PERSONAL DATA PROTECTION POLICY

Version: V. 2023-02
Approved on: September 15th , 2021
Approved by: Chief Executive Officer
Owner: Director of Finance & Compliance Committee
Next update due: September 15, 2024

PERSONAL DATA PROTECTION POLICY

Through this document, BIOENA SAS., in compliance with the regulatory requirements indicated in Law 1581 of 2012, Regulatory Decree 1377 of 2013 and the other concordant regulations on the matter, implements its Policy for the Treatment and Protection of Personal Data (hereinafter the "Policy").

For these purposes, it is important to consider that the Company is a commercial corporation, registered in the city of Bogotá, Colombia and it is dedicated to producing and selling renewable fuels.

Due to the foregoing and taking into account what is determined by the corporate purpose of the Company, it is possible to determine that there is personal data that make up databases owned by the Company. These are treated according to the established guidelines in the current legal framework applicable in Colombia.

For all of the above, the Policy will be applied both to protect personal data and transactional information currently processed by the Company, as well as to protect those that may interact with the Company in the future and in the midst of the development of its commercial activity.

GENERAL PROVISIONS

1. **Identification of the person in charge.**

BIOENA SAS., is identified with NIT 901387859-9. Its main address is at Calle 81 No 11 - 68, Suite 202, Bogotá - Colombia. Its main Email is; contact@BIOENA.co and its website is www.BIOENA.co.

2. **Goal.**

For the purposes of this Policy, the Company is Responsible for the Processing of personal data by virtue of the collection it carries out directly. For this reason, the Policy has as its main objective, the definition and subsequent determination of all the issues related to the procedures, principles and security policies according to which the Company will guarantee the proper treatment of personal data that is collected in the development of its corporate purpose.

3. **Legal framework.**

The Policy was prepared in strict compliance with all the provisions of the current regulations on the matter, in this way, this document complies with the provisions of Articles 15 and 20 of the Political

Constitution of Colombia, in Law 1581 of 2012 by the which "general provisions for the protection of personal data are dictated", in Regulatory Decree 1377 of 2013 and in the other regulations that in the future may modify, regulate or add the applicable regulations regarding the Protection of Personal Data.

4. **Definitions.**

As provided in Article 3 of Decree 1337 of 2013 and Article 3 of Law 1581 of 2012, the following terms will be defined throughout the Policy:

File: Set of data recorded as a single unit storage, containing personal data.

Authorization: Prior, express and informed consent of the owner to carry out the processing of personal data, which is obtained at the time of data collection.

Privacy Notice: Verbal or written communication generated by the person in charge, addressed to the owner, for the treatment of their personal data, through which they are informed about the existence of the Information Treatment Policy that will be applicable to them, the form of access it and the purposes of the treatment that is intended to give personal data.

Database: Organized set of personal data that is subject to treatment.

Successor in title: Person who has succeeded another due to the death of the latter (heir).

Personal data: Any information linked or that can be associated with one or more specific or determinable natural persons.

Public data: It is the data that is not semi-private, private or sensitive. Data relating to the marital status of individuals, their profession or trade and their quality as a merchant or public servant are considered public data. Due to its nature, public data may be contained, among others, in public records, public documents, official gazettes and bulletins, and duly executed judicial decisions that are not subject to reservation.

Sensitive data: Sensitive data is understood as data that affects the privacy of the owner or whose improper use may generate discrimination, such as revealing racial or ethnic origin, political orientation, religious or philosophical convictions, membership in trade unions, organizations social, human rights or that promotes the interests of any political party or that guarantees the rights and guarantees of opposition political parties, as well as data related to health, sexual life, and biometric data.

in Charge of Treatment: Natural or legal person, public or private, that by itself or in association with others, performs the processing of personal data on behalf of the person responsible for Treatment.

Responsible for the Treatment: Natural or legal person, public or private, that by itself or in association with others, decides on the database and/or the treatment of the data contained therein.

Holder: Natural person whose personal data is subject to treatment.

Treatment: Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.

Transfer: The Transfer of data takes place when the person in charge and/or Person in Charge of the Processing of personal data, located in Colombia, sends the information or personal data to a receiver, who in turn is Responsible for the Treatment and is inside or outside from the country.

Transmission: Treatment of personal data that implies the communication of the same inside or outside the territory of the Republic of Colombia when its purpose is to carry out a treatment by the Manager, on behalf of the person in charge.

Deletion: This is the name given to the action that the owner of the personal data requests from the person in charge and/or in charge of the data, in exercise of the right that assists him of freedom and purpose regarding his information.

It is noted that the definitions included in this Policy were taken from the regulations in force to date, which regulates the due protection of personal data of natural persons against the circulation and treatment thereof.

5. **Beginning.**

By virtue of the provisions of current regulations, the Company has incorporated into the Policy, the general principles related to the processing of personal data. In this way, these principles have a general application that encompasses all the content of the Policy across the board. These fundamental principles are taken from Article 4 of Law 1581 of 2012.

6. **Validity and application.**

The Databases and the Policy will have an indefinite period of validity, in accordance with the duration of the Company's corporate purpose.

The Policy will apply to the treatment of the Databases in which the Company has the quality of person in charge and/or Manager, from the date of its publication, leaving without effect the other institutional provisions that are contrary to it.

Given the foregoing, any situation that is not covered in the Policy will be regulated in accordance with the General Regime for the Protection of Personal Data in force in Colombia and the other applicable regulations on the matter.

DUTIES OF THE RESPONSIBLE AND/OR IN CHARGE OF THE TREATMENT – RIGHTS OF THE HOLDERS OF THE INFORMATION

7. **Duties of the Company as Responsible for the Treatment.**

The Company will have the following duties in its capacity as Data Controller, which arise from the applicable legislation on the matter, without prejudice to all other duties provided for in the provisions that regulate or come to regulate.

- Guarantee the Owner, at all times, the full and effective exercise of their rights in relation to their personal data.
- Allow access to the information of the Holders only to the people authorized to have access to it.
- Rectify the information when it is incorrect and communicate what is pertinent.
- Request and keep a copy of the Authorization granted by the Holder for the Treatment of your personal data.
- Duly inform the Holder about the purpose of the collection and the rights linked to it, from the Authorization granted.
- Guarantee that the information is true, complete, accurate, updated, verifiable and understandable. In addition, prove at all times that the information must correspond to the personal data initially granted for the Treatment.
- Keep the information under physical and digital security conditions that prevent adulteration, loss, consultation, use or unauthorized or fraudulent access, in addition to any conduct regulated and sanctioned in the computer crime law.
- Timely update the information, thus attending to all the news regarding the Holder's data, in a term not less than five (5) business days from the receipt of the request.
- Implement all the necessary measures so that the information is kept up to date.
- Implement a data processing procedure regarding queries and claims that the Holders may make of it.
- Identify when certain information is under discussion by the Owner.
- Respect the security and privacy conditions of the Holder's information.
- Process queries and claims formulated in the terms indicated by law.
- Inform, at the request of the Owner, about the use given to their data.
- Comply with the requirements and instructions issued by the Superintendency of Industry and Commerce on the particular subject.
- Inform the data protection authority when there are violations of the security codes and there are risks in the administration of the Holders' information.
- Ensure the proper use of the personal data of children and adolescents, in those cases in which it is obtained with the express authorization of their legal representative, of the Treatment of their data.
- Use only data whose Treatment is previously authorized in accordance with the provisions of Law 1581 of 2012, Decree 1377 of 2013 and the other regulations that develop and complement the matter.

- Refrain from circulating information that is being controversial by the Holder and whose blocking has been ordered by the Superintendency of Industry and Commerce or any other public entity competent in this decision-making.
- Use the personal data of the Holder only for those purposes for which it is duly empowered and respecting in all cases the current regulations on the protection of personal data.

8. **I entrust the personal data of the Company to a third party.**

For the fulfillment of its corporate purpose, the Company may entrust the Processing of the personal data it possesses to a third party, so that the latter may carry out communication, promotion, marketing, notification, data updating, programs and special projects that allow, among others, the fulfillment of the following purposes both by physical and digital means:

- Celebration, subscription or maintenance of contractual relations with the Holders.
- Treatment of information required in labor and corporate matters of the Company.
- Confidential, privacy and non-disclosable information.
- Compliance with the purpose of the service as a provider.

All of the above, always respecting the purposes that the Holder of the information has authorized to the Company or authorized by the Ministry of Justice.

The Person in Charge of the Treatment of any of the Databases delivered or shared by the Company, must comply with the following Duties:

- Guarantee the Holder, at all times, the full and effective exercise of the right of habeas data.
- Update the information reported by the Company within five (5) business days from its receipt.
- Timely update, rectify or delete the data in the terms established by law.
- Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.
- Process the queries and claims made by the Holders in the terms indicated in the Law.
- Register in the Databases the legends "claim in process" in the manner in which it is regulated in the regulations regarding the Treatment of personal data.
- Insert in the Database the legend "information under judicial discussion" once notified by the competent authority about judicial processes related to the quality of personal data.

- Adopt an internal policy of procedures to guarantee adequate compliance with the regulations regarding the Processing of personal data and, in particular, for the attention of queries and claims by the Holders.
- Allow access to information only to people who can have access to it.
- Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.
- Refrain from circulating information that is being controversial by the Holder and whose blocking has been ordered by the Superintendence of Industry and Commerce.
- Inform the Superintendence of Industry and Commerce when there are violations of the security codes and there are risks in the administration of the information of the Holders.

9. **Rights of the holders of personal data.**

In accordance with the Law applicable to the protection of personal data, the following are the rights of the Holders who have authorized the Processing of their data to the Company:

- Access, know, update, rectify and delete their personal data against the Company in its condition of Responsible.
- Submit to the Superintendency of Industry and Commerce, complaints for violations of the provisions of Law 1581 of 2012, prior consultation or request before the Company.
- Request proof of the Authorization granted by the Owner of the data or by the Data Controller to the Company, by any valid means.
- Be informed by the Company, upon request, regarding the use that it has given to your Personal Data.
- Revoke the Authorization or request the Deletion of the data when the principles, rights and constitutional and legal guarantees are not respected in the Treatment.
- Free access to your Personal Data that has been subject to Treatment by the Company as responsible for them.

The Company acknowledges that the personal data found in its Databases belongs to the Owner who authorized its Treatment.

INFORMATION PROCESSING

10. **Collection Channels.**

The Owner may authorize the Company to execute the Processing of their personal data through different means, among them are the following:

- Physical documents;
- Electronic documents;
- data message;
- Internet;
- Websites;
- Any other format that in any case allows the consent of the Holder through unequivocal behaviors through which it is possible to conclude that if it had not been supplied by the Holder, or the person entitled to do so, the data would not have been stored or captured in the Database.

The Authorization will be requested by the Company prior to the Processing of personal data.

11. **Mechanisms for capturing personal data.**

The Company carries out the collection of Personal Data by the mechanisms that are stated and defined below:

- **Virtual:** Mechanism through which the Company, using previously enabled non-face-to-face technological means (Web Page and Official Accounts on Social Networks), collects data personally, according to the established formats.
- **Written:** It is the means through which, physically and in person, the Company in the development of its corporate purpose, will carry out the collection of personal data, through the information provided in documents of incorporation or modification of the shareholding composition of the company. , in contracts with Suppliers, in contracts with employees, in candidate resumes and in recruitment forms in owned establishments or those operated by third parties.

12. **Information capture fields.**

In development of the principles of protection of habeas data, the collection of personal data will be limited to those that are pertinent and adequate for the purpose for which they are collected or required by the Company.

13. **Authorization for use of personal data.**

The Company acting as Responsible for the Processing of personal data and Transactional Information, obtains from the Owners of the data their clear, express, prior, informed and error-free

Authorization, through electronic forms, data collection formats and/or through the other means available or may be available for this purpose.

For the above, the Company will request the Owners of the personal data and the Transactional Information, their Authorization, informing them of the purpose for which the Treatment of their personal data will be provided. The foregoing, except in cases expressly authorized by law, which are regulated in article 10 of Law 1581 of 2012.

14. **Revocation of Authorization**

All Holders of personal data may at any time revoke their Authorization granted to the Company for the Treatment of your personal data and even request the Company to delete or eliminate your personal data contained in its Databases. The foregoing, as long as said conduct does not contravene a current legal or contractual provision.

The Company will guarantee the Holder easy access to these requests, establishing simple and straightforward mechanisms that allow the Holder to revoke his Authorization or request the deletion of his personal data, at least by the same means by which he initially granted them.

For the above procedure, the Holder must take into account that the revocation of consent may be expressed in whole or in part in relation to the authorized purposes. (i) If it is totally revoked, the Company must cease any Data Processing activity provided by the Holder; on the contrary (ii) if it is partially revoked only in the face of certain types of Treatment, the Company will cease the treatment for the purposes that were expressly revoked by the Owner. In the latter case, the Company may continue to process personal data for those purposes that were not revoked.

15. **Treatment to which the data will be submitted and its purpose.**

All Treatment of the data of the Holders with whom the Company has established a relationship as Responsible for the Treatment and of the Transactional Information for the offer of value-added services, will be carried out by the Company based on the prescriptions of Law 1581 of 2012 and Law 1266 of 2008 as applicable, and in general for the fulfillment of its corporate purpose.

In any case, the Company will collect and process the personal data of the Holders, with the purpose of executing certain purposes, which vary according to the Database, as described below:

Payroll:

- Advance selection processes.
- Develop and execute the employment relationship if it is concluded.
- Send information by any known or unknown means (email, physical mail, SMS, telephone calls, data messages, among others) about selection processes, execution of

employment contracts, disabilities, payments, campaigns, information on products and services, notifications of activities, promotions, offers and launches.

- Carry out educational and training programs and activities.
- Conduct evaluations and performance appraisals.
- Issue labor and/or commercial references when the Holder requires it.
- Validate the labor and/or commercial references that the Holder had provided.
- Provide personal information of a commercial nature, for the execution of contractual relations acquired by the Company with third parties.
- Update personal data.
- Consult, report, process and disclose all the information that refers to its financial, commercial and service behavior, to any Information Operator (Risk Center) or to any entity or source of public or private, national, foreign or multilateral information. that administers or manages databases, for commercial purposes and credit services.
- Advance procedures for linking to the social security system.
- Perform biometric data processing for the implementation and use of entry and security systems that require biometric authentication.

Purchases, payments and accounting:

- Establishment of communication channels with the Holder, through email, telephone calls, sending SMS or any communication channel known or to be known, provided that it is authorized by the Holder.
- Create and track purchase orders.
- Manage payment to suppliers.
- Analyze information for statistical purposes.
- Provide personal information of a commercial nature, for the execution of contractual relations acquired by the Company with third parties.
- Request proposals and quotes.
- Address claims.
- Contact potential suppliers or current suppliers for purchases and contracting.
- Send and request information on the performance of products.
- Update personal data.
- Assess quality of contracted products and services.
- Carry out marketing and advertising activities related to the corporate purpose of the Company.
- Consult, report, process and disclose all the information that refers to its financial, commercial and service behavior, to any Information Operator (Risk Center) or to any entity or source of public or private, national, foreign or multilateral information. that administers or manages databases, for commercial purposes and credit services.

- Analyze, evaluate and consult the information provided by the Holder in lists for the control of money laundering and financing of terrorism managed by any national or foreign authority.

Commercial:

- Establishment of communication channels with the Holder, through email, telephone calls, sending SMS or any communication channel known or to be known, provided that it is authorized by the Holder.
- Grant incentives to customers, with the aim of boosting sales, through discounts, gifts, bonuses, or any activity associated with customer loyalty.
- Carry out studies of transactional behaviors, consumption habits and hobbies, for the offer of own services and those of third parties, or of future allies, for the execution of segmented strategies.
- Carry out customer service procedures and their claims of all kinds.
- Run Campaigns to update personal data and commercial campaigns.
- Coordinate, execute and promote strategic campaigns of the Company and the offer of services.
- Execute surveys for customer knowledge.
- Sending Commercial Campaigns.
- Prepare sales invoices.
- Share with allied companies, associates, branches, franchises, affiliates and subsidiaries, and third parties with whom they have signed personal data processing agreements for the offer of value-added services.
- Provide personal information of a commercial nature, for the execution of contractual relations acquired by the Company with third parties.
- Consult, report, process and disclose all the information that refers to its financial, commercial and service behavior, to any Information Operator (Risk Center) or to any entity or source of public or private, national, foreign or multilateral information. that administers or manages databases, for commercial purposes and credit services.
- Analyze, evaluate and consult the information provided by the Holder in lists for the control of money laundering and financing of terrorism managed by any national or foreign authority.
- Invite the Holders to participate and/or assist in training programs, logistics coordination, sales or any other topic developed or related to the corporate purpose of the Company.

Shareholders:

- Establishment of communication channels with the Holder, through email, telephone calls, sending SMS or any communication channel known or to be known, provided that it is authorized by the Holder.
- Control of the register of shareholders of the Company and the exercise of their rights.
- Control of the Company's Shareholders' Registry Book.
- Provision and delivery of information on payment of dividends or profits.
- Analyze, evaluate and consult the information provided by the Holder in lists for the control of money laundering and financing of terrorism managed by any national or foreign authority.

16. **Treatment of data of children and adolescents.**

In the Processing of personal data, the Company will ensure respect for the prevailing rights of minors (boys, girls, and adolescents). For this reason, in the event of any collection of personal data corresponding to this type of person, the provisions of article 7 of Law 1581 of 2012 and the other concordant provisions on the matter will be complied with.

17. **Processing of sensitive personal data**

The Company knows that it performs Processing on personal data that are sensitive, so it will ensure that, at the time of collecting personal data of this type, it will comply with the provisions of Article 6 of Decree 1377 of 2013 and the other concordant provisions on the matter.

SECURITY MEASURES

The Company, in compliance with its purpose of guaranteeing the care of the personal data of third parties, obtained through the Channels authorized by this Policy, has arranged a set of security measures which will be used and implemented seeking an adequate protection of all the information that is subject to Treatment.

With the foregoing, it is reasonably considered that the Company has adequate and sufficient document management and information protection models to adequately comply with its legal obligations in relation to the care and custody of information provided by third parties.

18. **Safety procedures.**

The Company, seeking to achieve adequate protection of the information subject to the Policy, has deployed various security mechanisms to guard and prevent any deterioration, loss or leak that may occur in the information contained in its Databases.

One of them is related to the location of the Database, which is in the cloud (Google Drive), with the proper access controls, among which are:

- A logical security model that allows restricting the users who have data access.

PROCEDURES FOR THE ATTENTION OF INQUIRIES AND CLAIMS.

19. **Care channels.**

For the attention of queries and claims related to the Treatment of Personal Data, they may be formulated through the following email, **contacto@bioena.co**

20. **Procedure to file a query.**

When the Holder of the personal data intends to know, access the information, or request a copy of the Authorization, the area will resolve his query within ten (10) business days following the date of receipt of the same.

When it is not possible to attend the query within the term indicated in the previous paragraph, the applicant will be informed of such situation, the reasons for the delay and the date on which the request will be resolved, a date that in no case will exceed five (5) business days following the expiration of the first term.

21. **Procedure for filing a claim.**

When the Holder of the personal data intends to rectify, update, delete any of his data or revoke his Authorization, the Customer Service area will resolve his claim within fifteen (15) business days following the date of receipt of the same.

When it is not possible to attend the query within the term indicated in the previous paragraph, the applicant will be informed of such situation, the reasons for the delay and the date on which the request will be resolved, a date that in no case will exceed eight (8) business days following the expiration of the first term.

22. **response medium.**

The Company will respond to the inquiries and claims of the Holders, within the terms established in numerals 22 and 23 of this Policy, in writing to the physical or electronic address provided by the applicant for that purpose.

When the applicant provides a physical address and an electronic address, or more than one address of those or of these, it will be at the discretion of the Company the decision on which address to send the response.

23. **Persons entitled to file a query or claim.**

In accordance with the regulations applicable to the matter, the following persons are entitled to file a query or a claim with the Company:

- The Holders of the personal data.
- The successors of the Holders.
- The legal representatives.
- Public or administrative entities in the exercise of their legal functions or by court order.
- Third parties authorized by the Owner or by law.

24. **Updating of databases.**

The Company will update its Databases permanently, in accordance with the provisions of Law 1581 of 2012.

25. **Data transfers for treatment by third parties, national and international.**

The Company may partially or totally transmit or transfer Personal Data and transactional information to third parties in the country or abroad, in the development of its corporate purpose, for which it requests Authorization from its Owner and implements the necessary actions to compliance with the regulatory precepts enshrined in Colombian National legislation, through the signing of Personal Data Transfer and Treatment Agreements.

26. **Security of the information.**

The Company has an Information Security Policy, which is an integral part of this Policy.

27. **Procedure for modifications to this Policy.**

Of each decision that determines the need to make any modification to this Policy, a written record signed by the members will be left.

Any modification that complies with the previously determined procedure will become part of this Policy and therefore will be mandatory and immediate compliance.

29. **Validity.**

This Policy will take effect from the date of its publication and will leave without effect the other institutional provisions that are contrary to it. Any element on the subject matter of this Policy that is not contained in it, will be regulated according to the General Regime for the Protection of Personal Data in force in the Republic of Colombia.