

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

1. INTRODUCTION	3
2. SCOPE	3
3. DEFINITIONS	3
4. PROCESSING OF PERSONAL DATA AND PURPOSES OF COLLECTION	4
4.1. PROCESSING OF PERSONAL DATA OF EMPLOYEES	4
4.2. PURPOSES OF EMPLOYEES DATA	4
4.3. PROCESSING OF PERSONAL DATA OF CUSTOMERS.....	5
4.4. CUSTOMER PURPOSES:.....	5
4.5. PROCESSING OF PERSONAL DATA OF SUPPLIERS	5
4.6. SUPPLIER PURPOSES	5
4.7. PROCESSING OF PERSONAL DATA OF CANDIDATES.....	6
4.8. CANDIDATES PURPOSES	6
4.9. PROCESSING OF PERSONAL DATA OF VISITORS.....	6
4.10.PURPOSES OF VISITORS.....	6
5. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA.....	6
6. RIGHTS OF PERSONAL DATA OWNERS.....	7
6.1. THESE RIGHTS MAY BE EXERCISED BY:.....	8
6.2. RIGHTS OF CHILDREN AND ADOLESCENTS	8
7. AUTHORIZATION OF THE OWNER.....	8
8. DUTY TO INFORM THE OWNER	9
9. PERSONS TO WHOM THE INFORMATION MAY BE PROVIDED.....	9
10. RIGHT OF ACCESS AND CONSULTATION	9
10.1.RIGHT TO COMPLAINTS AND CLAIMS	9
10.2.EXERCISE OF THE RIGHTS OF THE OWNERS	10
10.2.1. RIGHT OF ACCESS	10
11. PROCEDURE TO ADDRESS THE RIGHTS OF THE OWNERS.....	10
11.1.CONULTATION PROCEDURE:.....	10
11.2.RESPONSIBLE FOR HANDLING INQUIRIES:.....	10
11.3.RESPONSE TIMES TO INQUIRIES:.....	11
11.4.EXTENSION OF THE RESPONSE DEADLINE:.....	11
12. COMPLAINTS PROCEDURE.....	11
12.1. RIGHTS GUARANTEED THROUGH THE CLAIMS PROCEDURE:	11
12.2.MINIMUM INFORMATION THAT CLAIMS MUST CONTAIN:	11
13. RIGHT TO UPDATE, RECTIFICATION AND DELETION.....	12



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

14. SPECIAL DATA CATEGORIES 12
 14.1.1 PROCESSING OF SENSITIVE DATA EMPLOYED..... 13
 14.1.2 PROCESSING OF SENSITIVE CUSTOMER DATA 13
 14.1.3 PROCESSING OF SENSITIVE BIOMETRIC DATA..... 13
15. ATTENTION TO DATA OWNERS..... 13
16. DUTIES OF NEW STETIC AND THOSE IN CHARGE OF DATA PROCESSING..... 14
 16.1. NEW STETIC DUTIES:..... 14
 16.2.DUTIES OF THOSE IN CHARGE: 14
17. SECURITY MEASURES 15
18. INCIDENT MANAGEMENT WITH PERSONAL DATA 15
19. MANAGEMENT OF RISKS ASSOCIATED WITH DATA PROCESSING 15
20. TRANSFER OF DATA TO THIRD COUNTRIES..... 16
21. NATIONAL DATABASE REGISTRY 16
22. PROTECTION, SECURITY AND CONFIDENTIALITY OF INFORMATION AND DATA 16
23. SCOPE OF APPLICATION 17
24. VALIDITY 17



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

NEW STETIC PERSONAL DATA PROTECTION POLICY

1. INTRODUCTION

NEW STETIC SA, adopts this Data Protection policy in order to comply with the provisions of Statutory Law 1581 of 2012, its Regulatory Decree 1377 of 2013 and other concordant regulations, in order to guarantee the right to intimacy, privacy and the good name of individuals in the processing of their personal data, which will be carried out taking into account the principles of legality, purpose, freedom, veracity or quality, transparency, restricted access and circulation, security and confidentiality.

The company is committed to safeguarding information and complying with data protection regulations and the obligations arising therefrom, processing data responsibly and in accordance with the consent of the owner, to act with prudence and confidentiality.

2. SCOPE

This policy applies to all databases and/or files of NEW STETIC that contain Personal Data and that are processed by the controller and/or processor.

The company processes personal data under the terms, conditions and scope authorized by the owner of the information, except for special regulations when a legal exception is applicable to doing so.

3. DEFINITIONS

Personal information: This is any information that is linked to or can be associated with a specific person, such as their name or identification number, or that can make them identifiable, such as their physical characteristics.

Public data: Public data includes, among others, data relating to the civil status of persons, their profession or occupation, and their status as merchants or public servants. By their nature, public data may be contained in, among others, public registers, public documents, official gazettes, and bulletins, and duly executed court decisions that are not subject to confidentiality.

Semi-private data: These are data that are not of an intimate, reserved, or public nature and whose knowledge or disclosure may be of interest not only to the owner but also to a certain sector or to society in general. Financial and credit data from commercial or service activities are some examples.

Private data: This is data that, due to its intimate or reserved nature, is only relevant to the data subject. The tastes or preferences of individuals, for example, correspond to classified data.

Sensitive data: These are those that affect the privacy of the holder or may lead to discrimination, that is, those that reveal his or her racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social organizations, human rights organizations, as well as data relating to health, sexual life, and biometric data, among others.

Authorization: It is the consent given by any person so that companies or persons responsible for processing information can use their personal data. Database Organized set of personal data that are subject to processing.

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

Data controller: It is the natural or legal person who carries out the processing of personal data, based on a delegation made by the person responsible, receiving instructions about the way in which the data should be managed.



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

Data controller: The natural or legal person, public or private, who decides on the purpose of the databases and/or their processing. Owner: The natural person whose personal data is being processed.

Privacy Notice: It is one of the verbal or written communication options provided by law to inform the holders of the information of the existence and the ways to access the information processing policies and the purpose of its collection and use.

Transfer: This is the operation carried out by the person responsible for or in charge of processing personal data, when he sends the information to another recipient, who, in turn, becomes responsible for the processing of said data and is located within or outside the country.

Transmission: processing of personal data that involves the communication of the same within or outside the territory of the Republic of Colombia when its purpose is to carry out processing by the person in charge on behalf of the person responsible.

4. PROCESSING OF PERSONAL DATA AND PURPOSES OF COLLECTION

4.1. PROCESSING OF PERSONAL DATA OF EMPLOYEES

NEW STETIC, carries out the processing of your personal and sensitive data, which includes the collection, storage, use, circulation, transmission, updating, rectification, and deletion, for the following purposes:

4.2. PURPOSES OF EMPLOYEES DATA

- Comply with the obligations arising from the employment relationship, agreements, and/or service provision contracts.
- Manage procedures, requests, certification of documents, communicate information, registration of income, updating information, training and other administrative procedures and activities in which employees, retirees, and their families (spouse, permanent partner, children, parents, siblings or other relatives and personal references) are related or linked with NEW STETIC.
- Collect information for company events or communications through photographic records, videos that include employees and family members.
- Carry out administrative management, provide information for affiliation to social security, cash register compensation, photographic registration, and company events for minors.
- Contact family members in case of emergency or any eventuality that requires it.
- Keep medical records for employee follow-up and/or procedures with competent ARL medical personnel.
- Evaluate the qualification to perform a position or function, validate study certificates, confirm references, and communicate available positions.
- Communicate personal data to temporary companies when their employment relationship.
- Contact through electronic means, cell phone or mobile device, physical and/or personal, or through any analog and/or digital means of communication, known or unknown, to send information.
- Manage through electronic and/or physical means, digital platforms, Apps, devices, mobile phones, or any analogue and/or digital means of communication, known or unknown, information to control attendance and/or stay at NEW STETIC facilities, health status, reports, and other procedures necessary to comply with legal obligations.
- Transmit personal data to national third parties.
- Collect biometric data, through recordings or video surveillance systems for identification, security, and internal and external monitoring.
- Use their image in company media.
- Conduct tests to detect alcohol, drug, and other addictions prior to hiring, when there is justifiable suspicion, and randomly when deemed necessary.
- Carry out the relevant promotion and employment management procedures (resume validation,

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

- psychotechnical tests, background checks and security studies).
- Conduct home visits and pre-employment safety assessment.
- Conduct due diligence on compliance systems; consult your information on restrictive lists and public or private databases, directly or indirectly related to money laundering, financing of terrorism, corruption, fraud, bribery, transnational bribery, and other illicit activities of any kind.

4.3. PROCESSING OF PERSONAL DATA OF CUSTOMERS

The company will collect, store, and use the personal data of its customers for the following purposes:

4.4. CUSTOMER PURPOSES:

- Carry out the relevant procedures for the development of the company's corporate purpose in relation to compliance with the purpose of the contract and/or commercial relationship with the Owner of the information.
- Send you commercial, advertising, or promotional information about products and/or services, through electronic means including; email, SMS, and WhatsApp, or by telephone to carry out campaigns, promotions or contests of a commercial or advertising nature, as well as to inform you about events organized by the company, about the products, manage procedures (requests, complaints and claims) and to ask you to evaluate the quality of our products and/or services.
- Provide contact information to the sales force and/or distribution network, telemarketing, market research, and any third party with which NEW STETIC SA has a have a contractual link for the development of activities of this type (market research and telemarketing, etc.) for the execution thereof.
- Contact the Owner through electronic means, including email, SMS, and WhatsApp or by telephone to carry out surveys, studies, and/or confirmation of personal data necessary for the execution of a contractual and/or commercial relationship.
- Contact the Owner through electronic means; including email, SMS, and WhatsApp or by telephone to send news related to loyalty campaigns or service improvements.
- Contact the Owner through electronic means; including email, SMS, and WhatsApp or by telephone to send account statements or invoices in relation to the obligations arising from the contract entered between the parties and debt collection management.
- Transmit personal data outside the country to third parties with whom NEW STETIC SA has signed a data processing contract, and it is necessary to provide it to you for the fulfillment of the contractual purpose.
- Provide the services offered by NEW STETIC SA and accepted in the signed contract.
- Collect and use their image in photographs and videos, for advertising, internal and external company events, communications, and social networks.
- Registering the sale of controlled substances; filing complaints as a victim; control over the sale of acids, alkalis, and corrosive substances; reversal of transactions under Consumer Protection regulations; security protocols, the execution of transaction contracts to prevent litigation, among others.

4.5. PROCESSING OF PERSONAL DATA OF SUPPLIERS

NEW STETIC SA will be responsible for the collection, storage, and use of the personal data of its suppliers for the following purposes:

4.6. SUPPLIER PURPOSES

- Comply with the obligations arising from the legal relationship established with the supplier.

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

- Integrate your file as a supplier of the organization.
- Make requests for the service or products you provide.
- Prepare purchase orders for goods and services.
- Evaluate the performance, level of compliance and quality of the services or products provided.
- Monitoring of own vehicles (merchandise).
- Sending invoices, payments, and certificates.
- Record of internal procedures and compliance with accounting, tax, and legal obligations.
- Request commercial references, information updates and internal control.
- Perform supplier qualification, assurance (purchase orders) and audits.
- Management of indicators and legal advice on contracts.
- Information in which contractors and their employees are related or linked to NEW STETIC SA

4.7. PROCESSING OF PERSONAL DATA OF CANDIDATES

Within the personnel selection processes, personal data is processed in the collection, storage, use, circulation, transmission, updating, rectification, and deletion.

4.8. CANDIDATES PURPOSES

- Carry out the relevant promotion and employment management procedures (resume validation, psychotechnical tests, background checks and security studies).
- Conduct home visits and pre-employment safety assessment.
- Consult your information on restrictive lists and public or private databases, directly or indirectly related to money laundering or financing of terrorism, corruption, bribery, and illegal activities of any kind.

4.9. PROCESSING OF PERSONAL DATA OF VISITORS

When visitors access the company, we seek to maintain a record and control of entries where personal data may be collected, stored, and used.

4.10. PURPOSES OF VISITORS

- Identification and verification of visitor data, security control, entry and exit records and administrative management.

5. PRINCIPLES FOR THE PROCESSING OF PERSONAL DATA

For an appropriate application of the law, compliance with the following principles will be fundamental:

Principle of purpose: The purpose of the Treatment must obey a legitimate purpose in accordance with the Constitution and the Law, which must be communicated to the Owner of the information.

Principle of legality in data processing: The Treatment referred to in this law is a regulated activity that must be subject to the provisions established therein and in other provisions that develop it.

Principle of Freedom: Data processing may only be carried out with the prior, express, and informed consent of the Data Subject. Furthermore, the collection and disclosure of personal data may not be carried out without prior authorization and will only be permitted through a legal or judicial order that waives consent.

Principle of truthfulness or quality: Data that are subject to processing must be true, complete, accurate, up-to-date, verifiable, and understandable. Partial, incomplete, fragmented, or misleading data may not be processed.

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

Transparency principle: The controller or processor must guarantee without restrictions the right to obtain information about the existence of data that concerns him/her.

appropriate, reporting clearly and expressly and keeping proof of compliance with this duty:

- The treatment to which your data will be subjected and the purpose thereof.
- The optional nature of the Owner's response to questions asked when these concern sensitive data or data of children or adolescents.
- The rights that assist you as Owner.
- The identification, physical address, email, and telephone number of the person responsible for the treatment.

Principle of restricted access and circulation: The processing of personal data may only be carried out by persons authorized by the owner and/or by persons provided for in Law 1581 of 2012. The processing is subject to the limits arising from the nature of the personal data, the provisions of this law and the Constitution. Personal data, except for public information, 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 the Owners or authorized third parties in accordance with this law.

Safety principle: The information subject to processing by NEW STETIC SA or the Data Processor is processed under the technical, human, and administrative measures necessary to ensure the security of the records, avoiding their alteration, loss, consultation, unauthorized or rapid access or use. The company will ensure that it has all the corresponding security measures and that they are made known to all persons who have direct or indirect access to the data. Users who access the NEW STETIC SA information systems must be aware of and comply with the security rules and measures that correspond to their functions. These security rules and measures are included in the Internal Security Manual, which is mandatory for all users and company personnel. Any modification of the rules and measures regarding the security of personal data by the data controller must be made known to users.

Confidentiality principle: All persons involved in the processing of personal data that are not public in nature are obliged to guarantee the confidentiality of the information, even after their relationship with any of the tasks that comprise the processing has ended, and may only provide or communicate personal data when this corresponds to the development of the activities authorized in this law and under the terms thereof.

6. RIGHTS OF PERSONAL DATA OWNERS

The following are the rights of the holders of personal data, which can be exercised at any time as stipulated in Law 1581 of 2012:

- Right to know, update and rectify your personal data vis-à-vis those responsible for the processing or those in charge of the processing. This right may be exercised, among others, in the case of partial, inaccurate, incomplete, fragmented data that may lead to error, or data whose processing is expressly prohibited or has not been authorized.
- Right to request proof of the authorization granted to the person responsible for the Treatment, except when it is expressly excepted as a requirement for the Treatment, in accordance with the provisions of article 10 of law 1581 of 2012.
- Right to be informed by the Data Controller or the Data Processor, upon request, regarding the use that has been given to your personal data.
- Right to file complaints with the Superintendency of Industry and Commerce for violations of the provisions of this law and other regulations that modify, add to, or complement it.

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

- Right to revoke authorization and/or request the deletion of data when the Processing does not respect the constitutional and legal principles, rights and guarantees. Revocation and/or deletion will proceed when the Superintendence of Industry and Commerce has determined that in the Processing the controller or the Processor has engaged in conduct contrary to this law and the Constitution.
- Right to access free of charge your personal data that have been subject to processing.

6.1. THESE RIGHTS MAY BE EXERCISED BY:

- The owner is the one who must prove his identity sufficiently by the different means made available to him by NEW STETIC SA
- The successors in title of the owner, who must prove such status.
- The representative and/or agent of the owner, upon prior accreditation of the representation or power of attorney.
- Another in favor of or for which the owner has stipulated.

6.2. RIGHTS OF CHILDREN AND ADOLESCENTS

The processing of personal data of children and adolescents is not permitted, except when it involves data of a public nature, and when such processing complies with the following parameters and/or requirements:

- That they respond to and respect the best interests of children and adolescents.
- Ensure that their fundamental rights are respected.

The legal representative of the children or adolescents will grant the authorization, after the minor has exercised his or her right to be heard, an opinion that will be assessed considering the maturity, autonomy, and ability to understand the matter, after having fulfilled the previous requirements.

7. AUTHORIZATION OF THE OWNER

To properly process personal data, NEW STETIC will require the prior and informed authorization of the Owner, which must be obtained by any means that can be subject to subsequent consultation, without prejudice to the exceptions provided for in the law. These mechanisms may be predetermined through technical means that facilitate the Owner's automated manifestation.

7.1. THE AUTHORIZATION WILL MEET THE REQUIREMENTS WHEN IT IS CARRIED OUT:

- In writing
- Through unequivocal conduct of the holder that allows us to conclude that he granted the authorization

7.2. IT WILL NOT BE NECESSARY TO HAVE AUTHORIZATION FROM THE OWNER, WHEN IT COMES TO:

- Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- Public nature data
- Cases of medical or health emergencies;
- Processing of information authorized by law for historical, statistical, or scientific purposes;
- Data related to the Civil Registry of Persons.

A record will be kept of the delivery of the requested personal information, indicating the obligation to guarantee the rights of the Holder, both to the official who makes the request, to the person who receives it, as well as to the requesting entity.



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

Anyone who accesses personal data without prior authorization must in all cases comply with the provisions contained in this law.

8. DUTY TO INFORM THE OWNER

When requesting authorization to process data, NEW STETIC, as the party responsible for said processing, will be responsible for clearly and expressly indicating the following:

- The processing to which your personal data will be subjected and its purpose.
- The optional nature of the response to the questions asked, when these relate to sensitive data or the data of girls, boys, and adolescents.
- The rights that assist you as Owner.
- The identification, physical or electronic address and telephone number of the person responsible for the Treatment.

In all cases it will be essential to keep proof of compliance with the provisions of the paragraph above, and in cases where the owner so requests, provide a copy of this.

9. PERSONS TO WHOM THE INFORMATION MAY BE PROVIDED

NEW STETIC may provide information to others when the conditions established in Law 1581 of 2012 are met:

- To the Holders, their successors in title or their legal representatives;
- To public or administrative entities in the exercise of their legal functions or by court order;
- To third parties authorized by the Owner or by law.

10. RIGHT OF ACCESS AND CONSULTATION

- The Data Subjects or their successors in title may consult the personal information of the Data Subject that is stored in any NEW STETIC database. The Data Controller or Data Processor must provide them with all the information contained in the individual record or that is linked to the identification of the Data Subject.
- The query will be made through the means enabled by the company to maintain proof of this.
- The query will be answered within a maximum period of ten (10) business days from the date of receipt of the same. When it is not possible to answer the query within said period, the interested party will be informed, stating the reasons for the delay and indicating the date on which the query will be answered, which in no case may exceed five (5) business days following the expiration of the first period.

10.1. RIGHT TO COMPLAINTS AND CLAIMS

When it is considered that the information contained in a database should be corrected, updated, or deleted, or when they notice the alleged non-compliance, the Owner or his successors may file a claim with NEW STETIC, which will be processed under the following rules:

- The claim will be made by means of a request addressed to the company with the identification of the Holder, the description of the facts that give rise to the claim, the address, and accompanying the documents that you wish to assert. If the claim is incomplete, the interested party will be required within five (5) days following receipt of the claim to correct the deficiencies. After two (2) days, the claimant will be required to correct the deficiencies.
(2) months from the date of the request, if the applicant does not submit the required information, it will be understood that he has withdrawn the claim.

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

- If the person receiving the claim is not competent to resolve it, he/she will forward it to the appropriate person within a maximum period of two (2) business days and will inform the interested party of the situation.
- Once the complete claim has been received, a legend stating "claim in process" and the reason for the claim will be included in the database within a period of no more than two (2) business days. This legend must be maintained until the claim is decided.
- The company will have a maximum term of fifteen (15) business days to address the claim, counted from the day following the date of receipt. When it is not possible to address the claim within said term, the interested party will be informed of the reasons for the delay and the date on which the claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.

Only the Owner or successor in title may file a complaint with the Superintendency of Industry and Commerce once he or she has exhausted the consultation or claim process with the Data Controller or Data Processor.

10.2. EXERCISE OF THE RIGHTS OF THE OWNERS

10.2.1. RIGHT OF ACCESS

NEW STETIC will maintain mechanisms that are always available and that are simple and agile when accessing your personal data information so that you can exercise your rights over it. In addition, you may consult your personal data free of charge in two cases:

1. At least once every calendar month,
2. Whenever there are substantial modifications to the Information Processing Policies that motivate new consultations.

For queries that are more frequent than once per calendar month, NEW STETIC SA may only charge the holder the costs of shipping, reproduction and, where applicable, certification of documents. Reproduction costs may not be greater than the costs of recovering the corresponding material. For this purpose, the person responsible must demonstrate to the Superintendence of Industry and Commerce, when required, the support for said expenses.

The requested information may be provided by any means, including electronic means, as required by the Owner. The information must be easy to read, without technical barriers that impede access and must correspond in all respects to that which is stored in the database.

11. PROCEDURE TO ADDRESS THE RIGHTS OF THE OWNERS

11.1. CONSULTATION PROCEDURE:

NEW STETIC and/or the Managers, guarantee the holders of personal data contained in their databases, their successors in title or authorized persons, the right to consult all the information contained in their individual record or all that is linked to their identification as established in this Personal Data Processing Policy.

11.2. RESPONSIBLE FOR HANDLING INQUIRIES:

The company's Personal Data Protection Officer will be responsible for receiving and processing the requests submitted, under the terms, deadlines and conditions established in Law 1581 of 2012 and in this policy.

Minimum information that must be contained in queries addressed to the company:

1. Name and surname of the Owner.



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

2. Photocopy of the Citizenship Card of the Holder and, where applicable, of the person representing him/her, as well as the document proving such representation.
3. Petition specifying the request for access or consultation.
4. Address for notifications, date, and signature of the applicant.
5. Documents supporting the request made, where applicable.

Once the request for INFORMATION CONSULTATION is received by the Data Owner or his/her representative or duly authorized third party, through the channels established by NEW STETIC, the Personal Data Protection Officer will verify that the request contains all the specifications required in order to assess whether the right is exercised by an interested party or by a representative thereof, thereby proving that there is legal legitimacy to do so.

11.3. RESPONSE TIMES TO INQUIRIES:

Requests received through the above means will be attended to within a maximum period of ten (10) business days from the date of receipt.

11.4. EXTENSION OF THE RESPONSE DEADLINE:

In the event of impossibility to respond to the query within said term, NEW STETIC will inform the interested party before the expiration of ten (10) days, stating the reasons for the delay and indicating the date on which the query will be responded to, which in no case may exceed five (5) business days following the expiration of the first term.

12. COMPLAINTS PROCEDURE

12.1. RIGHTS GUARANTEED THROUGH THE CLAIMS PROCEDURE:

Correction or Update: NEW STETIC and/or the Data Processors will guarantee the owners of personal data contained in their databases or their successors in title the right to correct or update the personal data contained in their databases, by submitting a claim, when they consider that the parameters established by law or those indicated in this Personal Data Processing Policy are met so that the request for Correction or Update is admissible.

Revocation of authorization or Deletion of Personal Data: NEW STETIC and/or the Data Processors shall guarantee the owners of personal data contained in their databases or their successors in title the right to request the revocation of the authorization or to request the deletion of the information contained in their individual record or any information linked to their identification when they consider that the parameters established by law or those indicated in this Personal Data Processing Policy have been met. Likewise, the right to file complaints is guaranteed when they notice the alleged non-compliance with Law 1581 of 2012 or this Personal Data Processing Policy.

Claims Attention: The company's Personal Data Protection Officer will be responsible for receiving and processing the requests submitted, under the terms, deadlines and conditions established in Law 1581 of 2012 and in these policies.

12.2. MINIMUM INFORMATION THAT CLAIMS MUST CONTAIN:

1. Name and surname of the Owner.
2. Photocopy of the Citizenship Card of the Holder and, where applicable, of the person representing him/her, as well as the document proving such representation.
3. Petition specifying the request for access or consultation.
4. Address for notifications, date, and signature of the applicant.
5. Documents supporting the request made, where applicable.

Once the request for information CLAIM is received by the Data Owner or his/her representative or duly authorized

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

third party, through the channels established by NEW STETIC, the Personal Data Protection Officer will verify that the request contains all the required specifications in order to assess whether the right is exercised by an interested party or by a representative thereof, thereby proving that there is legal legitimacy to do so.

Claims without compliance with legal requirements: If the claim is submitted without compliance with the above legal requirements, the company will request the claimant within the following five (5) days from receipt of the claim, to correct the deficiencies and present the missing information or documents.

Withdrawal of Claim: After two (2) months from the date of the request without the applicant submitting the required information, it will be understood that he has withdrawn the claim.

Reception of claims that do not correspond to the Entity: If the company receives a claim addressed to another organization, it will forward it to the appropriate party within a maximum period of two (2) business days and will inform the claimant of the situation.

Inclusion of legend in the database: Within a maximum of two (2) business days from receipt, the company will include in the database where the personal data of the Holder is located, a legend that says "claim in process" and the reason for it. This legend must be maintained until the claim is decided.

Response Deadlines for Claims: The maximum term to address the claim will be fifteen (15) business days counted from the day following the date of receipt.

Extension of the Response Deadline: When for any reason it is not possible to address the claim within said term, the interested party will be informed of the reasons for the delay and the date on which his claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.

Procedure for Deletion of Personal Data: When the Deletion of the personal data of the owner of the database is appropriate according to the claim presented, the company must operationally carry out the deletion in such a way that the elimination does not allow the recovery of the information; however, the Owner must take into account that in some cases certain information must remain in historical records due to compliance with the legal duties of the organization, so its deletion will be in response to the active processing of the same and in accordance with the request of the owner.

13. RIGHT TO UPDATE, RECTIFICATION AND DELETION

In compliance with the principle of truthfulness or quality, in the processing of personal data, reasonable measures must be adopted to ensure that the personal data contained in the databases are accurate and sufficient and, when requested by the Owner or when the controller has been able to notice it, they are updated, rectified or deleted, in such a way that they satisfy the purposes of the processing.

14. SPECIAL DATA CATEGORIES

14.1. SENSITIVE DATA

Sensitive data is data that affects the privacy of the data subject or whose misuse may lead to discrimination, such as data that reveals 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.

Cases in which NEW STETIC may process sensitive data:

- When the Owner has given his/her explicit authorization to said Treatment, except in cases where the



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

granting of said authorization is not required by law.

- When the Processing is necessary to safeguard the vital interest of the Data Subject and he or she is physically or legally incapacitated. In such events, the legal representatives must grant their authorization.
- When the Treatment refers to data that is necessary for the recognition, exercise, or defense of a right in a judicial process.
- When the Processing has a historical, statistical, or scientific purpose. In this event, measures must be adopted to suppress the identity of the Data Subjects.

In any case, NEW STETIC SA will adhere to the provisions of current data protection regulations in accordance with the guidelines established in the cases provided for as exceptions to the processing of data.

14.1.1 PROCESSING OF SENSITIVE DATA EMPLOYED

Sensitive biometric data related to videos and photographic images, fingerprints or data that may be collected will be used for company events, communications and for identification, security, internal and external monitoring and to be published in print media, cards, audiovisual media, social networks or websites of our own or of third parties, including family members and minors.

Sensitive data concerning the health status will be used for employee monitoring and/or procedures with competent occupational medical personnel and/or ARL physicians and to safeguard medical concepts, laboratory test results, medical studies, general or specialized medical, psychological, or psychiatric diagnoses.

14.1.2 PROCESSING OF SENSITIVE CUSTOMER DATA

Sensitive biometric data related to videos and photographic images that may be collected will be used for advertising purposes, internal and external company events, communications, and social networks of NEW STETIC SA

14.1.3 PROCESSING OF SENSITIVE BIOMETRIC DATA

The company has video surveillance cameras where it processes biometric data, and therefore collects, stores, uses, distributes, and deletes sensitive information.

Biometric data stored in the company's databases are collected and processed strictly for identification, security, internal and external control and monitoring of assets and people, and to control access to employees, customers, visitors, and others. Biometric identification mechanisms capture, process and store information related to the physical features of people (fingerprints and facial features) to establish or "authenticate" the identity of each subject.

The management of databases containing biometric data is carried out with technical security measures that guarantee due compliance with the principles and obligations derived from the Statutory Law on Data Protection, also ensuring the confidentiality and confidentiality of the information of the owners.

15. ATTENTION TO DATA OWNERS

NEW STETIC SA, has designated a Data Protection Officer who will be responsible for handling requests, queries, and complaints before which the Data Owner can exercise his/her rights, through the following channels:

Digital channel: The holders of the information may exercise their rights via email at the address dataprotection@newstetic.com.



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

Physical channel: Holders may go to the address Carrera 53 # 50 – 09 in Guarne, Antioquia, to submit requests, queries, and complaints by means of a letter addressed to the company, in accordance with the terms of section 10.1 of this policy.

16. DUTIES OF NEW STETIC AND THOSE IN CHARGE OF DATA PROCESSING

16.1. NEW STETIC DUTIES:

The company, as the Data Controller, must comply with the following duties, without prejudice to other provisions provided for in the law and in others that govern its activity:

- Guarantee the Holder, always, the full and effective exercise of the right to habeas data.
- Request and retain, under the conditions provided by law, a copy of the respective authorization granted by the Owner.
- Duly inform the Owner about the purpose of the collection and the rights that assist him/her pursuant to the authorization granted.
- Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or rapid access.
- Ensure that the information provided to the Data Processor is true, complete, accurate, up-to-date, verifiable, and understandable.
- Update the information, communicating in a timely manner to the Data Processor, all the updates regarding the data that you have previously provided and take other measures necessary to ensure that the information provided to you remains up to date.
- Rectify the information when it is incorrect and communicate the relevant information to the Person in Charge of Data Processing.
- Provide the Data Processor, only with data whose processing has been previously authorized in accordance with the provisions of the law.
- Demand from the Data Processor always, respect for the security conditions and privacy of the Owner's information.
- Process queries and complaints made under the terms set out in the law.
- Adopt specific procedures to ensure proper compliance with the law and to address queries and complaints.
- Inform the Data Processor when the Owner is discussing certain information once the claim has been submitted and the respective process has not been completed.
- Inform the Data Subject upon request about the use of his/her data.
- Inform the data protection authority when security code violations occur and there are risks in the management of the information of the Holders.

16.2. DUTIES OF THOSE IN CHARGE:

Data Processors must comply with the following duties, without prejudice to other provisions provided for in the law and in others that govern their activity:

- Guarantee the Holder, always, the full and effective exercise of the right to habeas data.
- Keep the information under the necessary security conditions to prevent its alteration, loss, consultation, unauthorized or rapid use or access. Those responsible must comply with the minimum-security conditions defined in the National Database Registry.
- Carry out the update, rectification, or deletion of data in a timely manner in accordance with the terms of the Law 1581 of 2012 and other concordant and current regulations.
- Update the information reported by those responsible for the Treatment within five (5) business days from its

**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

receipt.

- Process queries and complaints made by the Owners in the terms indicated in this policy.
- Adopt an internal manual of policies and procedures to ensure proper compliance with the law and, particularly to address queries and complaints from the Owners.
- Register the legend "claim in process" in the databases in the manner regulated by law.
- Insert the legend "information under judicial discussion" into the database once notified by the competent authority about judicial processes related to the quality of personal data.
- Refrain from circulating information that is being disputed by the Owner and whose blocking has been ordered by the Superintendency of Industry and Commerce.
- Allow access to information only to people who can access it.
- Inform the Superintendency of Industry and Commerce when security code violations occur and there are risks in the management of the information of the Holders.
- Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.
- Verify that the Data Controller has authorization to process the personal data of the Owner.

17. SECURITY MEASURES

NEW STETIC manages the information stored in its databases with the technical, human, and administrative measures necessary to ensure the security of the records, avoiding their adulteration, loss, consultation, use or unauthorized or rapid access.

In addition, the company, when signing the transmission contracts, has requested that those in charge of the treatment implement security measures that guarantee the security and confidentiality of the information in the processing of personal data. All security measures are contemplated in the Data Protection System Manual.

18. INCIDENT MANAGEMENT WITH PERSONAL DATA

NEW STETIC will ensure compliance with due process in the event of security incidents that may occur in the organization and that may put at risk the confidentiality, availability and integrity of the information contained in the databases. Therefore, there is a security incident protocol included in the Data Protection System Manual, to mitigate the impact that may be generated by the materialization of a risk with personal data.

19. MANAGEMENT OF RISKS ASSOCIATED WITH DATA PROCESSING

NEW STETIC, has implemented within this policy the processes and procedures to manage risks to mitigate their causes through internal security policies contained within the manual.

The company considers the tools, indicators and resources necessary for its administration, taking into account its organizational structure; the internal processes and procedures, the amount of databases and types of personal data processed by the organization that could be exposed to frequent or high-impact events or situations that affect the proper provision of the service or threaten the information of the owners.

The policy considers sources such as technology, human resources, infrastructure, and processes that require protection, their vulnerabilities, and threats, to assess their level of risk. Therefore, to ensure the protection of personal data, the type or group of internal and external persons, the different levels of access authorization will be taken into account. Likewise, the possibility of occurrence of any type of event or action that may cause damage (material or immaterial) will be observed, such as:

Criminality: Understood as actions, caused by human intervention, which violate the law and are penalized by it.



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

Events of physical origin: Understood as natural and technical events, as well as events indirectly caused by human intervention.

Negligence and institutional decisions: Understood as actions, decisions or omissions by people who have power and influence over the system. At the same time, they are the least predictable threats because they are directly related to human behavior.

Within its policy, the company establishes protective measures to avoid or minimize damage if a threat materializes.

20. TRANSFER OF DATA TO THIRD COUNTRIES

According to article 26 of Law 1581 of 2012, the transfer of personal data of any kind to countries that do not provide adequate levels of data protection is prohibited. A country is deemed to offer an adequate level of data protection when it complies with the standards set by the Superintendency of Industry and Commerce on the subject, which in no case may be lower than those required by this law for its recipients.

20.1. THIS PROHIBITION SHALL NOT APPLY IN THE CASE OF:

- Information for which the Owner has given his express and unequivocal authorization for the transfer;
- Exchange of medical data, when required for the Treatment of the Owner for reasons of public health or hygiene;
- Bank or stock transfers, in accordance with the applicable legislation;
- Transfers agreed upon within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity;
- Transfers necessary for the execution of a contract between the Owner and the Data Controller, or for the implementation of pre-contractual measures, provided that the Owner's authorization is obtained.
- Transfers legally required to safeguard the public interest, or for the recognition, exercise, or defense of a right in a judicial process.
- In cases not contemplated as an exception, it will be the responsibility of the Superintendency of Industry and Commerce to issue the declaration of conformity regarding the international transfer of personal data.

21. NATIONAL DATABASE REGISTRY

NEW STETIC SA registers its databases together with this Personal Data Processing Policy in the National Registry of databases administered by the Superintendency of Industry and Commerce, as established in the regulations and makes updates to the changes that may occur in it, as contemplated in article 25 of Law 1581 and its regulatory decrees.

22. PROTECTION, SECURITY AND CONFIDENTIALITY OF INFORMATION AND DATA PERSONAL

The company has established policies, guidelines, procedures, and processes focused on data protection, which may vary if there are changes in regulations or if any changes are required as determined by the company to safeguard the information, always focusing on security, confidentiality and privacy.

Furthermore, NEW STETIC guarantees that the collection, storage, use, processing, destruction, or elimination of the information provided is carried out using technological tools focused on secure mechanisms in transmission and storage, as well as on the restriction of access to information and backup.

In cases where it is necessary to transfer the information to a Data Processor due to a contractual relationship, NEW STETIC signs data transmission contracts, with the aim of always guaranteeing the security, confidentiality and



**ANNEX No. 4
DATA PROCESSING POLICY DATA
PROTECTION
PLPDAN - 006**

reserve of the information, thus complying with the regulatory guidelines, policies, information security manuals and protocols for attention to the owners.

23. SCOPE OF APPLICATION

The data processing policy will be applicable to all interested parties of the organization, this includes employees, clients, suppliers, and others.

24. VALIDITY

The databases held by NEW STETIC SA are processed for as long as is reasonable and necessary for the defined purpose. Once the purposes of the processing have been fulfilled, and without prejudice to legal regulations that provide otherwise, the personal information is deleted, unless there is a legal or contractual obligation that requires its conservation. These databases have been created without a defined period of validity.

When substantial changes occur in the personal data processing policies, the owners will be informed so that they can consult them through the different means enabled by the company for this purpose, or through open notices at the NEW STETIC headquarters.

"This processing policy has been in effect since November 2, 2016, and was updated on August 15, 2024.