zemoga
build better

POLICIES AND PROCEDURES MANUAL

Date: August 2020

INDEX

1. Legal basis and scope of application

The information processing policy is developed in compliance with articles 15 and 20 of the Political Constitution of Colombia; articles 17, literal k), and 18, literal f), of Statutory Law 1581 of 2012, *"Which sets out general provisions for the Protection of Personal Data "* (hereinafter LEPD); and Article 13 of Decree 1377 of 2013, *"Which partially regulates Law 1581 of 2012"*.

This policy will be applicable to all personal data registered in databases that are subject to processing by the data controller.

2. Definitions established in article 3 of the LEPD and article 3 of Decree 1377 of 2013

- **Authorization:** Prior, express and informed consent of the Holder to duly process personal data.
- **Database:** Organized set of personal data, subjected to processing.
- **Personal data:** Any information linked to or associated with one or more specific or determinable natural persons.
- **Public data:** Data that is not semi-private, private or sensitive. Public data include, among others, data pertaining to the marital status of people, their profession or craft, and their capacity of trader or public servant. Given their nature, public data may be contained, among others, in public records, public documents, gazettes and official bulletins, and judicial rulings duly executed, not subjected to confidentiality.
- **Sensitive data:** Sensitive data includes the data that affect the intimacy of the Owner or which undue use may give rise to their discrimination, such as those that disclose their race or ethnic background, political preference, religious or philosophical convictions, affiliation to unions, social, human rights organizations, or entities that guarantee the rights and guarantees of opposition political parties, as well as the data pertaining to health, sexual life and biometric data.
- **Data processor:** Natural or legal person, whether public or private, which by itself or together with others, conducts the personal data processing on behalf of the processing controller.
- **Processing controller:** Natural or legal person, whether public or private, which by itself or together with others decides on the database and/or data treatment.

- **Holder:** Natural person whose personal data are subjected to processing.
- **Processing:** Any operation, or set of operations with personal data, such as collection, storage, use, circulation or deletion.
- **Privacy Notice:** Verbal or written communication generated by the responsible party, addressed to the Holder for the treatment of his/her personal data, by means of which the holder is informed about the existence of the information treatment policies that will be applicable thereto, how to access them and the purposes of the treatment to be given to personal data.
- **Transfer:** The data transfer takes place when the controller and / or processor of personal data, located in Colombia, sends the information or personal data to a recipient, who in turn is responsible for the processing and is inside or outside the country.
- **Transmission:** Processing of personal data that implies the communication thereof within or outside the territory of the Republic of Colombia, when aimed at the processing by the party in charge on behalf of responsible party.

3. Authorization of the processing policy

In accordance with article 9 of the LEPD, the prior and informed authorization of the Owner is required for the processing of personal data. By accepting this policy, any Holder who provides information regarding his/her personal data is accepting the processing of his/her data by **ZEMOGA S.A.S.**, in the terms and conditions contained therein.

The authorization of the Holder will not be necessary when it comes to:

- Information is required by a public or administrative entity in the exercise of its legal functions or by court order.
- Data of a public nature.
- Cases of medical or health emergency.
- Processing of information authorized by law for historical, statistical or scientific purposes.
- Data related to the Civil Registry of Persons.
- To databases or files kept exclusively for personal or domestic purposes.
- Those whose purpose is the national security and defense prevention, detection, monitoring and control of money laundering and the financing of terrorism.
- Those that are intended and contain intelligence and counterintelligence information.

• Those that contain journalistic information and other editorial content
• The databases with financial, credit, commercial and service information, and the population and housing censuses.

4. Processing controller

The processing controller of the databases object of this policy is **ZEMOGA S.A.S.** , whose contact details are the following:

- Address: Calle 95 # 15 - 09 in the city of Bogotá D.C.
- Email: habeas.data@zemoga.com
- Telephone: 7443555 EXT. 7049

5. Processing and purposes of the databases

ZEMOGA S.A.S., in furtherance of its business activity, carries out the processing of personal data related to natural persons, which are contained and processed in databases destined for legitimate purposes, complying with the Constitution and the Law.

The following table (Table I) presents the different databases managed by the company and the purposes assigned to each of them.

TABLE I. DATABASES AND PURPOSES

Database	Internal Purpose	Purpose of the Superintendency of Industry and Trade
EMPLOYEE (CVs) **PHYSICAL AND AUTOMATED PROCESSING**	Manage everything related to the employee's personal data with the company's activity, such as: CVs, disabilities, records, affiliations and other documents issued in accordance with the employee's relationship with the employer.	Employee information. Human Resources - Payroll Management
SUPPLIERS DATA	Data collection for the creation of suppliers in the accounting system	Accounting, tax and administrative management - Supplier and Contractor Management. Accounting, tax and administrative management - Economic and accounting management.
CANDIDATES	Recruitment of personnel for hiring	Human Resources - Promotion and selection of personnel.
AFFINITY (Accounting Software)	Registration of data from suppliers, client, employees to carry out accounting management	Accounting, tax and administrative management - Supplier and Contractor Management. Accounting, tax and administrative management - Economic and accounting management.
CLIENTS	Manage everything related to customers, billing, contracts and service offerings.	Manage everything related to customers, billing, contracts and service offerings.

6. Rights of the Holders

In accordance with the provisions of article 8 of the LEPD and articles 21 and 22 of Decree 1377 of 2013, the Data Holders may exercise a series of rights in relation to the processing of their personal data. These rights may be exercised by the following persons.

1. By the Holder, who must sufficiently prove his identity by the different means made available thereto by the controller.
2. By their successors, who must prove such capacity.
3. By the representative and / or attorney-in-fact of the Holder, prior accreditation of the representation or power of attorney.
4. By stipulation in favor of either one.

The rights of children and adolescents shall be exercised by persons empowered to represent them.

The rights of the Holder are the following:

- **Right of access or consultation:** It is the right of the Holder to be informed by the processing controller, upon request, on the origin, use and purpose given to the personal data.
- **Complaint and claim rights.** The Law distinguishes four types of claims:
  - **Correction claim** : the right of the Holder to have partial, inaccurate, incomplete, fractionated, misleading data updated, rectified or modified, or those whose processing is expressly prohibited or has not been authorized.
  - **Deletion claim:** The right of the Holder to have data that is inappropriate, excessive or that does not respect constitutional and legal principles, rights and guarantees deleted.
  - **Withdrawal claim:** The right of the Holder to render the authorization previously given for the processing of personal data ineffective.
  - **Infringement claim:** the right of the Holder to request that the breach of the Data Protection regulations be remedied.
- **Right to request evidence of the authorization granted to the processing controller**: unless it is expressly exempted as requisite for processing, in accordance with that foreseen in article 10 of LEPD.
- **Right to file with the Superintendency of Industry and Trade claims for infringements:** the Holder or successor may only file this claim, once the consultation or complaint process has been exhausted with the processing controller or processor.

7. Attention to the Holders of the data

JENNY LAINE MEDINA MEZA with Colombian ID No.52.119.742 of **ZEMOGA S.A.S.**, will be in charge of the attention of requests, queries and claims, with whom the data Holder can exercise his/her rights. Telephone: 7443555 EXT. 7049, e-mail: habeas.data@zemoga.com

8. Procedures to exercise the rights of the Holder

8.1. Right of access or consultation

According to article 21 of Decree 1377 of 2013, the Holder may consult his/her personal data for free in two cases:

1 . At least once each calendar month.

2 . Whenever there are substantial changes to the information processing policies, giving rise to further consultations.

For enquiries whose frequency is more than once per calendar month, **ZEMOGA S.A.S.** may only charge the Holder for submittal, reproduction and, where applicable, document certification rates. The reproduction costs may not exceed the costs of recovery of the corresponding material. For this purpose, the processing controller must demonstrate to the Superintendence of Industry and Trade, when it so requires, the support of said expenses.

The owner of the data may exercise the right of access or consultation of his/her data by a written document sent to **ZEMOGA S.A.S.** , sent via email to habeas.data@zemoga.com indicating in the Subject "Exercise of right of access or consultation", or through postal mail sent to the address: Calle 95 # 15 - 09 in the city Bogotá D.C. The request must contain the following information:

- Name and surname of the Holder.
- Photocopy of the identity card of the holder and, where appropriate, of the representing person, as well as the document proving such representation.
- Request specifying the request for access or consultation.
- Address for notifications, date and signature of the applicant.
- Documents accrediting the request made, when applicable.

The Holder may choose one of the following forms to access the database to receive the requested information:

- On-screen display.
- In writing, with a copy or photocopy sent by certified mail or otherwise.
- Tele-copy.
- Email or other electronic means.
- Another system appropriate to the configuration of the database or the nature of the processing, offered by **ZEMOGA S.A.S**.

Once the request is received, **ZEMOGA S.A.S.** will resolve the request for consultation within a maximum period of ten (10) business days from the date of receipt. When it is not possible to attend the consultation within this term, the interested party will be notified, stating the reasons for the delay and indicating the date in which the enquiry will be addressed, which in no case may exceed five (5) business days following the expiry of the first term. These deadlines are set in article 14 of the LEPD.

Once the consultation process has been exhausted, the Holder or successor may raise a complaint with the Superintendence of Industry and Trade.

8.2. Complaint and claim rights

The Holder of the data may exercise the right to claim on his/her data by a written document sent to **ZEMOGA S.A.S.** , sent via email to habeas.data@zemoga.com indicating in the Subject "Exercise of right of access or consultation", or through postal mail sent to the address: Calle 95 # 15 - 09 in the city Bogotá D.C. The request must contain the following data:

- Name and surname of the Holder.
- Photocopy of the identity card of the Holder and, where appropriate, of the representing person, as well as the document proving such representation.
- Description of the facts and request in which the request for correction, deletion, revocation or violation is based.
- Address for notifications, date and signature of the applicant.
- Documents accrediting the request made, which are to be enforced, when applicable.

If the claim is incomplete, the interested party will be required, within five (5) days following receipt of the claim to remedy the failures. When two (2) months have elapsed since the date of the request without the applicant submitting the requested information, it will be understood that he has withdrawn the claim.

Once the complete claim has been received, a legend that says "claim in process" and the reason therefor, in a term not greater than two (2) business days, will be included in the database. This legend must be maintained until the claim is resolved.

ZEMOGA S.A.S. will resolve the request for consultation within a maximum period of fifteen (15) business days from the date of receipt. When it is not possible to deal with the claim within that 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 expiry of the first term.

Once the claim process has been exhausted, the Holder or successor may raise a complaint with the Superintendence of Industry and Trade.

9. Security measures

ZEMOGA S.A.S., in order to comply with the security principle enshrined in article 4 literal g) of the LEPD, has implemented technical, human and administrative measures necessary to guarantee the security of the records, avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access.

On the other hand, **ZEMOGA S.A.S.**, by signing the corresponding transmission contracts, has requested the processing controllers with whom it works to implement the necessary security measures to guarantee the security and confidentiality of the information in the processing of personal data.

The following are the security measures implemented by **ZEMOGA S.A.S.**, which are collected and developed in its Internal Safety Manual (Tables II, III, IV and V).

Table II. Common security measures for all types of data (public, semi-private, private, sensitive) and databases (automated, non-automated)

Document and support management	Access control	Incidents	Personnel	Internal Security Manual
1. Measures that prevent improper access or recovery of data that has been discarded, deleted or destroyed. 2. Restricted access to the place where the data is stored. 3. Authorization of the processing controller for the withdrawal of documents or attachments by physical or electronic means. 4. Labeling system or identification of the type of information. 5. Support inventory.	1. User access limited to the data needed for the development of their functions. 2. Updated list of users and authorized accesses. 3. Mechanisms to prevent access to data with rights other than those authorized. 4. Granting, alteration or cancellation of permits by authorized personnel	1. Incident registry: type of incident, time when it occurred, issuer of the notification, recipient of the notification, effects and corrective measures. 2. Procedure for incident notification and management.	1. Definition of the functions and obligations of the users with access to the data 2. Definition of the control functions and authorizations delegated by the processing controller. 3. Disclosure to staff of the rules and the consequences of non-compliance therewith	1. Preparation and implementation of the Manual of mandatory compliance for staff. 2. Minimum content: scope of application, security measures and procedures, functions and obligations of the personnel, description of the databases, procedure in case of incidents, procedure of copies and data recovery, security measures for transport, destruction and reuse of documents, identification of those in charge of the treatment.

Table III. Common security measures for all types of data (public, semi-private, private, sensitive) according to the type of databases

Non-automated databases			Automated databases	
File	Document storage	Custody of documents	Identification and	Telecommunications
1. Documentation file following procedures that ensure correct conservation, location and consultation and allow the exercise of the rights of the Holders.	1. Storage devices with mechanisms that prevent access to unauthorized persons.	1. Duty of diligence and custody of the person in charge of documents during their review or processing.	1. Personalized identification of users to access information systems and verification of their authorization. 2. Identification and authentication mechanisms; Passwords: allocation, expiration and encrypted storage.	1. Access to data through secure networks.

Table IV. Security measures for private data according to the type of databases

Automated and non-automated databases			Automated databases			
Audit	**Head of security**	**Internal Security Manual**	**Document and support management**	**Access control**	**Identification and authentication**	**Incidents**
1. Ordinary audit (internal or external) every two months. 2. Extraordinary audit for substantial modifications in information systems. 3. Report with the detection of deficiencies and proposal of corrections. 4. Analysis and conclusions of the security officer and the person responsible for the processing. 5. Preservation of the Report, available to the authority.	1. Appointment of one or more security officers. 2. Appointment of one or more people in charge of the control and coordination of the measures of the Internal Security Manual. 3. Prohibition of delegation of responsibility from the data controller to the security manager.	1. Periodic compliance controls	1. Registration of incoming and outgoing documents and media: date, sender and receiver, number, type of information, submittal method, responsible for receipt or delivery.	1. Access control to the place or places where the information systems are located.	1. Mechanism that limits the number of repetitive unauthorized access attempts.	1. Record of data recovery procedures, executing individual, restored data, and manually recorded data. 2. Authorization of the person responsible for the treatment for the execution of the recovery procedures.

Table V. Security measures for sensitive data according to the type of databases

Non-automated databases				Automated databases		
Access control	**Document storage**	**Copy or reproduction**	**Document transfer**	**Document and support management**	**Access control**	**Telecommunications**
1. Access only for authorized personnel. 2. Access identification mechanism. 3. Record of access by unauthorized users.	1. Filing cabinets, shelves or others located in access areas protected with keys or other measures.	1. Only by authorized users. 2. Destruction that prevents access or recovery of data.	1. Measures that prevent access to, or manipulation of documents.	1. Confidential labeling system. 2. Data encryption. 3. Encryption of portable devices when available.	1. Access record: user, time, database accessed, type of access, record accessed. 2. Control of the access log by the security manager. Monthly report. 3. Data conservation: 2 years.	1. Data transmission through encrypted electronic networks.

10. Data transfer to third countries

In accordance with Title VIII of the LEPD, the transfer of personal data to countries that do not provide adequate levels of data protection is prohibited. It is understood that a country offers an adequate level of data protection when it complies with the standards set by the Superintendency of Industry and Trade on the matter, which in no case may be lower than those that the LEPD demands from its recipients. This prohibition will not apply when it comes to:

- Information regarding which the Holder has granted his express and unequivocal authorization for the transfer.
- Exchange of medical data, when required by the Holder's processing for health or public hygiene reasons.
- Bank or stock transfers, in accordance with the legislation that is applicable thereto.

- Transfers agreed in the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.
- Transfers needed for the execution of a contract between the Holder and the person responsible for the processing, or for the execution of pre-contractual measures as long as the Holder'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 considered as exceptions, the Superintendency of Industry and Trade shall issue the declaration of conformity regarding the international transfer of personal data. The Superintendent is empowered to request information and carry out the proceedings aimed at establishing compliance with the budgets required for the viability of the operation.

The international transmissions of personal data made between a person in charge and a manager to allow the manager to carry out the treatment on behalf of the person in charge, will not require the Holder to be informed or have his/her consent, provided that there is a contract for the transmission of personal data."

11. Term

The databases for which **ZEMOGA S.A.S.** is responsible will be processed for as long as is reasonable and needed for the purpose for which the data is collected. Once the purpose or purposes of the processing have been fulfilled and without prejudice to legal norms providing otherwise, **ZEMOGA S.A.S.** will proceed to the deletion of the personal data in its possession unless there is a legal or contractual obligation that requires its conservation. Therefore, said database has been created without a defined period of validity.

This treatment policy remains in force as of August 2020.