ABCs OF PERSONAL DATA PROTECTION

CONTENTS

INTRODUCTION

All citizens have the Constitutional Right to know, update and correct any information stored or gathered in the databases managed by private companies or public entities. This constitutional right is regulated by Law 1581/2012, known as the General Personal Data Protection Regime, which sets outs the principles and obligations of all those who process personal data to ensure the protection of the constitution right to Habeas Data.

1. What is personal data and how is it classified?

Personal data is any information that may be associated with or that enables identifying an individual. Personal data can be classified as follows:

a) **Public Data**: All personal data that is contained in public records, public documents, official gazettes and bulletins and court rulings. The regulations give some examples of public data, such as: data related to the marital status of a person, their profession, trade or capacity as a public servant.

b) **Semi-private data**: All information of a financial, commercial and credit nature mainly used in the analysis of credit risk. E.g., Financial and credit data, employment or educational information, among others.

c) **Private Data**: All personal data that is not public or semi-private. These data are subject to confidentiality and their Processing affects the privacy of the Data Owner. E.g., The Data Owner's e-mail, land line or cell phone, residence address, tastes or tendencies, among others.

d) **Sensitive Data**: All personal data whose use can lead to the discrimination of an individual and that therefore require special authorization. Access to data of this type is restricted. E.g., Data related to the Data Owner's health, biometric data, sexual or religious orientation, among others.

e) **Data of Children and Adolescents**: the personal data of minors under 18 years of age are understood to be a special category due to the restrictions that their Processing entails. These can only be used for very specific purposes related to the best interests of the minor and only with the express consent of the parents or legal representatives of the minor. Regardless of their category, these personal data are classified as sensitive personal data.

2. Who is the owner of the personal data?

All individuals are the owners of their personal data. In the case of minors, their legal representatives have the power to authorize or not to authorize processing of their personal data. Information associated with legal entities is not classified as personal data and its use is not regulated by the laws on the protection of personal data.

3. What is personal data processing?

Personal data processing consists in any operation or set of operations on such data, such as gathering, storing, using, circulating or deleting such data.

4. When does the personal data protection regime apply?

The principles and provisions contained in the Law apply to the personal data recorded in any database that makes the data suitable for processing by public or private entities.

It also applies to any personal data processing carried out in the Colombian territory, whenever a Data Controller or Data Processor not incorporated in the national territory is subject to applicable Colombian law by virtue of international laws or treaties.

5. Who is involved in the processing of personal data?

Two main parties may be involved in personal data processing:

- **Data Controller:** An individual or public or private legal entity that makes decisions on the Database and/or Data Processing by itself or in association with others.
- **Data Processor:** An individual or public or private legal entity that processes the personal data on its own or in association with others on behalf of the Data Controller.

6. What is an authorization for personal data processing and when is it necessary?

The authorization is a consent granted by the data owner or individual to companies or Data Controllers to use their personal data. Such consent must be prior, express and informed.

When is such authorization not necessary? Such authorization is not necessary in the following cases:

- The information is requested by a public or administrative entity in exercising its legal duties or by court order.
- When personal data processing is performed on information of a public nature.
- Cases of medical or health emergency
- Processing information authorized by law for historical, statistical or scientific purposes.
- Data related to the Civil Registry of Persons.

How can we obtain the authorization? Data owners can indicate their authorization for processing their data through different means:

- In writing
- Orally
- By means of unequivocal conducts of the information owner.

What elements must the authorization include?

- The Processing to which the personal data will be subjected and the purpose of processing it;
- The optional nature of the answer to the questions that are asked when they deal with sensitive data or the data of children and adolescents;
- The rights of the Data Owner;
- The Data Controller's identification, physical or electronic address and telephone number.

Authorization to process sensitive personal data. The data owner must be informed that because the data is sensitive, the data owner is not under the obligation of authorizing its processing. The Data Controller has the duty of previously and explicitly informing the data owner about which data are sensitive and the purpose of processing the data. It should be noted that no activity may be conditioned to the data subject providing sensitive personal data.

Personal data processing in video surveillance The images recorded by video surveillance systems is personal data, and its use must be authorized by the data owner in an unequivocal manner that enables inferring that such authorization was given. Given the above, the Data Controllers must have signs in place informing the data owner that he/she is in an area that is being recorded and monitored by video surveillance systems. Informing the data owner by means of such signs is a legal means for obtaining the data owner's authorization.

Our Company has video surveillance signs in place at our facilities that inform data owners of the security monitoring purpose for performing the recordings. Personal information must be destroyed when it is no longer necessary or at the end of the term established by current regulations.

7. What are the special requirements for processing data of minors?

Processing of the personal data of children and adolescents is prohibited, except when the data is public in nature and when such processing fulfills the following requirements:

- It responds to and respects the best interests of the children and adolescents.
- It ensures respect for their fundamental rights.

When the above requirements are fulfilled, the legal representative of the child or adolescent may grant authorization.

8. What duties do we have as Data Controllers?

- Guarantee the data owner, at all times, the full and effective right of habeas data;
- Request and keep, in the terms established by law, a copy of the respective authorization granted by the data owner;
- Duly notify the data owner of the purpose of the data collection and the rights the data owner is entitled to by virtue of the authorization granted;
- Keeping the information under the safety conditions necessary to prevent unauthorized or fraudulent adulteration, loss, consultation, use or access.
- Process the inquiries and complaints in the terms established by law;
- At the request of the Data Owner, report on the use that was or will be given to the data.

9. What is the transmission and transfer of personal data?

Transfer of personal data: A Data Controller or Data Processor located in Colombia sends the personal data to another Data Controller that is located in or outside of the country.

Transmission of personal data: The Data Controller sends the personal data to a Data Processor that is located in or outside the country.

10. What are your rights in terms of personal data protection and how can you exercise them?

The Owner of the personal data, in the framework of his/her constitutional rights to Habeas Data and applicable law, has the following rights:

- To know, update and correct his/her personal data with the Data Controllers or Processors.
- To request proof of the authorization granted to the Data Controller.
- To be informed by the Data Controller or Data Processor, upon request, of the use given to his/her personal data.
- To submit to the Superintendence of Industry and Commerce complaints for violations of the provisions of law and other regulations that modify, add to or complement it.
- To revoke the authorization (exclusion) and/or request deletion of the data when the process fails to observe constitutional and legal principles, rights and guarantees.
- The aforementioned rights are described in greater detail in GEB's Personal Data Processing Policy.

Through which channels can I exercise my rights with GEB?

GEB has made available to its data owners, through its Personal Data Processing Policy, the following channels to exercise their rights:

- E-mail: datospersonales@geb.com.co
- To the address Carrera 9 No. 73 – 44 Piso 6

11. Did you know that at GEB we have training and communications plans on personal data protection?

GEB understands that, in order to guarantee adequate processing of the personal data of its data owners, it must generate spaces of knowledge that consolidate the culture of Compliance and Data Protection within the Company and its employees. To this effect, we have a Personal Data Protection Training Program to train employees in the proper processing of the personal data and their role in guaranteeing compliance with the Company's guidelines regarding Personal Data Protection.

12. How do we manage inquiries and claims from our data owners?

GEB is committed to the proper processing of the personal data of its data owners; for this reason, we recognize the vital importance of guaranteeing that they can exercise their ARCO rights (access, rectification, cancellation and opposition) through any of the channels authorized for this purpose, which are published in our Personal Data Protection Policy. The data owner may submit an inquiry or claim to exercise his/her rights, as follows:

Inquiry: By means of an inquiry on personal data protection, the data owner may:

- Request access to his/her personal information.
- Request proof or evidence of the authorization granted to GEB for the Processing of his/her personal information
- Inquire on the use given to his/her personal information.

Claims: The data owner may request the correction and updating of the personal information, the deletion of the data and the partial or total revocation of the authorization given to GEB, by submitting a claim through the channels enabled to this end.

Revoke the authorization for personal data processing - additional or secondary purposes of personal data processing on clients

GEB's electricity transmission business does not have end users or clients who are individuals or physical natural persons. GEB's clients are legal entities, which implies that most of the information obtained from them consists of technical data related to contractual relationships with the companies. Regarding its clients, GEB only performs personal data processing for the purposes described in our Personal Data Processing Policy. This document is made available to our clients for their knowledge before any processing. In view of the above, GEB does not use the personal information of its clients for additional or secondary purposes. Thus, the percentage of customers whose data is used for secondary purposes is 0%.

13. What do we do in the event of occurrence of an incident involving personal data protection?

Personal Data Protection Incidents occur for various reasons ranging from simple human error to attacks directed from outside. These are events that can affect the confidentiality, availability and integrity of the Company's personal databases.

GEB's Personal Data Protection Officer is responsible for assessing and managing any personal data protection incidents that may arise, and for reporting the event to the Control Authority, following the internal procedure established to this effect.

14. How do we manage the risk of personal data protection?

GEB assures through a Risk Management System the risks associated with the protection of personal data, the identification, measurement, control and monitoring of all events or situations that may affect the proper management of the Personal Data Protection risks to which GEB is exposed, especially in connection with compliance with the guidelines established in the Personal Data Processing Policy. The Personal Data Protection Officer will guarantee the administration of the Company's Personal Data Protection Risk Management System.

To this end, the Company has developed a Personal Data Protection Risk Matrix, which is managed by the Personal Data Protection Officer and monitored in accordance with the internal procedure established to this effect. In turn, the risk of non-compliance with applicable regulations related to personal data protection forms part of the Strategic Risk Management Matrix of the Corporate Compliance Department and the Compliance process. Lastly, our Company performs periodic external and internal audits on compliance with the Personal Data Protection Policy and the Personal Data Protection Program.

15. How do we manage the information we provide third-party Data Processors?

In fulfilling its corporate purpose, the Company may transmit the personal data of its data owners to third parties, which will act in the capacity of Data Processors of the transmitted personal data. In compliance with the legal obligation of managing the third-party Personal Data Processors, the Company has established relevant and appropriate measures to ensure that these Processors strictly comply with applicable regulations on this matter.

16. How do we comply with our obligation of registering our databases in the National Database Registry?

In compliance with the regulations on personal data protection, the Company has an inventory of its personal data databases, which is reported and updated in the terms required by law to the National Database Registry carried by the Superintendence of Industry and Commerce. The databases registered in the National Database Registry can be accessed by the public through the website https://rnbd.sic.gov.co/sisi/consultaTitulares/consultas/

17. What is the internal sanctions regime in the event of breach of the Personal Data Protection Program?

The Company's Internal Work Regulations establish the employees' duty and obligation to follow and comply with the Company's guidelines on Ethics and Conduct (personal data protection) and Information Security. In turn, the Internal Work Regulations establish that any violation of the Company's ethical framework represents a serious breach. The Company's ethical framework is defined in our Code of Ethics and Conduct, which, regarding personal data protection, establishes the employees' duty of knowing, understanding and fully complying with the guidelines set out in the Company's Personal Data Protection Program, and particularly with the provisions of the Personal Data Processing Policy. Any violation of the above guidelines would represent a serious breach by the employee, which could give rise, subject to the respective due process, to the suspension of the employee's employment contract.

In turn, by virtue of the employment contract signed by the employees, any violation of the duty of Confidentiality would represent a breach of the employment contract and consequently of the Internal Work Regulations.

18. Did you know that we have an area in charge of the protection of personal data?

The GEB Corporate Compliance Department, through the Personal Data Protection Officer, is in charge of leading the management for the implementation, follow-up, monitoring, control and continuous improvement of the Company's Personal Data Protection Program. The scope of its management includes the periodic evaluation of the Program in order to establish its relevance and functionality, making the necessary adjustments if required.

19. Definitions

- **Authorization:** Express and informed prior consent by the data owner to Process the Personal Data.
- **Database:** An organized set of Personal Data subject to Processing.
- **Data Processor:** An individual or public or private legal entity responsible for processing the personal data on its own or in association with others.
- **Regulations:** The Political Constitution of Colombia, laws, decrees, resolutions, ordinances, agreements, and opinions by the National Authority for Personal Data Protection and jurisprudence.

- **Personal Data Protection Officer:** The person responsible for addressing petitions, inquiries and claims submitted by the data owners in exercising their right to review, update, correct and delete the data and revoke the authorization. The Personal Data Protection Officer will support and guide the implementation and maintenance of the Personal Data Protection Program.
- **Data Controller:** An individual or public or private legal entity that makes decisions on the Database and/or Data Processing by itself or in association with others.
- **Data Owner:** An individual whose personal data is subject to Processing.
- **Transfer:** A data transfer occurs when the personal data controller and/or processor sends the information or Personal Data to a recipient who is the Data Controller and is either inside or outside the country from which it was sent.

NOTE: For additional information on how GEB manages the processing of personal data, please read our Personal Data Processing Policy, which is published at https://www.grupoenergiabogota.com/conoce-geb/programa-de-etica-y-cumplimiento/proteccion-datos

These ABCs of Personal Data Protection are issued on May 31, 2023 and form integral part of GEB's Personal Data Protection Program.

Luis Rodolfo Hernandez Casadiego
GEB Corporate Compliance Director (d)
(Signature on original copy)

Reviewed by: Catalina Casas Arevalo
GEB's Detection and Response Manager (d)

Drafted by: María Claudia Álvarez Rincón
GEB's Personal Data Protection Officer