracity thereof, implementing verification and updating measures for Personal Data.

Security	The Company must always carry out Processing while providing the technical and human and administrative security measures necessary to maintain the confidentiality and security of the Personal Data. This is in order to prevent them from being adulterated, modified, consulted, used, accessed, deleted or known by unauthorized third parties. The Company will adjust Processing to the security standards established by the competent authorities in the future.
Severability of the Databases	The Company will maintain the Databases where it acts as Party in Charge separate from those where it acts as the Responsible Party.
Temporary Nature	The Company will not use the Personal Data beyond the reasonable period required for the purposes notified to the respective Holder and will take measures to guarantee the deletion of the Personal Data when it ceases to fulfill the purpose for which it was collected.
Transparency	When the Holder requests it, the Company must provide them with information about the existence of Personal Data concerning them or about those where they are a Party with Legitimate Right to request it. The response to the request must be granted through the same channel or, at least, through a channel similar to that used by the Holder to request information and within the terms established by the Law.
Later Processing	All Personal Data that is not Public Data must be Processed by the Responsible Parties and Parties in Charge as confidential and under the security parameters established by the Superintendency of Industry and Commerce. Upon termination of said relation, such Personal Data must continue to be processed in accordance with the Policy, the Manual and the Law.

5. Processing and Purposes

The Company while developing its business activities, will carry out the Personal Data Processing, for the purposes established below and for those purposes that are accepted by the Holders at the time of the collection of their Personal Data. These purposes will also be applicable to all Parties in Charge or third parties who have access to Personal Data by virtue of Law, contract or other document that connects them to the Company:

Purposes
Corporate, Administrative and Marketing Purposes
Managing all the information necessary to comply with the tax obligations and business, corporate and accounting records of the Company.

Complying with the internal processes of the Company regarding the administration of suppliers and contractors.
Delivering information to third parties for evaluation and classification of suppliers.
Performing marketing activities
The process of filing, updating systems, protecting and safeguarding information and Databases.
Processes within the Company for the system development, operation and/or administration.
Performing the analysis for the control and prevention of fraud and money laundering, including, but not limited to, consulting and reporting to restrictive lists and financial credit bureaus.
Holding events, extending invitations to concerts, and play and entertainment activities.
The Company's human resources management, including but not limited to the evaluation of candidates interested in being employees of the Company, hiring new employees of Company, training processes, performance evaluation, advancing social welfare and occupational health programs, issuance of labor certifications, supply of work references if requested, creating the human resources map of the staff working in the Company, and payroll.
Carrying out data update campaigns to guarantee the integrity thereof.
Carrying out internal investigations in accordance with the different policies of the company in the event of suspicious activities that may affect the good name of the Company (only applies to employees or service providers of the Company).
Carrying out customer satisfaction and service quality surveys.
Sending modifications to this Policy, as well as the request for new authorizations for Personal Data Processing.
The other purposes determined by the Responsible Party in the processes of obtaining Personal Data for its Processing, in order to comply with legal and regulatory obligations, and the development of the Company's business activities.
Business and business activities
Implementing communication channels between the customer, suppliers and other natural or legal persons relevant to the development of the Company's business activities.
Carrying out visitor and customer loyalty activities.
Performing information analysis and segmenting to prepare studies and statistics on consumer preferences.
Performing opinion surveys and/or polls about products and services.
Share either through transfer or transmission of personal data of customers to PROLIBU LLC in the United States.
Before third parties
Complementing the information and, in general, performing the necessary activities to manage the requests, complaints and claims presented by the Company's customers and by third parties, and directing them to the areas responsible for issuing the corresponding responses.
Transmitting Personal Data to third parties with whom contracts have been executed or documents such as amendments or declarations have been signed that allow Personal Data

to be transmitted, for commercial, administrative and/or operational purposes.

To comply with the aforementioned purposes, to transfer, transmit, transfer, share, deliver, and/or reveal Personal Data to third parties, inside and outside the national territory, even to countries that do not provide adequate levels of protection of Personal Data.

In accordance with the Law, the Holders have the following rights:

Right	Description
Updating	Update the Personal Data that is stored in the Company's Databases to maintain its integrity and veracity.
Knowledge and Access	Know and access your Personal Data before the Company or the Parties in Charge. This access will be done for free at least once a month.
Proof	Request proof of the Authorization granted to the Company, unless the Law indicates that said Authorization is not necessary.
Complaint	Submit complaints for infractions of the Law before the Superintendency of Industry and Commerce after exhausting the procedural requirement and going first to the Company.
Correction	Correct the information and Personal Data that are under the control of the Company.
Revocation	Request that the Authorization be revoked, as long as there is no legal duty or a contractual obligation of the Holder before the Company under which such Personal Data must remain in the Company's Databases.
Request	Submit requests to the Company or the Party in Charge regarding the use that they have given to the Holder's Personal Data, and that they provide the Holder with such information.
Deletion	Request the deletion of Personal Data from the Company's Databases, as long as there is no legal duty or a contractual obligation of the Holder before the Company under which such Personal Data must remain in the Company's Databases.

Holders may exercise their legal rights and carry out the procedures established in this Policy by presenting their citizenship card or any identification document. Minors may exercise their rights personally or through their parents or adults who have parental authority, who must prove it through the relevant documentation. Likewise, all the Parties with Legitimate Right may exercise the rights of the Holder by presenting the respective document.

6. Sensitive Data

Within the framework of its business activities, the Company may collect and Process Sensitive Data, such as medical information, and images, photographs and/or voice recordings and, in general, biometric data. Other Sensitive Data related to health, sex and

any information whose Processing affects privacy may also be processed. The Company will inform the Holders so that they give independent and free consent to Process such Sensitive Data a particularly sensitive nature.

Sensitive Data will be processed with the upmost diligence and with the highest security standards. For this, the Company's area in charge will internally develop procedures to maintain at all times the confidentiality and integrity required by this type of Sensitive Data. Limited access to Sensitive Data will be a guiding principle to safeguard their privacy, for which reason only authorized personnel may have access to this type of information.

The Authorization for Sensitive Data Processing is **optional and entirely at the choice of the Holder**; therefore, no activity will be restricted or conditioned to the supply thereof, so that the Holder has the right not to authorize the Processing of their Sensitive Data, and that decision will be respected by the Company.

7. Authorization

An Authorization must be obtained before performing any Processing. To that end, prior to the collection of Personal Data, the Company, its employees and Authorized Persons, must obtain the Authorization signed by the Holder and keep a copy of this document for future inquiries.

The authorization of the Holder will not be necessary in the case of:

- Information required by a public or administrative entity in the exercise of its legal functions or by court order;
- Public data;
- Medical or health emergency cases;
- Information processing authorized by law for historical, statistical or scientific purposes;
- Data related to the Office of Vital Statistics

Any case of new procedures for collecting Personal Data must be validated with the Company’s legal department if the legal exceptions to the Authorization, mentioned above, apply.

8. Personal Data Protection Area

The Company has a department in charge of receiving and handling Petitions, Complaints and Claims related to Personal Data, called [Business and Customer service Department]. The agency has Customer Service, which will specifically process inquiries and claims regarding Personal Data in accordance with the Law, the Manual and this Policy. Some of the particular functions of this area in relation to Personal Data are:

- Receiving and tending to all requests from the Holders, process and respond to

those that are based on the Law or this Policy, such as: requests to update their Personal Data; requests for knowledge of their Personal Data; requests for the deletion of Personal Data, requests for revocation of the authorization when such revocation applies pursuant to Decree 1074; requests for information on the Processing and purposes of their Personal Data, and requests to obtain proof of the Authorization granted, when it applies pursuant to Law.

- Responding to the Holders on those requests that do not apply under the Law.

The contact information for [Customer Service] is:

Contact information for the person and/or area in charge	
Office, person and/or area in charge of data protection issues	Customer Service Ivandavid Rueda
Physical address	Cra 9 # 115-06 / Piso 17 Of. 01
Email	info@prolibu.com
Phone number	
Position of the contact person	Commercial Manager – Customer Service

9. **Procedures to exercise the Holders' rights.**
    a. **Inquiries (see Annex 1)**

The Company has various mechanisms so that the Holder, the Parties with Legitimate Right or the representatives of underage Holders can make all kinds of INQUIRIES regarding:

- The Personal Data of the Holder that is stored in the Company's Databases.
- The Processing to which they are subjected.
- The purposes intended.

The mechanisms used to formulate the Inquiries may be physical, such as in person procedures, or electronic channels such as the email info@prolibu.com. Whatever the channel, the Company will keep evidence of the inquiry and its response.

Before proceeding, the person responsible for tending to the inquiry will verify:

1. The identity of the Holder or the Party with Legitimate Right. To that end, they will demand the citizenship card or any original identification document of the Holder and the special or general powers of attorney, as the case may be.
2. The Authorization or contract with third parties that gave rise to Processing by the Company.
3. They will indicate the date on which the inquiry was received by the Company.

If the applicant has the capacity to formulate the inquiry, the person responsible for tending to it will collect all the information about the Holder that is contained in that person's individual record or that is connected to the Holder's Identification within the Company's Databases. Once the information has been collected, it will be provided to the Holder so that they have access and is able to know it.

The person responsible for tending to the query will respond to the applicant, as long as the latter has the right to do so as the Holder, the Party with Legitimate Right, or the legal guardian in charge in the case of minors. This response will be sent within **ten (10) business days**, counted from the date the request was received by the Company.

This response will be mandatory even in cases in which it is considered that the applicant does not have the capacity to perform the inquiry, in which case the applicant will be informed, and the option will be given to demonstrate power and capacity by providing additional documentation.

In the event that the request cannot be tended to within **ten (10) business days**, the applicant will be contacted to be notified of the reasons why the status of their request is in process, with the date on which the consultation will be tended to, which in no case may exceed **five (5) business days** following the expiration of the first term. To this end, the person responsible will use same channel through which the query was submitted or one equivalent to it.

The final response to all requests may not take **more than fifteen (15) business days** from the date the initial request was received by the Company. For that reason, the Company will follow up on any inquiries that may arise.

b. Claims (see Annex 2)

The Company will have mechanisms so that the Holder, the Parties with Legitimate Right or the representatives of underage Holders can make CLAIMS regarding:

- Personal Data Processed by the Company that must be corrected, updated or deleted;
- The alleged breach of the Company's legal duties.

These mechanisms may be physical, such as an in-person procedure, or electronic, such as email. Whatever the channel, the Company must keep proof of the inquiry and the response, in case its subsequent checking is necessary.

The CLAIM must be submitted by the Holder, the Parties with Legitimate Right, or their representatives in the event that the Holder is a minor, as follows:

- They must address Customer Service, if electronically via email to the address info@prolibu.com and if physically to the physical address Cra 9 # 115-06 / Piso 17 Of. 01
- It must contain the name and identification document of the Holder.
- It must contain a description of the occurrences that give rise to the claim and the objective pursued (update, correction or deletion, or fulfillment of duties).
- It must indicate the address and contact information and identification of the

claimant.

- It must be accompanied by all the documentation that the claimant wants to enforce.

Before proceeding, the person responsible for tending to the claim will verify:

1. The identity of the Holder or their representative. To that end, they may demand the citizenship card or any other identification document of the Holder, and the special or general powers of attorney of the representative, as the case may be.
2. The Authorization or contract with third parties that gave rise to Processing by the Company.
3. The date on which the claim was submitted will be set.
4. If the claim or the additional documentation is incomplete, the Company will require the claimant only once, **within five (05) business days**, after receiving the claim, to correct the issues. If the claimant does not submit the required documentation and information **within two (02) months** from the date of the initial claim, it will be understood that they have withdrawn the claim.
5. If for any fact the person who receives the claim within the Company does not have the power to solve it, they will transfer it to the Data Protection Area – Customer Service, **within two (02) business days** after receiving the claim and will inform the claimant of said referral.
6. Once the claim with the complete documentation has been received, a legend that reads “claim in process” and the reason thereof will be included in the Company's Database where the Holder's Personal Data subject to the claim is stored, in a period not greater than two (02) business days. This legend should be kept until the claim is decided.
7. The maximum term to tend to the claim will be **fifteen (15) business days** from the day following the date of receipt. When it is not possible to tend to the claim within said term, the interested party will be informed of the reasons for the delay and the date on which their claim will be tended to, which in no case may exceed eight (08) business days following the expiration of the first term.

To graphically consult our procedures and terms to respond to inquiries and claims, please consult the Annexes to the Policy.

10. Term

This Policy will take effect on [November 1, 2019]. The Personal Data that is Processed will remain in the Company's Database, with basis on the criteria of temporary nature, for as long as it is necessary to fulfill the purposes mentioned in this Policy, and for which they were collected. Therefore, the term of the Database is closely related to the purposes for which the Personal Data was collected.

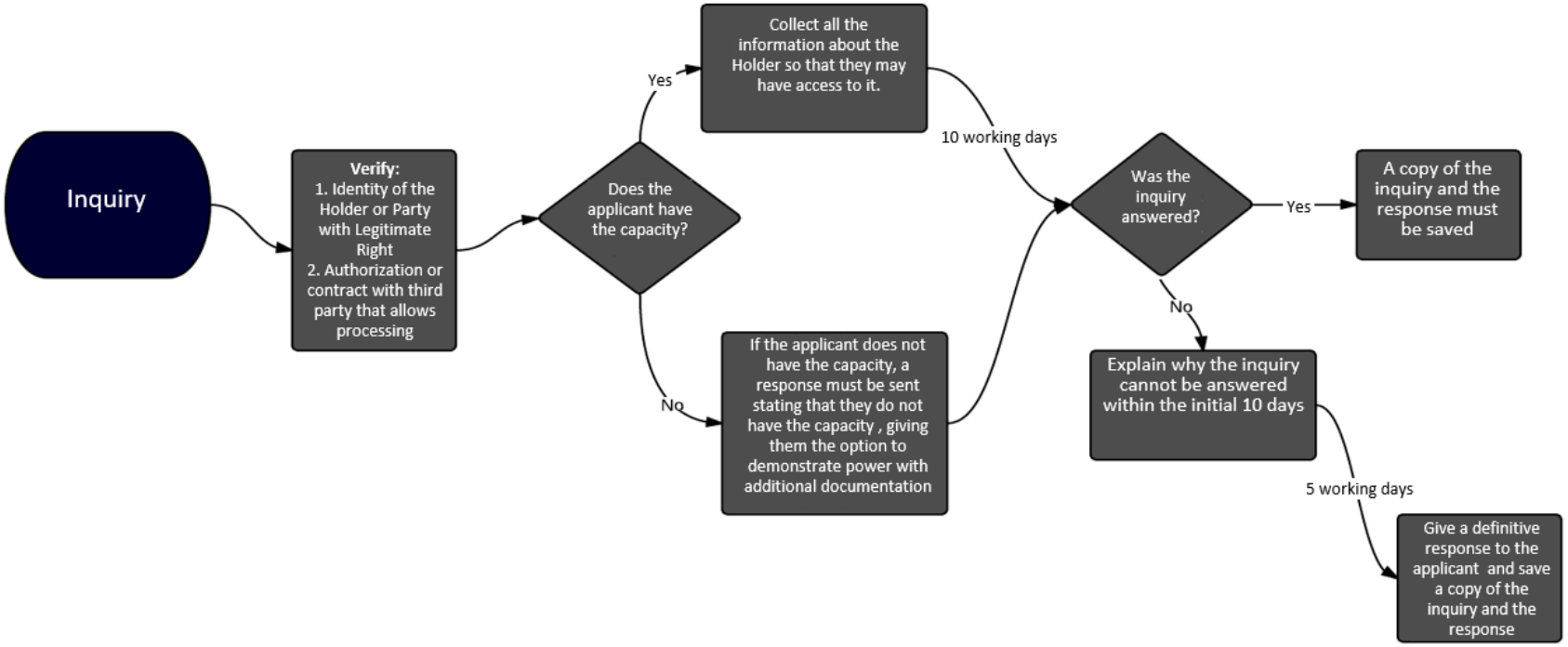
11. Modifications

The Company may modify this Policy from time to time and will be part of the contracts executed by the Company, where appropriate. Any substantial modification of this Policy will have to be previously notified to the Holders through the channels available to them, such as the Company's website and/or emails. Substantial modification means, among others, the following situations:

1. Modification in the identification of the area, office or person in charge of tending to inquiries and claims.
2. Clear modification of the purposes that may affect the Authorization. In this case, the Company will seek a new Authorization.

The modifications will be informed on the Company's website and/or via an email that will be sent to the Personal Data Holders, as long as the Company has that information in its possession.

1. ANNEX 1: FLOW CHART FOR INQUIRIES.



2. ANNEX 2: FLOW CHART FOR CLAIMS