## TABLE OF CONTENTS

## OBJECTIVE

In line with the corporate value of Integrity, Grupo Energía Bogotá SA ESP (hereinafter "GEB" or the "Organization") is committed to the correct processing of the data of their data subjects. To do this, it recognizes the vital importance of having a Manual of Personal Data Protection Policies and Procedures that sets out the general corporate guidelines for the correct implementation, application, monitoring, support and continuous improvement of the guidelines and procedures related to the correct processing of personal data.

Through this manual, GEB seeks to comply with the Personal Data Protection Regime - Law 1581 of 2012-, Decree 1074 of 2015, the Accountability Guide of the Superintendency of Industry and Commerce, and the Principle of Demonstrated Responsibility regarding the Protection of Personal Data.

## SCOPE

This Manual is mandatory and must be strictly complied with by all representatives and administrators of the Organization, employees of GEB; individuals or legal persons linked through any of the contractual modalities established in the GEB Contracting Manual, contractors and third parties acting on behalf of GEB.

All GEB employees In the performance of their duties must observe and respect the regulations on data protection, the Personal Data Processing Policy and the duties contained in this Manual.

Any concern or doubt regarding compliance with the Law, the Personal Data Processing Policies or this Manual should be directed to the Personal Data Protection Officer who will be in charge of resolving them and giving the corresponding instructions.

## DESCRIPTION OF THE MANUAL

This Manual will apply to the processing of any database or files created, managed and/or stored by the Organization, as either the Data Controller or Processor. Similarly, this manual applies to the processing of personal data or personal databases that the data owners in their capacity as bidders, suppliers, contractors, employees, applicants or clients, among others, have delivered to GEB.

Likewise, it will apply to personal data that is collected and handled by GEB in Colombian territory.

This manual will not apply to:

a. To databases or files maintained in an exclusively personal or domestic environment.

b. Whenever these databases or files are going to be supplied to third parties, the Data Subject must be previously informed and their authorization requested. In this event, the controllers and processors of data and files will be subject to the provisions contained in Law 1581 of 2012;

c. To the databases and files whose purpose is national security and defense, as well as the prevention, detection, monitoring and control of money laundering and the financing of terrorism;

d. To the Databases that have as their purpose and contain intelligence and counterintelligence information;

e. To the databases and archives of journalistic information and other editorial content;

f. To the databases and files regulated by Law 1266 of 2008;

g. To the databases and files regulated by Law 79 of 1993.

## DEFINITIONS AND ACRONYMS

1. **Authorization:** Express and informed prior consent by the data subject to process the personal data.[1]

2. **Database:** Organized set of personal data subject to processing.[2]

3. **Assignee:** Person who has succeeded or has been subrogated in any way in the right of another or others.

4. **Employee**: Natural person who has a direct employment relationship with GEB.

5. **Personal Data:** Any information linked or that can be associated with one or more specific or determinable individuals.[3] Personal data is classified into:

    - **Public Data:** Data that is not semi-private, private or sensitive. Public data is considered, among others, data related to the marital status of people, their profession or trade and their capacity as a merchant or public servant.

[1] Law 1581/2012, Article 3 (a).
[2] Law 1581/2012, Article 3 (b).
[3] Law 1581/2012, Article 3 (c).

- **Semi-private Data:** These are the data that, although private, are only of interest to the data owner and a certain group of people who can consult the information through authorization.

- **Private Data:** Data that, due to its intimate or confidential nature, is only relevant to the data owner.

- **Sensitive Data:** These are data that affect the data owner's intimacy or whose inappropriate use may result in discrimination, such as data that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership in labor unions or social or human rights organizations, or those that promote the interests of any political party, or guarantee the rights and assurances of oppositional political parties, as well as data pertaining to health, sexual life and biometric data.

6. **Data Processor**: Individual or legal entity, public or private, that on its own or in association with others, processes the personal data of GEB's employees, suppliers, bidders and other data subjects. The data processor or third party will process the personal data in compliance with the guidelines and directives given by GEB.

7. **Personal data protection impact assessment**: It is considered a proactive measure to comply with the Principle of Demonstrated Responsibility, and also serves to implement an effective system of risks and internal controls to ensure that the data will be processed properly and in accordance with existing regulations. Said assessment must include a detailed description of the personal data processing operations. - Assessment of specific risks to the rights and freedoms of the data subjects (identify and classify risks), as well as the adoption of measures to mitigate them. [4]

8. **Personal data protection incident:** A personal data protection incident occurs when an event generates the collection, use, disclosure, unauthorized destruction, loss or theft of the Organization's personal data, whether accidental or intentional, and therefore there is a breach of the Policy on Processing of Personal Data and other procedures that are part of the GEB Data Protection Program, as well as the Personal Data Protection Regime – Law 1581 of 2012.

9. **Regulations:** The Political Constitution of Colombia, laws, decrees, resolutions, ordinances, agreements, and opinions by the National Authority for Personal Data Protection and jurisprudence.

10. **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 of the principle of proven responsibility. The Personal Data

[4] Guide on the processing of personal data for marketing and advertising purposes - Superintendence of Industry and Commerce.

Protection Officer for GEB is part of the Corporate Compliance Department and the contact channel is datospersonales@geb.com.co.

11. **Principle of restricted access and circulation:** This principle is directly related to the nature of personal data. In this regard, the processing can only be done by persons authorized by the data subject and/or by the persons provided for in Law 1581 of 2012 or the General Law of Protection of Personal Data. Personal data, except for data classified as public data, may not be available on the Internet or other means of mass dissemination or communication, unless the access is technically controllable to provide restricted knowledge only to data owners or third parties authorized according to law.[5]

12. **Principle of confidentiality:** Every person involved in processing personal data that is not a public servant is obligated to guarantee the confidentiality of the information, even after its relationship with some of the tasks included in the processing, only able to provide or communicate personal data when appropriate to the development of activities authorized by the regulations that pertain to the right to habeas data.[6]

13. **Principle of purpose:** Personal data must be processed only for legitimate purposes pursuant to the Constitution and the law, which must be made known to the data subject.[7]

14. **Principle of legality in matter of personal data protection:** The processing of personal data is an activity regulated by Law 1581 of 2012 or the General Law on the Protection of Personal Data, constitutional regulations, and thus a regulated activity that must be subject to that set out the regulations and in the other provisions that implement it.[8]

15. **Principle of freedom:** The processing may only be exercised with the prior, express and informed consent of the data subject. Therefore, personal data may not be obtained or disclosed without prior authorization of the data subject, or in the absence of a legal or judicial mandate which replaces the data subject's consent or authorization.

16. **Principle of security:** Information subject to processing by the Data Controller or Processor shall be handled with the technical, human and administrative measures necessary to convey security to the records information, avoiding adulteration, loss, or unauthorized or fraudulent consultation, use or access.[9]

17. **Principle of transparency:** The data subject shall be guaranteed the right to obtain from the Data Processor or Controller, at any time and without restrictions, information about the existence of relevant data.[10]

[5] Law 1581/2012, Article 4 (f).
[6] Law 1581/2012, Article 4 (h).
[7] Law 1581/2012, Article 4 (b).
[8] Law 1581/2012, Article 4 (a).
[9] Law 1581/2012, Article 4 (g).
[10] Law 1581/2012, Article 4 (e).

18. **Principle of veracity or quality:** The personal data subject to processing must be true, complete, accurate, updated, verifiable and understandable. Pursuant to the foregoing, processing data that is partial, incomplete, fragmented or can lead to error is prohibited.[11]

19. **Privacy by design and by default:** Privacy and security must be part of the design, architecture and default configuration of the information management process and the infrastructures that support it. For this purpose, before information is collected and throughout its life cycle, preventive measures of a diverse nature (technological, organizational, human, procedural) must be adopted to avoid violations of the right to the privacy or confidentiality of information.[12]

20. **Demonstrated responsibility:** Also known internationally as "Accountability", in which the role of the Data Controller is emphasized to implement necessary measures within the organizations that allow compliance with the principles and obligations as such. Thereby observing the organization's commitment to increase the standards of protection of personal information and guarantee the data subject the correct processing of personal data[13].

21. **Data controller**: Individual or legal person, public or private, that by itself or in association with others, decides on the database and/or personal data processing. GEB has capacity as the Data Controller of its databases.

22. **Data Owner:** Individual whose personal data is subject to processing. The data subject will also be understood as the person who is authorized to request information regarding personal data, such as successors in title or representatives, duly empowered to do so.[14]

1

23. **Transfer:** Data transfer occurs when the personal data controller and/or processor located in the Republic of Colombia sends the information or personal data to a recipient who, in turn, is the processing controller and is either inside or outside the country.

24. **Transmission:** Processing personal data that implies communication thereof inside or outside of each country when the purpose is for the Processor to do processing at the behest of the Controller.

25. **Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.[15]



11 Law 1581/2012, Article 4 (d).

12 Decree 620/2020, Article 2.2.17.1.6.

13 Superintendence of Industry and Commerce – Guide for the implementation of the Principle of Demonstrated Responsibility (Accountability).

14 Law 1581/2012, Article 3 (f).

15 Law 1581/2012, Article 3 (g).

# 1. GUIDELINES FOR COLLECTING PERSONAL DATA

## Scope of application

The provisions contained in these guidelines will be applied to all forms of personal data collecting carried out by GEB, since, in its capacity as Data Controller, it must obtain the prior, free, express and informed consent of the data subjects, as established in article 9 of Law 1581 of 2012.

## Nature of Personal Data

One of the main concerns that arises when handling the data of individuals is to determine whether or not one is dealing with personal data. For these purposes, it is necessary to identify whether it is possible or not to identify that person with the information or with the set of information that we have about them.

By way of illustration, the main examples of personal data are, among others: name, surname, e-mail, residence address, telephone, etc.

**Note:** The images contained in photographs and recordings are considered personal data. Additionally, the corporate data of natural persons, such as corporate e-mail, are personal data of a public nature.

If you are not sure whether or not the information you are dealing with is personal data, contact the Personal Data Protection Officer at the email datospersonales@geb.com.co

## Personal Data Categories

Once you are sure that you are dealing with personal data, it is necessary to determine its nature, in accordance with the classification presented by the Colombian regulation of personal data. This is of vital importance, because the authorization forms and security measures will depend on the category the personal data being processed belongs to.

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. Authorization is not required to carry out the processing of these data. However, public personal data is subject to the application of all the principles established by the regulations. E.g., People's citizenship I.D., names and surnames.

b) **Semi-private Data***:* All information of a financial, commercial and credit nature mainly used in the analysis of credit risk. Express authorization is required from the Data Subject for this processing. 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. Express authorization is required from the Data Subject for this processing. 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 therefore require special authorization. These data are of restricted access, require express and unequivocal authorization in accordance with legal provisions, among others, and the Data Subject must also be informed that obtaining them cannot impede access to any good or service. 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.

As a guideline, GEB will take into account that the more confidential the personal data, for example, Sensitive Data or Data of Children and Adolescents, the more diligence the Controller must have and/or require of the Processor in taking care of the Databases and their content.

### Requirements for the collection of personal data

The processing of personal data will only be carried out by GEB, if prior authorization has been requested from the data owner, in anything related to semi-private, private or sensitive data. For this purpose, the staff of the Organization will make use of the different means contained in the authorizations, according to the capacity of each data subject.

Likewise, and in accordance with the provisions of the principles of purpose and freedom, the collection of personal data will be limited to personal data that are pertinent and adequate for the purpose for which they are collected or required in accordance with current regulations.

Except in the following scenarios, personal data may be collected without the authorization of the data subject:

a) Information requested by a public or administrative entity in the exercise of its legal duties or by court order;

b) Data of a public nature;

c) Cases of medical or health emergency;

d) Processing information authorized by law for historical, statistical or scientific purposes;

e) Data related to the Civil Registry of Persons.

The personal data collected upon executing a contract, employment or legal relationship, will only be processed for the purposes directly related to the link in question. If there is a desire to use the data for different purposes, the consent of the data subject must be obtained.

### Authorization for the processing of personal information

Law 1581 of 2012 defines authorization as: *"That prior, express and informed consent of the data subject, to carry out the processing of personal data."*[16]

GEB will request the data owners' prior, express, unequivocal and informed authorization to carry out the processing of the related personal information in its databases.

Authorization may be granted in the following ways:

**a) Written:** Through the Organization's forms in physical formats on which the data subject authorizes the processing of their personal data by signing.

**b) Verbal:** Through forms available on telephone or video channels, or any other channel that allows recording verbal authorization.

**c) Digital:** Through forms on web forms and other technological developments of GEB.

**d) Unequivocal conduct:** The unequivocal conduct of the data subjects that allows a reasonable conclusion that they granted the authorization. In no case shall silence be understood as an unequivocal conduct.[17]

### Characteristics of the authorization

When GEB requests the data holder to authorize the processing of their personal data, it must clearly and expressly of the following:

**a)** The Processing to which the personal data will be subjected and the purpose for it.

**b)** 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.

**c)** The rights of the data subject.

**d)** The Data Controller's identification, physical or electronic address and telephone number.

### Custody of authorizations

GEB must keep the proof or evidence that allows it to demonstrate that it has requested their prior, express, and informed authorization from its data owners.

To do this, GEB will guarantee the adequate custody of the authorizations obtained through its different collection channels, physical, verbal or digital.

**a) Authorizations collected through physical formats:** GEB will adequately safeguard in its physical repositories the forms for requesting the authorization of the processing of personal data from its different data owners.

[16] Law 1581/2012, Article 3 (a).
[17] Decree 1074/2015, Article 2.2.2.25.2.4.

**b) Authorizations collected through verbal channels:** GEB will adequately guard the technological evidence that allows supporting the request for authorization for the processing of personal data through its telephone or video channels, or any other channel that allows recording the verbal authorization.

**c) Authorizations collected through digital channels:** GEB will safeguard in its digital repositories all technological supports or "logs" of acceptance of the authorizations for the processing of personal data collected by technological platforms, websites, apps, among others.

The data holder may, at any time and in the exercise of his rights, request that GEB gives him the support of evidence of the authorization to process personal data that he granted to GEB.

### Authorization regarding sensitive data

The processing of sensitive data is expressly prohibited by Article 6 of Law 1581 of 2012. However, the above prohibition provides for the following exceptions:

**a)** The Data Subject has given their explicit authorization to said Processing, except in cases where the granting of said authorization is not required by law.

**b)** The Processing is necessary to safeguard the vital interest of the Data Subject and they are physically or legally incapacitated. In these events, the legal representatives must grant their authorization.

**c)** The Processing is carried out in the course of legitimate activities and with due guarantees by a foundation, NGO, association or any other non-profit organization, whose purpose is political, philosophical, religious or trade union, provided that they refer exclusively to its members or to people who maintain regular contact by reason of its purpose. In these events, the data may not be provided to third parties without the authorization of the Data Subject.

**d)** The Processing refers to data that is necessary for the recognition, exercise or defense of a right in a judicial process.

**e)** The Processing has a historical, statistical or scientific purpose. In this event, the measures leading to the suppression of the identity of the Data Subjects must be adopted.[18]

Authorization for the processing of sensitive personal data must be given explicitly in all cases, taking into account the identity that they imply. Additionally, when this type of personal data must be carried out, the data subject will be informed of the power they to refrain from handing over this information.

### Guidelines for the collection of sensitive data

If sensitive data is collected (when there is a purpose for it, in accordance with the previous paragraph), the following obligations must also be fulfilled.

[18] Law 1581/2012, Article 6.

a) Inform Data Subjects that since it is sensitive personal data, they are not under the obligation to authorize its processing.

b) Inform the Data Subject, explicitly and in advance, in addition to the general requirements of the authorization for the collection of any type of Personal Data, which of the data that will be subject to Processing are sensitive and the purpose of the Processing, as well as obtaining their express consent.

c) Do not condition the activities of the Data Subject upon providing sensitive Personal Data, unless there is a legal cause.

### Authorization regarding the data of children and adolescents

The processing of personal data of children and adolescents is prohibited, except those that are of a public nature, as provided in Article 7 of Law 1581 of 2012 and when said processing meets the following requirements:

a) The processing responds to and respects the best interests of the children and adolescents.

b) The processing ensures respect for the fundamental rights of the children and adolescents.

c) Assess the opinion of the minor when he/she has the maturity, autonomy and capacity to understand the matter.

d) The processing of the personal data of minors shall be preceded by the express authorization of their legal representative.

e) The legal representative of the minor must be informed that, since it is the data of minors, they are not obliged to authorize its processing.

f) The legal representative of the minor be informed of the purpose of the data processing.

The authorization for the processing of personal data must be granted by the legal representative of the child or adolescent, after exercising the minor's right to be heard, an opinion that will be valued taking into account the maturity, autonomy and ability to understand the matter.

### Personal Data Processing Policy

In order to guarantee the constitutional right that all people have to know, update and rectify the information that has been collected about them in the databases or files that GEB has compiled and in compliance with the provisions of Decree 1377 of 2013, today compiled in Decree 1074 of 2015 and Law 1581 of 2012, GEB as the controller of personal data, has designed and made available to its different data owners its *Personal Data Processing Policy.* This Policy is published on the website www.grupoenergiabogota.com.co

### Purposes for the collection and processing of personal data

In order to comply with the principles of purpose and freedom enshrined in Law 1581 of 2012, the collection of personal data carried out by GEB will be limited to personal data that are relevant and adequate for the purpose for which they are collected or required.

The GEB may collect or process the personal data of its data owners for the fulfillment of the following purposes, which are available for consultation in the *GEB Personal Data Processing Policy.*

### General purposes for Processing Personal Data

As Data Controller, GEB will Process your Personal Data to fulfill a legitimate purpose. Therefore, the collection of Personal Data will be limited to those that are pertinent, adequate, necessary and useful for the purpose(s) for which they are collected or required in accordance with the regulations. With regard to all Data Subjects, without prejudice to the specific purposes indicated below, Personal Data is collected with the following general purposes:

**a)** Sending correspondence and notifications.
**b)** Contacting the Personal Data Subject by any means, especially, but not limited to, e-mail and/or cell phone.
**c)** Send information about activities, events, products and/or services of the Organization through the channels or media established for such purpose.
**d)** Maintain a shareholder registry, control of shares and payment of profits.
**e)** Have meetings of the board of directors, pay the board members' fees and send communications of interest to board members.
**f)** Carry out actions aimed at the community in general, where information is provided and activities are carried out related to the Organization's purpose.
**g)** Conduct market research, statistics and surveys within the framework of GEB's bylaws and policies.
**h)** Allow access to GEB facilities.
**i)** Capture images through video surveillance systems to ensure the safety of people and property on GEB facilities.
**j)** Use the data subject's image to generate notes or videos and publish them in different media highlighting GEB's activities and services.
**k)** Consult the information of the data subject registered in other databases or files of any public or private, national or international entity.
**l)** Carry out procedures before authorities for which said information is pertinent.
**m)** Address requirements of public or private entities that, in compliance with legal or contractual mandates, are authorized to request and access Personal Data.
**n)** Provide information to auditors who are verifying the adequate administration of GEB.
**o)** Contacting stakeholders for brand positioning and reputation management.
**p)** Invite to events and offer new products and services.
**q)** Managing proceedings (requests, complaints and claims).
**r)** Carry out the pertinent steps to implement GEB's corporate purpose with regard to fulfilling the object of the contract entered into with the Data Subject or party to the legal relationship.
**s)** Conduct satisfaction surveys for the products and services GEB offers.
**t)** Transfer Personal Data in the country or abroad to companies related economically to GEB (affiliates and subsidiaries), third parties, contractors or GEB partners, for them to Process

the Personal Data, in accordance with the provisions of this Policy.

**u)** Transmit Personal Data in the country or abroad to companies related economically to GEB (affiliates and subsidiaries), third parties, contractors or GEB partners, for them to Process the Personal Data, in accordance with the provisions of this Policy.

**v)** Transfer Personal Data within the framework of defining, structuring and executing strategic transactions, such as selling assets, in the event the Organization or parts of its business are sold, merged or acquired by third parties.

### Purposes of Personal Data Processing Specific to Suppliers and/or Contractors.

The Personal Data owned by GEB suppliers and/or contractors will additionally be processed for the following specific purposes:

**a)** Carry out the necessary activities required in the pre-contractual, contractual and post-contractual stages of the Organization.

**b)** Carry out selection processes and register them by categories and/or classes of suppliers. Likewise, register them as suppliers in GEB's accounting and computer systems, make the payments corresponding to the contracted obligations and keep a historical list of the suppliers.

**c)** Access, consult, validate or corroborate the Personal Data in the Databases or files of any national or foreign Public or Private Institution. This verification may be carried out directly or through third parties hired by GEB.

**d)** Supervise or audit the contracts, as well as to assess and rate the performance of the Organization's suppliers and contractors.

**e)** Comply with contractual and legal obligations and exercise the rights that arise from its capacity as a Commercial Company and, in general, from the activities of its main and related corporate purpose, as well as from the company's internal policies.

**f)** Nationally and/or internationally transfer and/or transmit Personal Data to commercial partners, strategic partners, affiliates or subsidiaries of GEB or to third parties as a result of a contract, law or legal connection that requires it, or to implement cloud computing services.

**g)** For the security of the Organization’s staff, assets and facilities, and to be used as evidence in any proceeding with respect to the data (i) collected directly at security points, (ii) taken from the documents provided by individuals to security staff and (iii) obtained from video recordings inside and outside of GEB facilities.

**h)** Provide information to third parties such as mail companies, technological services, commercial and/or strategic partners, among others in Colombia and abroad.

**i)** Create a record of suppliers in the SAP system that contains tax indicators for the purpose of paying invoices.

**j)** For evidentiary, legal, judicial and/or administrative purposes in potential internal or legal processes.

**k)** Develop the purpose of the contract.

**l)** Evaluate the performance of the contractor's and/or supplier's employees.

**m)** Send advertising and publications related to the activities carried out by the Organization.

**n)** Carry out market studies, statistics and surveys, framed within the Organization's corporate purpose.

**o)** Transfer the Personal Data of suppliers within the framework of defining, structuring and

executing strategic transactions, such as selling assets, in the event the Organization or parts of its business are sold, merged or acquired by third parties.

**p)** Report, under the terms of Law 1266 of 2008, before any information operator or legally authorized risk center, on timely compliance or non-compliance with monetary obligations or duties of patrimonial content, presenting truthful, pertinent, exact, complete and updated information.

### Specific Purposes of Personal Data Processing for bidders.

The Personal Data of GEB bidders will additionally be processed for the following specific purposes:

**a)** Assess the request for Authorization to Offer and Purchase Offer.
**b)** Verify the Data of the Representatives who will participate in the contractual selection processes.
**c)** Carrying out market studies, statistics, storage of contractor information and Organization surveys.
**d)** All others related to implementing the contractual selection process, particularly the one in which the proponent is presented.

### Specific Purposes of Personal Data Processing for employee candidates and employees

The Personal Data of GEB candidate employees and employees will additionally be processed for the following specific purposes:

**a)** Select staff, study resumes, verify data provided by the candidate, verify personal, family and/or commercial reference contacts and location data.
**b)** Carry out and verify onboarding, regular or separation health exams by the Organization.
**c)** Conduct written and oral selection tests, psychotechnical tests and/or interviews.
**d)** Accepting internal procedures for selection, admission, occupational health and recruitment.
**e)** Allow access to the Organization's facilities.
**f)** Carry out access control and guarantee the security of people and goods.
**g)** Have a record of the activities carried out by the Organization.
**h)** Process affiliations to the Health Promotion Entities (EPS, for the Spanish original), Pension and Severance Fund Managers (AFP, for the Spanish original), Family Compensation Funds (CCF, for the Spanish original), insurance policies or an additional health plan when applicable.
**i)** Carry out security studies for onboarding and monitoring during the duration of the employment relationship.
**j)** Verify the information related to the System for Prevention of Money Laundering and Terrorist Financing, conflicts of interest, disqualifications and incompatibilities.
**k)** Guarantee compliance with trade union rights in Articles 38, 39 and 55 of the Political Constitution of Colombia, as well as comply with the current collective labor agreement, when applicable.
**l)** Maintain a record of employees and pensioners.
**m)** Collect and custody resumes.
**n)** Review of the criminal, contractual and tax records of the Data Subjects before the relevant

authorities.

o) Fully identify the Data Subjects by filing and handling their contact details, professional and academic information, among others.
p) Enter into employment, apprenticeship, services or any contracts that apply.
q) Comply with any other benefit derived from the contractual relationship between the Data Subjects and the Organization.
r) Inform instructions when hiring Data Subjects, if applicable.
s) Assess the performance of the Data Subjects.
t) Manage payroll, payment of financial support, among others, by the Organization or a third party; manage and make the necessary payments to the bank account indicated by the Data Subjects or entities expressly indicated by the Data Subjects.
u) Contract life insurance and medical expenses with the Organization or a third party.
v) Notify relatives of the Data Subjects in cases of emergency during working hours or in connection with contract performance.
w) Communicate, reproduce and publish photographs and/or videos of the Data Subjects by the Organization for marketing and advertising purposes, in the Organization's internal or external media.
x) Maintain the health and safety of the Data Subjects in the workplace directly by the Organization or by a third party, in accordance with the regulations applicable to the Occupational Safety and Health Management System (hereinafter "OSHMS").
y) Collect information and evidence in order to carry out disciplinary processes, if applicable.
z) Use the information for procedures and documents related to the contractual relationship of the Data Subjects with the Organization.
aa) Send information about the Organization to the Data Subjects.
bb) Communicate and carry out well-being activities for the Data Subjects and their families within the Organization.
cc) Take photographs of the Data Subjects and their families in the framework of well-being activities or other activities.
dd) Decision-making in labor and/or contractual matters regarding the performance and termination of the contract with the Data Subjects, either by the legal area of the Organization or its external advisor.
ee) Transfer the Personal Data of the Data Subjects to GEB companies located inside or outside of Colombia for the aforementioned purposes.
ff) Nationally or internationally transfer and/or transmit the Personal Data of the Data Subjects to third parties or business partners for the purpose of business prospecting or marketing.
gg) Transfer the Personal Data of suppliers within the framework of the definition, structuring and execution of strategic transactions, such as the sale of assets in the event that the Organization or parts of its business are sold, merged or acquired by third parties.
hh) Transmit the Personal Data of the Data Subjects for them to be processed by third parties, as Processors, located in Colombia or abroad, for the aforementioned purposes.
ii) Register the employee in the computer systems of the Organization, for the accounting, administrative and financial activities inherent to the contractual relationship.
jj) Coordinate professional development and training programs for employees and access to computer resources for this purpose.
kk) Use the provided information to carry out forensic analyses and investigations directly or with

the assistance of third parties, whether of a private nature or by court order in order to protect and safeguard the assets of the employee or GEB.

**II)** The other necessary purposes provided in the context of labor or contractual performance to comply with the object and the obligations derived from the relationship between the Data Subjects and the Organization.

### Specific Purposes of Personal Data Processing for Clients

The Personal Data owned by GEB clients will additionally be processed for the following specific purposes:

**a)** Prepare a data record for sales.

**b)** Contact the data subject by telephone, e-mail, chat or SMS, to carry out satisfaction surveys.

**c)** Prepare and update a record of sales statistics.

**d)** Report, under the terms of Law 1266 of 2008, before any information operator or legally authorized risk center, on timely compliance or non-compliance with monetary obligations or duties of patrimonial content, presenting truthful, pertinent, exact, complete and updated information.

**e)** Transfer the Personal Data of clients within the framework of the definition, structuring and execution of strategic transactions, such as the sale of assets in the event that the Organization or parts of its business are sold, merged or acquired by third parties.

**f)** Transmit the Personal Data of customers to be processed by third parties, as Processors (e.g., third party marketing companies) located in Colombia or abroad, for the aforementioned purposes.

**g)** Subsequently contact customers through calls, email, and any other means of communication to inquire about possible purchase interest.

**h)** Carry out campaigns to send information to e-mails, through social networks or other third-party platforms, about brand promotions, events, products and services that may be of interest.

### Privacy and video surveillance notices

In order to comply with Decree 1377 of 2013, compiled in Decree 1074 of 2015 and Law 1581 of 2012, GEB has made its Privacy and Video Surveillance Notice available by means of which it notifies data owners of the processing conditions for their personal data.

The GEB Privacy Notice is published on the website www.grupoenergiabogota.com.co and in our offices. Regarding the Video Surveillance Notice, it is installed in GEB offices that have a closed circuit television video surveillance system. The notices placed in the offices are installed in places of easy access and identification.

### Guidelines for video surveillance in GEB facilities

This guideline is of general and mandatory observance for all GEB personnel. The purpose of video surveillance is to maintain the safety of people who enter the Organization's facilities by recording images captured by fixed video cameras installed in places designated for this, for the purpose of identifying risky behaviors constituting a crime or endangering the people who work and enter the Organization and its facilities.

**General parameters**

**a)** Fixed video surveillance cameras are installed in GEB that make up a closed television system with real-time recordings that saves images that will be kept for a maximum period of 180 days (the Security Area will establish the period of conservation of the information) under the protection and responsibility of the Security Area.

**b)** The data collected through video surveillance systems may be used to collect information and evidence to carry out disciplinary processes or internal investigations, if applicable.

**c)** The security team is authorized to perform the following functions:

- Ongoing recording in digital video format of the selected perimeter;
- Daily storage of the videos obtained by the video surveillance cameras for a limited period of time, designated by the Security Area. If no situation is reported that warrants the review of the videos, they will be automatically removed by the automatic overwriting mechanism.
- The following are considered a risk situation that warrants the review of the videos: - Theft of equipment or any asset owned by GEB, - Vandalism in equipment or physical facilities of GEB, - Alterations in the configuration of GEB equipment, and - Behaviors that may constitute crimes, among others.

**d)** Review of video-recorded material: GEB staff, upon identifying any of the aforementioned risk situations, must notify the Security Area so that, in coordination with the technology area, they will carry out the review of the video-recorded material and proceed to identify the risk situation or possible crime.

**e)** Prohibitions: The staff responsible for the video surveillance system must make proper use of it solely for the established purposes. Therefore, the following practices are prohibited:

- The creation of photo files;
- Unauthorized disclosure of the material obtained in the video recording;
- Recording of specific areas or people and for purposes other than those previously established; and
- Any others that are contrary to the purposes set out in these guidelines.

## Guidelines for the collection of personal data in the Human Talent process

The personal data of employees candidates, active employees, SENA apprentices, university interns, family members of employees, former employees, among others, are directly linked to the Talent Management Department. This Department is in charge of the reception, custody, storage and final disposal of the information associated with personal data of data owners of the aforementioned information.

**Selection process**

a) **Collection of Resumes:** The Organization has established different types of procedures to announce job vacancies, collecting information through the publication of vacancies in employment search engines on the web and in the official accounts of the Organization on social networks.

b) **Selection of candidates:** Resumes that are received by the Organization are subject to review and provide a process in the selection of the candidate in accordance with the parameters established by the Talent Management Department. Once the candidate selection process is completed, the employee candidates begin the selection process, through which they are called for interviews, knowledge or psychotechnical tests, home visits, security studies, psychotechnical tests, among other activities of the selection process.

Once GEB has selected the candidates who will complete the selection process, it requests each candidate for their authorization for the processing of personal data collected in said process, through the form **CUM-MAN-004-F-002 Authorization for the processing of personal data - applicants**.

Once GEB concludes the convened selection process, it will store the resumes received within the framework of this process for a maximum term of one (1) year, after which it will eliminate the resumes received.

c) **Hiring process:** The hiring process is defined by procedures that compose it. However, in relation to the protection of personal data, the Talent Management Department and the process leader who is carrying out the hiring, must guarantee that the employee signs the form **CUM-MAN-004-F-001 Authorization for the processing of personal data-employees.**

By means of this authorization, the employee will grant the Organization their consent to carry out the processing of their personal data for the purposes required by the Organization and published on our website. *Personal Data Processing Policy.*

d) **Storage of work histories of active and inactive employees:** The work histories of active or inactive employees must be protected under security conditions that prevent access by third parties or unauthorized persons.

e) **Taking occupational medical exams:** Within the process of contracting and performing contracts, there are occupational health provisions that oblige the Organization to carry out

occupational medical examinations for onboarding, regular exams and retirement exams, on a case-by-case basis.

In cases in which occupational medical examinations must be carried out, the results thereof must be safeguarded by the Organization, guaranteeing compliance with adequate security measures for the storage thereof, taking into account the sensitive nature of this personal information. This information may only be accessed by those who, due to their functions or role, should know it.

f) **Medical disabilities:** Medical disabilities, being sensitive information due to their medical content, must be guarded with adequate measures to guarantee and prevent access by unauthorized third parties or employees. The storage of these must be focused so that the consultation of the information can only be carried out by those who have the right to do so in order to do their work at the Organization, and these officials must keep this information absolutely confidential.

### Guidelines for the collection of personal data in the linking of bidders, contractors and/or suppliers

Upon linking the bidders, contractors and/or suppliers, our Organization will collect their authorizations for the processing of the personal data collected, those owned by the legal representative of the legal entity, the contact authorized by the supplier for the communications that are the object of the signed contract, or of any individual whose personal data is provided to GEB. Authorization will be requested through the technological tool provided by the Supply area.

### Guidelines for handling photographs and/or videos

Prior to the registration of images, whatever their photography, illustration or video format and whose objective is their publication in printed, online and/or audiovisual media, GEB will implement the following parameters to protect the fundamental rights of their data subjects and comply with personal data protection regulations.

**General parameters**

a) Images whose purpose is publication in magazines, advertising, social networks, among others, must also have the authorization of the Data Subject for the assignment of the rights to use their image in these contexts. To do this, the area responsible should use the form **CUM-MAN-004-F-004 Authorization for the processing of personal data- employees, use of image and the assignment of equity rights.**

b) Obtain prior consent for the recording and publication of photographs in any eventuality. This consent must have the specific purposes for which that photograph will be used.

c) In the case of personal images that are in the image bank authorized by GEB, it must be verified that said images have the authorization of their data owner for the processing and the intended purpose.

d) In the event that an image and/or photograph recorded by a third party external to GEB is used, it must be verified that it has the authorization in due form of the Data Owner of the

image.

**e)** Apply corrective anonymization measures in the event that it has not been possible to obtain the consent of the data subjects of the images to be processed.

**f)** The processing of personal images must ensure compliance with fundamental rights such as dignity or good name and, in particular, prevent the use of personal images from generating any type of discrimination.

**g)** When taking photographs and/or recordings during events and meetings, the data subjects must be shown, in a visible place, a notice prior to taking them that notifies of the processing of their personal data and includes the minimum information requirements established by law, as follows:

***DATA PROTECTION NOTICE***

*Dear attendee, you will be recorded during the duration of this meeting by Grupo Energía de Bogotá S.A. ESP (hereinafter "GEB"), identified with NIT 899.999.082-3 and with address in Bogotá DC, address Carrera 9 No. 73 – 44 Floor 6. The GEB will process your personal data by taking photographs and/or voice and video recordings, which is why, by remaining at this event, you authorize the processing of your personal data. The collection, storage, use and circulation of the photographs and recordings taken during the event will be done for the following purposes: i) Record your image by taking photographs or recording film evidence in order to have evidence of the events held by GEB. ii) Publish the photographic and film evidence on our website, social networks and other internal and external communications media.*

*As the owner of the information you have the following rights: (i) access free of charge to the personal data provided to GEB that have been processed; (ii) to know, update and correct your personal information; (iii) to request proof of the authorization granted to GEB; (iv) to be informed by the responsible person or person in charge of the use that has been given to your personal data; (v) to file complaints before the Superintendence of Industry and Commerce for violations of the provisions of the current regulations; (vi) to revoke the authorization granted and request the deletion of the data when the principles, rights and constitutional and legal guarantees are not represented; (vii) to refrain from answering questions about sensitive data or data concerning children and adolescents. You may exercise any of your rights, including, without limitation, your rights of access, rectification, cancellation and opposition (ARCO), by sending an e-mail to datospersonales@geb.com.co or at the address: carrera 9 No. 73 - 44 Piso 6.*

*GEB is committed to keeping personal data protected, so please be informed that you may consult our **Personal Data Processing Policy** and/or any substantial change in it on our website www.grupoenergiabogota.com.*

### Special parameters for the use of images of minors

GEB, prior to recording images where minors appear, will obtain the respective consent of the legal representatives or guardians. For the use of personal images of minors, GEB will apply the following additional criteria to the requirements set forth in the law for the authorization of data processing:

**a)** The processing responds to the best interests of the children and adolescents.

**b)** Observation of the fundamental rights of children and adolescents is ensured.

**c)** According to the maturity of the child or adolescent, their opinion is taken into account.

Therefore, it will take into account that the data of children and adolescents may be processed as long as the prevalence of their fundamental rights is not put at risk and it unequivocally responds to the realization of the principle of their best interests.

At events where the image or photograph desired is of a minor, the authorization of their registered agent must be requested though the form **CUM-MAN-004-F-005 Authorization for the processing of minors' personal data.**

### Guidelines for the processing of personal data related to COVID-19

GEB collects sensitive health data from all its employees through the daily health report which, in turn, collects information related to the vaccination process, among other aspects related to biosecurity protocols.

Prior to the collection and processing of personal data related to the COVID-19 pandemic and the biosecurity protocols implemented as a consequence thereof, GEB will implement the following parameters to protect the fundamental rights of its data owners and comply with personal data protection regulations.

**General parameters**

**a)** The personal data collected in relation to COVID-19 and the biosecurity protocols adopted by GEB will be those expressly required by the Ministry of Health and Social Protection for the purposes of complying with the protocols.

**b)** Obtain prior consent for the collection and processing of personal data related to biosafety protocols. This consent must have the specific purposes for which that information will be used. These purposes may only be those indicated by the Ministry of Health and Social Protection.

**c)** When prior consent for the collection and processing of personal data related to COVID-19 is being obtained, the citizen must be informed of the specific rule that orders the collection of the requested data to comply with biosafety protocols.

**d)** GEB will implement any technical, human and administrative measures that are necessary to provide security to personal data, avoiding its adulteration, loss, consultation, use or unauthorized or fraudulent access, as well as guaranteeing the principles of confidentiality, access and restricted circulation.

**e)** The personal data collected in relation to COVID-19 and the biosafety protocols will be stored only for the reasonable and necessary time required to fulfill the indicated purposes. Once the purpose has been fulfilled, GEB will delete the collected data.

f) The databases that are created to comply with the biosecurity protocols adopted by the GEB and ordered by current regulations will be registered with the National Registry of Databases.

**Special parameters for the use of sensitive data - health data**

Prior to the collection and processing of sensitive data related to COVID-19 and the adopted biosecurity protocols, GEB will obtain the respective consent of the data owners, except in cases where the law does not so require. For the processing of sensitive data, GEB will apply the following additional criteria, in accordance with Law 1581 of 2012, Decree 1377 of 2013 and other regulations that regulate the matter:

a) Notification to the data subject that because these are sensitive data, the data subject is not obligated to authorize the process.

b) Notification to the data subject that because these are sensitive data, the data subject is not obligated to answer questions related thereto.

c) No activity may be conditioned on the data subject providing sensitive personal data.

d) The collection, use, circulation and processing of sensitive data will be surrounded by special care and diligence in their collection, use, security or any other activity that is carried out with them.

### Guidelines related to the processing of data in work meetings through corporate tools

GEB has corporate tools for its work meetings, where the employees who attend can record the meeting and have access to said recordings. These guidelines are mandatory for all GEB staff and establish the general parameters that must be respected for proper compliance with Colombian personal data protection regulations.

**General parameters**

a) Attendees should be notified in advance when meetings are recorded and/or monitored for later access, use, and storage.

b) In accessing the recordings of GEB staff meetings, privacy and confidentiality must be respected and guaranteed in the use of information technologies. Likewise, when making use of technological resources, all users will do so responsibly, efficiently, effectively, ethically and legally.

c) The voice and/or image recordings that are collected for these purposes must be kept under information security and confidentiality measures.

d) Appropriate use should be made of voice and/or image recordings only for the purposes previously established and authorized by the data subjects.

## Organization Databases

**Inventory of the personal data that make up a database**

In order to give adequate processing to personal data, GEB will identify and keep the inventory of personal data updated, defining and validating the elements described below:

**a)** Identification of the information databases where personal data is stored.

**b)** Nature of personal data contained in each of the databases.

**c)** Number of data subjects associated with each of the databases.

**d)** Purposes of the processing for each of the databases.

**e)** The data processors associated with each of the databases.

**f)** Information security measures for each of the databases.

## Criteria that define a database

A database is defined as an organized set of personal data that is subject to processing[19]. Databases can be classified into two categories: (i) Physical databases: Those whose personal information is organized and stored physically and; (ii) Automated Databases: Those whose information is organized and stored with the help of computer tools.[20]

The criteria that GEB has established for the identification of its databases are set out below:

| CRITERION | DATABASE | INFORMATION REPOSITORY |
|---|---|---|
| **Identity** | Associated with the content that allows a specific group of people to be identified. The database is characterized by containing data that directly reveal the identity of a group of people associated with a purpose of the database. | A repository will contain anonymous information or elements that make it difficult to determine the data subjects whose information belongs to them. |
| **Formality** | Refers to the structure of the database that allows a consultation or registration of personal information within the activities of a process. | Characterized by performing the unnecessary or uncontrolled replication of the personal information required for the activities of a process. |



[19] Law 1581/2012, Article 3 (b).
[20] Decree 1074/2015, Article 2.2.2.26.2.6

| | | |
|---|---|---|
| **Structure** | The structure of the database is identified as that characteristic that allows establishing the content or entry of its information in a predetermined or standardized way. | Non-homogeneous content, which does not reflect consistency with the relationship of personal data established in it; information may be included in an inconsistent manner. |
| **Term** | Its purpose is associated with the conservation of the information incorporated in it, with the purpose of making consultations or serving as input for decision-making. This keeps information of a personal nature for a certain period of time, during which its content is required for its practical utility or by legal requirement. | It is in temporary transit within the activities of the process or is characterized by being a flow of information from a formal database destined for another formal database or an informal data repository. |
| **Unit** | The content is associated with a purpose and means. Example: Documentation stored in several physical folders that have the same purpose. | This, despite having the same content, is found in different storage media or is registered under criteria whose purpose is not the same. |



The previously described criteria have been defined as an instrument that allows the identification of databases that, due to their structure, can be reported or registered with the National Registry of Databases -RNBD- of the Superintendence of Industry and Commerce.

Based on the exposed criteria, GEB registered its databases before the National Registry of Databases -RNBD- of the Superintendence of Industry and Commerce.

### Permanence of the databases

GEB may only collect, store, use or circulate personal data for as long as is reasonable and necessary, in accordance with the purposes that justified the processing, taking into account the provisions applicable to the matter in question and the administrative, accounting, tax, legal and historical information aspects.

Once the purpose or purposes of the processing have been fulfilled and without prejudice to legal regulations that provide otherwise, the Organization must proceed to delete the personal data in its possession. Notwithstanding the foregoing, personal data must be kept when required to comply with a legal or contractual obligation.

### Determination of the data subjects that make up the database

Determining the number of data subjects in a database allows control over the flow of information that makes it up. The methodology for identifying the number of data subjects that make up the databases is established below:

a) **Consecutive:** It is the mechanism by which the total number of data subjects is determined,

through the last data recorded in a consecutive numerical control of entries to the database. In general, there are indices that allow determining the ascending numerical follow-up of the records.

**b) Count:** It is the procedure through which the data subjects registered in the database are counted one by one.

**c) Estimated:** In accordance with the nature of the database and given the impossibility of carrying out a count through consecutive or counting, an average of data subjects will be globally verified in accordance with the established records that allows to account for the income of information recorded in the database. This method will be applied in cases in which, due to the volume of information, a count could not be carried out in a reasonable time.

### Registration of Personal Databases in the RNBD

GEB must register all Personal Databases in the RNBD within the following two (2) months, counted from their creation. The record must be updated in the terms indicated below:

a) Annually, between January 2 and March 31.

b) When Substantial Changes are made to the registered information, these changes must be registered within the first ten (10) business days of each month.

c) When claims are submitted by the Data Subjects, the update must be made within the first fifteen (15) business days of the months of February and August of each year.

d) When there are security incidents related to the violation of security codes or the loss, theft and/or unauthorized access of information from a Database managed by GEB, it must be reported to the RNBD within fifteen (15) days business days following the time they are detected and brought to the attention of the GEB Personal Data Protection Officer.

To update the databases, the GEB has the procedure **CUM-PRO-025 National Registry of Databases.**

## 2. GUIDELINES FOR THE USE OF PERSONAL DATA

### Scope of application

The provisions contained in these guidelines will be applied to all forms of personal data processing carried out by GEB, since, in its capacity as Data Controller, it must obtain the prior, free, express and informed consent of the data subjects, as established in article 9 of Law 1581 of 2012.

### Confidentiality of personal information

In the performance or exercise of their functions, our Organization's employees may make use of the personal information entrusted to GEB by their data owners. In regard thereof, all employees have the obligation to safeguard the confidentiality of the information and to handle it appropriately. This obligation continues even after the employment relationship with our Employees has ended.

Through this Manual, the Organization establishes the guidelines and directives that must be followed by its employees, especially those related to confidentiality, the protection of personal

information and the proper use thereof. Some guidelines that GEB employees must abide by, regarding the privacy of personal information are:

**a)** Comply with guidelines, procedures and processes for storing, saving, and controlling access to sensitive electronic and physical information.

**b)** Follow all guidelines, procedures and processes for transmitting confidential information.

**c)** Do not send confidential information through insecure means such as e-mail or the Internet (this includes internal social media platforms). Secure email operating procedures must be followed when sending sensitive information outside of GEB.

**d)** Do not carelessly display confidential information (e.g., leaving information on a computer screen, or confidential documents in plain view, or that may be lost or misplaced).

**e)** Do not disclose confidential information to persons outside of GEB (including family or members thereof or close associates) or to other employees who do not require the information to do their jobs.

**f)** Be careful not to discuss confidential information where it could be overheard or intercepted (such as when using a cell phone), for example, making sure who you are talking to and that your conversation cannot be overheard by unauthorized persons. Do not discuss confidential information in public places, such as restaurants, elevators and other public places.

**g)** Destroy or dispose of information in accordance with security requirements and in accordance with the guidelines and procedures for the retention and destruction of documents.

**h)** Know and comply with GEB's Personal Data Processing Policy, as well as the other guidelines and procedures that it has established to protect personal information.

**i)** Do not access personal information of a data subject without a legitimate business reason and with the proper authorization.

**j)** Request the performance of Data Protection Impact Assessments in the required events.

**k)** Report personal data protection incidents appropriately and promptly.

**l)** GEB staff will refrain from using databases that do not have the authorization of the data owner or that do not come from public records, since they are aware that personal information can only be used if it has been duly gathered and authorized.

**m)** All GEB officials must use the information for the sole purpose of fulfilling the assigned tasks related strictly to the operation of each unit.

**n)** GEB staff must at all times be aware that the lack of authorization for the processing of personal data generates a breach of current regulations on data protection, since the data owner does not empower the employee but rather the entity to process their personal data. It must be remembered by all employees that the authorization falls on the GEB. In the case of personal data from public records, the prior authorization of the data subject is not required for it to be processed, but the other provisions contained in the regulations for its proper use must

be complied with in any case.

**o)** In the event that the entity's staff carry out any activity that implies the collection of personal data, they must always use the forms authorized by the entity. Once the collection forms are completed by the data subject, they must safeguard said documents and may not at any time create databases with said information for personal use.

**p)** No GEB employee may reveal information that is sensitive or confidential and that they know by reason of their work activity.

**q)** All GEB workers and/or third-party Managers must maintain the confidentiality of the personal data processed by GEB. All contracts entered into by GEB with its employees or with third parties who will have access to the personal data contained in the GEB databases must contain a confidentiality clause regarding said personal data. Personal data may only be processed for the purposes described in this Manual or in GEB's Personal Data Processing Policy.

**Note:** In the event that you have concerns about the confidentiality of certain information, you should approach the GEB Personal Data Protection Officer so that they allow you to be clear about the special obligations of care that may exist regarding certain information.

### Internal sanctions

Failure to comply with the obligations described in this Manual by Employees of the Organization will result in disciplinary sanctions in accordance with the Internal Work Regulations.

### Sanctions for breach of the duty of confidentiality

Any violation of the confidentiality obligation by workers will be considered a violation of the Employment Contract, and will be subject to the consequences contained therein.

Likewise, any infringement of the confidentiality obligation by third-party Managers that puts Personal Data at risk, may be grounds for termination of the respective contracts with said Managers.

### Criminal sanctions for the unauthorized processing of personal data

In accordance with Article 269F of the Penal Code, it states the following:

> *"Violation of Personal Data. Whoever, without being empowered to do so, for their own benefit or that of a third party, obtains, compiles, subtracts, offers, sells, exchanges, sends, buys, intercepts, discloses, modifies or uses personal codes, Personal Data contained in files, archives, Databases or similar means, will incur a prison sentence of forty-eight (48) to ninety-six (96) months and a fine of 100 to 1000 current legal monthly minimum wages."*

GEB may file the corresponding complaints in the event that it is aware of the participation of any worker or third party linked to GEB in the commission of the conduct established in article 269F of the Penal Code, when these are carried out in relation to Personal Data contained in GEB Databases.

Workers who access the GEB Databases must perform the Processing in strict compliance with GEB's Personal Data Processing Policy, and those established in this Manual.

### Security of personal information

The Organization has an Information Security Program that aims to ensure the confidentiality of the information in its custody, guaranteeing its integrity and ensuring the availability and continuity of the systems.

All guidelines and procedures that are an integral part of the GEB Information Security Program must be fully known and applied by the Organization's employees. These have the responsibility to protect the information, whether it is proprietary information or information entrusted to GEB by the data owners. Therefore, they must exercise the care, diligence and skill that would be expected of a reasonably prudent person when dealing with personal information.

To guarantee compliance with the guidelines that are part of the Information Security Program, activities are carried out that guarantee administrative, technical and physical measures that allow:

**a)** Maintain the information under the conditions necessary to prevent adulteration, loss, consultation, unauthorized or fraudulent use or access, for which it has **GTI-MAN-002 Methodology for the management of information assets**, which sets out the steps for the identification, valuation, classification, protection and review or update of GEB's information assets.
**b)** Implement, operate, monitor, review and improve information security measures; for which there are information security guidelines in the document **GTI-MAN-003 Manual of cybersecurity standards for operating infrastructure,** which make it possible to reduce risks linked to threats to GEB's technological infrastructure, guaranteeing the protection of personal data, among other risks associated with the information of GEB.

### Privacy by design and by default

The Superintendency of Industry and Commerce has referred to privacy by design and by default (*Privacy by Design and by Default*) as a proactive measure to comply with the Principle of Demonstrated Responsibility that promotes the vision that the future of privacy cannot be guaranteed only by complying with regulatory frameworks; rather, privacy assurance should ideally become an organization's default mode of operation.

Given the foregoing, the control entity recommends that, prior to any collection of information and throughout its life cycle, organizations adopt preventive measures of a diverse nature (technological, organizational, human and procedural, among others) in order to avoid violations of the right to privacy or confidentiality of information, as well as security failures or improper processing of personal data.

The technological, human, administrative, physical, contractual and any other measures adopted by the organizations must tend to avoid:

**a)** Improper or unauthorized access to information.

**b)** Information manipulation.

**c)** Destruction of information.

**d)** Improper uses or non-authorization of the information.

**e)** Circulate or provide the information to unauthorized persons.[21]

In turn, Decree 620 of 2020, in its Article 2.2.17.1.6. "Principles", defines privacy by design and by default as:

> *"Privacy and security must be part of the design, architecture and default configuration of the information management process and the infrastructures that support it. For this purpose, before information is collected and throughout its life cycle, preventive measures of a diverse nature (technological, organizational, human, procedural) to avoid violations of the right to privacy or confidentiality of information."*[22]

GEB has decided to implement the procedure **CUM-PRO-038 Assessment of the Impact of Personal Data Protection** by which it implements the aforementioned best practices regarding privacy by design and by default. The impact of Personal Data Protection is assessed through this procedure via Personal Data Protection Impact Assessments that are essential to assess in advance the impact of GEB's activities from the point of view of Personal Data Protection and to mitigate risks.

### New products, services or personal data collection channels

For the development, structuring, improvement or modification of the products or services provided by the company, or the development of marketing plans or technological adaptations, among others, in which it is necessary to obtain, deliver, store or carry out any type of processing or activity on personal data or databases must have the prior written opinion of the Personal Data Protection Officer, who will be in charge of implementing mechanisms that guarantee Privacy by design and by default in these new strategies of the Organization, carrying out the respective Personal Data Protection Impact Assessment mentioned in the previous section.

### Management of Personal Data Protection Incidents

Personal Data Protection Incidents occur for various reasons ranging from simple human error to attacks directed from outside. Effective and timely management of incidents at the time they occur is critical to containing the impact. Incidents that are not dealt with in an efficient and timely manner can grow in terms of magnitude and could lead to adverse consequences for GEB, its clients, suppliers, employees and other data subjects.

The GEB Personal Data Protection Officer must know, analyze and promptly report any events that can be classified as Personal Data Protection Incidents before the Control Authority within the established legal deadlines.

GEB has the procedure **CUM-PRO-037 Management of Personal Data Protection Incidents**

[21] Superintendency of Industry and Commerce, Marketing, Advertising and Personal Data Processing Guide, page 12.
[22] Decree 620/2020, Article 2.2.17.1.6.

through which details the activities to address incidents involving the loss, inappropriate collection or access, use, disclosure, retention or destruction of personal data belonging to GEB data subjects.

### Management of Consultations and Claims in Personal Data Protection

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) on any of the channels authorized for this purpose, which are published in our Personal Data Protection Policy.

GEB has the procedure **CUM-PRO-035 Management of Consultations and Claims regarding the Protection of Personal Data**, which makes it possible to stipulate the activities that are carried out by the Personal Data Protection Officer at the time of responding to a Personal Data Protection consultation or claims.

### Procedures for the exercise of the rights of Access, Rectification, Cancellation or Opposition (ARCO)

In compliance with the constitutional and legal provisions, GEB as Controller for the Processing of personal information, must guarantee the data owners the exercise of the following rights:

**a)** Know, update and rectify their personal data.

**b)** Requesting proof of authorization granted to GEB, except when expressly exempted as a requirement for Processing, in accordance with provisions of Article 10 in Law 1581 of 2012.

**c)** Being informed by GEB, upon request, as to how they Process their Personal Data.

**d)** Submit to the Superintendency of Industry and Commerce complaints for violations of the provisions of Law 1581 of 2012 and other regulations that modify, add to or complement it.

**e)** Revoking the authorization and/or requesting deletion of the data when the process fails to observe constitutional and legal principles, rights and guarantees. Revoking and/or deleting data will apply when the Superintendence of Industry and Commerce has determined we have incurred in conducts that violate the law and Constitution during Processing.

**f)** Accessing the personal data that was subject to processing, free of charge.

**g)** Refraining from answering questions or providing information related to your Sensitive Data, without this conditioning any activity or service.

Only the following individuals may exercise these rights:

**a)** The Data Subject, who must sufficiently prove their identity.

**b)** Their successors, who must verify said capacity.

c) The Data Subject's representative and/or attorney-in-fact, upon accreditation of the representation or power of attorney.

d) By stipulation in favor of another or for another person.

The data subjects have the right to access their Personal Data and the details of the Processing of said personal information, as well as to rectify and update them if they are inaccurate, or to request their deletion when they consider them excessive or unnecessary for the purposes that justified them being obtained, or oppose the Processing of these for specific purposes.

**Consultation Management**

Authorization for the Processing of personal information in the different scenarios described in the Personal Data Processing Policy will be obtained by GEB, through requests made available to the data owners in each of the information capture channels or points associated with our activities. Through the Consultation procedure, the data owner may:

a) Request access to his/her personal information.

b) Request proof or evidence of the authorization granted by you to GEB for the Processing of your personal information.

c) Inquire on the use given to his/her personal information.

Consultations must be submitted through the authorized channels and following the procedure described below:

1. At any time and free of charge, the data subject or his representative may make inquiries regarding the Personal Data that are subject to Processing by GEB. In all cases, the identity and the power to make the consultation must be proven.
2. The consultation will be addressed within ten (10) business days from the date it is received. When it is not possible to address the consultation in that time, the interested party will be notified, stating the reasons and indicating the date the consultation will be resolved. Under no circumstances may that period exceed five (5) business days after the expiration of the first term.

**Internal procedure for dealing with consultations.**

When a consultation is submitted, the Personal Data Protection Officer will act in accordance with the provisions of the procedure **CUM-PRO-035 Management of Consultations and Claims for the Protection of Personal Data.**

**Claims Management**

The data subject 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, through the

presentation of a claim that will follow the following procedure.

1. At any time and free of charge, the data subject or his representative may make inquiries regarding the Personal Data that are subject to Processing by GEB. In all cases, the identity and the power to make the claim must be proven.
2. The claim will be addressed within a maximum term of fifteen (15) business days as of the day after the date of receipt. When it is not possible to address the claim in that time, the interested party will be informed of the reasons for the delay, indicating the date the claim will be addressed. Under no circumstances may this exceed eight (8) business days after the expiration of the first term.

**Internal procedure for handling complaints.**

When a claim is filed, the Personal Data Protection Officer will act in accordance with the provisions of the procedure **CUM-PRO-035 Management of Consultations and Claims for the Protection of Personal Data.**

**Requirements for addressing consultations and claims**

The minimum requirements established in the Personal Data Processing Policy are stipulated in Law 1755 of 2015, regulations that regulate the Right of Petition in Colombia. According to the above, the request must be addressed to GEB and have at least the following items:

a) Contain the identification of the Data Subject (name and identification document).
b) Contain the description of the facts that generated the consultation or claim.
c) The purpose of the request.
d) Specifying the notification address of the Data Subject, either physical or electronic (e-mail).
e) Attaching the documents the petitioner wishes to use for support (especially for claims).

If the data subject wishes to present a consultation or a claim through third parties, after accreditation of the representation or power of attorney, the request must contain:

a) Identification of the authorizing data subject.
b) A copy of the citizen's I.D. or I.D. of the data subject.
c) Name, identification data and copy of the I.D. or identification document of the authorized person.
d) The time for which they can consult, update or correct the information (only once, for one year, for the duration of the legal relationship, or until further notice, etc.).
e) The voluntary and discretionary nature of the authorization.

**Prerequisite for submitting complaints to the Superintendence of Industry and Commerce**

In the event that the data owner wishes to file a complaint with the Superintendence of Industry and Commerce regarding Personal Data, the data owner must have previously exhausted the consultation or claim process with GEB in accordance with the aforementioned indications; we declare our total willingness to address his concerns.

**Corrections or updates of the data owner's personal data.**

The claim consisting of the correction of personal data must, in addition to the requirements stipulated above, contain the specification of the corrections to be made and supporting documentation for the request.

**Partial or total revocation of the Processing authorization.**

Data subjects have the right to revoke the authorization when the constitutional and legal principles, rights and guarantees are not observed in the process, which shall prevail in cases in which, once the request is made, the Organization so determines, or when the personal data protection authority so orders. However, if the Organization considers that the revocation is not admissible, it will inform them by means of a communication with supporting arguments. Once the authorization has been revoked, the Organization can proceed to delete information contained in the respective databases.

**Service channels for consultations and claims**

GEB has implemented the following channels to guarantee the exercise of the rights of the data owners. The established channels are:

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

Personal Data Subjects or third parties authorized by law to act on their behalf may use these channels to exercise their rights.

**About the area responsible for processing consultations and claims.**

GEB, through the Personal Data Protection Officer, who is part of the Corporate Compliance Department, will address all requests, consultations and claims of the data owners so that they can exercise their rights to know, update, rectify and delete the data and revoke the authorization related to the protection of Personal Data.

## Personal Data Protection Training Program

GEB understands that, in order to guarantee an adequate processing of the personal data of its data owners, it must tend to generate spaces of knowledge that consolidate the culture of Compliance and Data Protection within the Organization and in its employees.

For this reason, our Organization has a Personal Data Protection Training Program, through which it trains its employees in the proper processing of the personal data of GEB's data owners, and their role in guaranteeing compliance with the guidelines of the Organization regarding the Protection of

Personal Data.

The Personal Data Protection Officer is responsible for designing, managing and supervising the Training Program on Personal Data Protection within GEB. The execution of this program will be carried out jointly by the Personal Data Protection Officer and the GEB training area.

The training program has different mechanisms through which our employees are educated on the protection of personal data. These mechanisms are listed below:

a) Training programs, internal or external, on the protection of personal data for all company employees (new and old).
b) Special training programs, internal or external, for senior management and for officials who, due to the type of function they perform, have greater responsibility in the management of personal data.
c) Training programs for strategic allies that process personal data on behalf of the company.
d) Measurements of the assessment and participation of officials.
e) Establish a question bank for the assessments.

### Internal Governance of Personal Data Protection

In its capacity as Data Processing Controller, GEB understands the importance of complying with the Principle of Demonstrated Responsibility implemented by Decree 1377 of 2013 and by the Guide for the Implementation of the Principle of Demonstrated Responsibility of the SIC. Due to the foregoing, it has implemented appropriate and effective internal measures and/or guidelines to comply with the applicable Law, regarding the comprehensive protection of Personal Data. As a parameter for the approach of these measures, the provisions of Article 27 of Decree 1377 of 2013 have been followed by requiring that the measures must guarantee:

- The existence of an administrative structure proportional to the structure and business size of the Data Controller for the adoption and implementation of guidelines consistent with the applicable Law.
- The adoption of internal mechanisms to put these guidelines into practice including implementation tools, training and education programs.
- The adoption of processes for addressing and responding to the consultations, requests and claims of the Data Subjects, with respect to any aspect of the Processing.

#### Administrative and Compliance Structure

In order to ensure high standards of compliance with data protection regulations, certain functions are assigned to some areas of the organization, which will have the following functions:

#### Board of Directors

The board of directors will have the functions of:

- Support, through the provision of financial and personnel resources, to GEB for the administration and operation of the Data Protection Program;

- Review and reach decisions on the management report of the Compliance Department regarding the personal data protection program.

**Audit and Risk Committee of the Board of Directors**

The Audit and Risk Committee of the Board of Directors will have the following functions in relation to Personal Data Protection:

- Review and assess the periodic reports submitted by the Corporate Compliance Department and/or the Personal Data Protection Officer on compliance and other issues related to GEB's Personal Data Protection Program.
- Make the recommendations that they consider pertinent so that within the Organization there is adequate compliance with regard to the protection of personal data.
- Promote the consolidation of the organizational culture of Personal Data Protection.

**Senior management**

GEB senior management is responsible for managing the risk of noncompliance with the data protection program as part of their overall responsibilities for managing compliance risk. They responsible for creating a suitable control environment and contributing to the maintenance of a robust and effective data protection culture. For the above, the following functions are carried out by senior management:

- Support and generate within GEB a culture of respect for data protection;
- Approve the personal data protection policy.
- Support and socialize within the teams the communications, training and collection of information initiatives associated with the implementation of the PDP program.
- Designate and appoint the GEB Personal Data Protection Officer.

**Compliance Department**

The Compliance Department will have the following functions:

- Submit a periodic report to the Board of Directors and senior management, at least once a year, on the operation, compliance and monitoring of the data protection program.
- Carry out the definition, execution and monitoring of the Personal Data Protection Program, ensuring regulatory compliance as part of the Compliance Program.
- Inform the Audit and Risk Committee of the Board of Directors any deviation, opportunity for improvement on the personal data protection program and the monitoring and follow-up carried out on it.

**Personal Data Protection Officer**

The Personal Data Protection Officer will have the following functions:

- Coordinate the definition and implementation of the controls of the Comprehensive Personal Data Management Program.
- Lead the development and implementation of a system that allows managing the risks of

personal data processing.

- Be the link and coordinate with the other areas of the organization to implement the Comprehensive Personal Data Management Program.
- Define and promote a data protection culture within the organization.
- Register the organization's databases in the National Registry of Databases and update the report in accordance with the instructions issued by the SIC on the matter.
- Obtain the declarations of conformity from the SIC when required.
- Review, together with the legal area, the contents of international data transmission contracts signed with non-resident Processors in Colombia.
- Adopt the necessary measures to mitigate any possible damages that may occur as a result of the breach of the data protection regime.
- After notifying the Information Security Officer, notify the SIC in the event of violations of the security codes or risks when managing the data subjects' data.
- Analyze, together with the Head of the Human Resources area, the responsibilities of each position in the organization, to: i) suggest changes in the function manuals; ii) design a specific data protection training program for each of them and iii) define in which cases special confidentiality agreements must be signed.
- Define and carry out general data protection training for all company employees; this training may be face-to-face, virtual or mixed.
- Carry out differential training for employees, new and old, who have access, due to the conditions of their employment, to personal data managed by the organization.
- Integrate the data protection guidelines within the activities of the other areas of the organization, such as: human resources, security, accounting, legal and supplier management, among others.
- Measure attendance at training sessions and assess the performance of each of the participants.
- Monitor the implementation of internal audit plans to verify compliance with its guidelines for the processing of personal information.
- Accompany and assist the organization in addressing the visits and the requirements made by the Superintendency of Industry and Commerce.
- Monitor the Comprehensive Personal Data Management Program.
- Any others stated in the procedure **CUM-PRO-017 Personal Data Protection Management**

**Talent Management Department**

- Support the Personal Data Protection Officer in the training and/or training that must be carried out within GEB.
- Support the Personal Data Protection Officer in the review and adaptation of the functions manuals of the positions that have to administer or manage Personal Data.
- Establish, when considered, as a point to take into account in the performance of employees, their participation and assessment results in training processes on personal data protection.

**Information Security Officer**

- Define the means for maintaining the information under the conditions necessary to prevent adulteration, loss, consultation, unauthorized or fraudulent use or access.
- Maintain an inventory of personal databases held by the organization and classify them according by type.
- Immediately inform the Personal Data Protection Officer of any security incident regarding data protection.
- Establish the measures, processes, security controls required by the organization to comply with the principle of security in terms of personal data protection.
- Perform periodic checks on security systems, document them and execute the necessary steps to, if applicable, modify, expand or correct them.
- Actively support the Personal Data Protection Officer in all activities or procedures required by the Organization in order to comply with data protection.
- Establish protocols to deal with information security incidents. These protocols should foresee the actions to be followed before, during and after each incident.

**Auditor General**

Carry out internal audits to verify compliance with current regulations and internal guidelines regarding the protection of personal data

### Audits, controls and monitoring

The Compliance area will define the controls and monitoring that must be established to ensure compliance with the personal data protection law, that the implementation within the company is being carried out properly, and the processes to adjust the points that can be improved.

For the above, at least the following points must be taken into account:

a) Information collection processes.
b) Activities of use or use of information.
c) Transfer and transmission of information.
d) Management of the data processors.
e) Elimination and/or deletion of information.
f) Addressing complaints and claims.
g) Security processes and measures.
h) Training and qualification.
i) Reinforced compliance when sensitive data or minors are processed.

Likewise, the controls and their frequency will take into account the type of information, type of data processing and area in charge of the processing, among other topics that they consider appropriate.

### Management of risks associated with Personal Data Protection

The GEB will guarantee through a Risk Management System 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 risk to which GEB is exposed in this matter. The Personal Data Protection Officer will guarantee the administration of the Personal Data Protection Risk Management System.

Th GEB has a Personal Data Protection Risk Matrix registered in the format **GIR-PRO-001-F-001 Risk and control matrix**, following the guidelines of the procedure **GIR-PRO-001 Corporate Risk Management**.

The Personal Data Protection Officer will monitor the risks identified in the aforementioned matrix, according to the definitions of the procedure. **CUM-PRO-032 Data Protection Monitoring Mechanisms**

## 3. GUIDELINES FOR THE CIRCULATION OF PERSONAL DATA

### Scope of application

The provisions contained in these guidelines will be applied to all forms of personal data circulation carried out by GEB, since, in its capacity as Data Controller, it must obtain the prior, free, express and informed consent of the data subjects, as established in article 9 of Law 1581 of 2012.

### Transmission of personal data

Decree 1377 of 2013, compiled in Decree 1074 of 2015, defines in Article 3 the transfer as that occurring when the personal data controller and/or processor located in the Republic of Colombia sends the information or personal data to a recipient who, in turn, is the data processor and is either inside or outside Colombia.

GEB, in compliance with its corporate purpose, may transmit the personal data of its data owners to third parties, which will hold the capacity of data processors of the personal data that is the object of the transmission.

In response to the legal obligation to manage those responsible for processing personal information, the Organization has provided the following actions to review, among others, that data processors are using the information for the purposes established by law, in contracts and in the authorizations; as well as whether or not the required security measures or standards are met.

- Request for reports or certifications Data Controllers
- Verification of security standards
- Other activities likely to verify the management of the Managers.

The type of action to follow and the frequency with which it will be carried out will be determined by the Personal Data Protection Officer, taking into account the type of information sent to the processors, the type of processing that has been established, the type of processor company, among others.

GEB carries out Personal Data Transmissions of workers, bidders, contractors, customers and

suppliers to third parties located inside or outside Colombia, in the capacity of Processors, to carry out the Processing of Personal Data on behalf of GEB. Therefore, GEB has implemented the Authorizations and/or Transmission Contracts necessary for this purpose, in accordance with the applicable legal provisions.

The contract signed by GEB with the Processors for the Data under its control and responsibility will indicate the scope of the Processing, the activities that the Processor will carry out on behalf of the Data Controller and the obligations of the Processor towards the Data Subject and the Controller.

Through the signing of contractual clauses for Data Transmission or Personal Data Transmission Contracts, GEB defines the scope of the processing that the person in charge will carry out, the obligations and duties of the processor with regard to the controller or with the data owners of the processing, the purposes of processing, compliance with GEB's Personal Data Processing Policy, safeguarding the security of the databases in which personal data is contained by the processor and the obligation of confidentiality regarding the processing of personal data transmitted, among other aspects of vital importance for the regulation of the transmission of personal data.

These regulated aspects comply with the provisions of Article 25 of Decree 1377 of 2013, compiled in Decree 1074 of 2015, through which the legal parameters for contracts for the Transmission of Personal Data or the contractual clauses for the Transmission are defined.

If the Organization delivers its databases to a Data Processor, it must be stated in this section whether they are individuals or legal persons; what the form of delivery or access to the information is and what type of Processing the Processor may carry out. In addition, the following must be done: (i) determine who will carry out the tasks of monitoring, management and control of the data processors within GEB; and (ii) define whether or not the Company allows third parties to collect information on its behalf, through what documents and what the requirements will be for these third parties.

The controller employee at GEB must guarantee, prior transmission of personal data, that the signing of the Personal Data Transmission Contract has taken place. The omission of this duty will constitute a serious offense in accordance with the provisions of the Internal Work Regulations.

For this purpose, the employee must verify if the standard supply contract agreement (acquisition of goods and services) applies, in which case it will not be necessary to sign an additional document, since said agreement contains the provisions that regulate the relationship between the Processor and the Controller.

In the event that there is no standard supply contract, the signing of the *Transmission Contract*, must be assured. This may be requested from the Personal Data Protection Officer at the following address datospersonales@geb.com.co

### International transmission of personal data

Article 24 of Decree 1377 of 2013, compiled in Decree 1074 of 2015, establishes the applicable rules for international transfers and transmissions of personal data.

Regarding the international transmission of personal data, the aforementioned article indicates that:

*"International transmissions of personal data between a Controller and a Processor to allow the Processor to carry out the processing on behalf of the Controller, will not require notification of the Data Subjects or have their consent when there is a contract in the terms of Article 25 below."*

In compliance with the stated legal mandate, GEB, as mentioned above, has the inclusion of contractual clauses or Personal Data Transmission Contracts, which allow compliance with article 25 of Decree 1377 of 2013, compiled in Decree 1074 of 2015. The foregoing, especially when international transmissions of personal data will be made.

### Transfer of personal data

Decree 1377 of 2013, compiled in Decree 1074 of 2015, defines in Article 3 the transfer as that occurring when the personal data controller and/or processor located in the Republic of Colombia sends the information or personal data to a recipient who, in turn, is the data controller and is either inside or outside Colombia.

Within the framework of strategic alliances, provision of services, or operations between our related companies, GEB may eventually transfer personal data of its data owners to said third parties, who will hold the status of Data Controller of said personal data, from the time of transfer. GEB will only transfer personal data of those data owners who have given their consent for the transfer of their personal data.

### International transfer of personal data

Law 1581 of 2012 establishes in Article 26 the general prohibition of international transfer of personal data:

*"(…)* ***Article 26. Prohibition.*** *The transfer of personal data of any kind 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 Superintendence of Industry and Commerce on the matter, which in no case may be lower than those required by this law for its addressees.*

*This prohibition will not apply in the case of:*

*a) Information for which the Data Subject has granted his express and unequivocal authorization for the transfer.*

*b) Exchange of medical data, when required by the Processing of the Data Subject for reasons of health or public hygiene.*

*c) Bank or stock transfers, in accordance with the applicable legislation.*

*d) Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.*

*e) Necessary transfers for the execution of a contract between the Data Subject and the Data Controller, or for the execution of pre-contractual measures as long as they have the authorization of the Data Subject.*

*f) Transfers legally required to safeguard the public interest, or for the recognition, exercise or defense of a right in a judicial process.*

*PAR. 1—In the cases not set out as an exception in this article, the Superintendency of Industry and Commerce shall issue the declaration of conformity regarding the international transfer of personal data. For this purpose, the Superintendent is empowered to request information and carry out the procedures aimed at establishing compliance with the budgets required for the viability of the operation.*

*PAR. 2—The provisions contained in this article will be applicable to all personal data, including those contemplated in Law 1266 of 2008 (…)"*

In accordance with the provisions of Article 26 of Law 1581 of 2012, there are 3 situations that enable the international transfer of personal data, which are:

**a)** The receiving country offers an adequate level of protection, in accordance with the standards set by the Superintendence of Industry and Commerce, which may not be less than those provided by law.

**b)** The transfer operation is framed within the exceptions established by Article 26.

**c)** The Superintendence of Industry and Commerce issues a declaration of conformity regarding the viability of the international transfer of personal data that is specifically submitted for its consideration.

Through Newsletter 005 of 2017, the Superintendence of Industry and Commerce (hereinafter "SIC") adds the Third Chapter to Title V of the Single Newsletter, specifying important aspects regarding the international transfer of personal data.

In the first place, regarding the measurement standards of the adequate level of protection of a receiving country of personal data transferred from Colombia, the SIC complied with the provisions established by the Constitutional Court in Ruling C-748 of 2011, which considered:

*"(...) It will be understood that a country has the elements or standards of guarantee necessary to guarantee an adequate level of protection of personal data, if its legislation has: principles that cover the obligations and rights of the parties (data subject, public authorities, companies, agencies or other bodies that carry out personal data processing), and data (data quality, technical security) and a data protection procedure that involves mechanisms and authorities that make the protection of information effective. From the foregoing, it follows that the country to which the data is transferred may not provide a level of protection lower than that contemplated in this regulatory body that is the object of study (...)".*

Following the recommendations of the Constitutional Court and based on different legal studies carried out by the SIC, the control entity established the following standards of an adequate level of protection of the country receiving personal information:

*"(…)* ***3.1. Standards of an adequate level of protection of the country receiving the personal information.***

*The analysis to establish whether a country offers an adequate level of protection of personal data in*

*order to carry out an international data transfer will be aimed at determining whether said country guarantees their protection, based on the following standards:*

*a) Existence of rules applicable to the processing of personal data.*

*b) Regulatory establishment of principles applicable to data processing, among others: legality, purpose, freedom, veracity or quality, transparency, access and restricted circulation, security and confidentiality.*

*c) Regulatory establishment of data subjects' rights.*

*d) Regulatory establishment of duties of Data Processors and Data Controllers.*

*e) Existence of judicial and administrative means and channels to guarantee the effective protection of the rights of the data subjects and require compliance with the law.*

*f) Existence of public authority(ies) in charge of supervising the processing of personal data, compliance with the applicable legislation and the protection of the rights of the data subjects, which effectively exercise their functions. (…)"*

Subsequently, the SIC, through Newsletter 002/2018, modifies number 3.2 of Chapter Three of Title V of the Single Newsletter, establishing a list of countries that have an adequate level of protection of personal data, considering:

*"(…)* ***3.2. Countries that have an adequate level of data protection.*** *Taking into account the standards indicated in section 3.1. above and the adequate analysis of protection the following countries: Germany; Australia; Austria; Belgium; Bulgaria; Cyprus; Costa Rica; Croatia; Denmark, Slovakia; Slovenia; Estonia; Spain; United States of America; Finland; France; Greece; Hungary; Ireland; Iceland; Italy; Japan; Latvia; Lithuania; Luxembourg; Malta; Mexico; Norway; Netherlands; Peru; Poland; Portugal; United Kingdom; Czech Republic; Republic of Korea; Romania; Serbia; Sweden and the countries that have been declared with the appropriate level of protection by the European commission. ( …)*

*The Superintendency of Industry and Commerce will exercise, at any time, its regulatory capacity to review the above list and proceed to include those who are not part thereof or to exclude those deemed appropriate, in accordance with the guidelines established by law.*

*PAR. 1st—Notwithstanding that the transfers of personal data are made to countries that have an adequate level of protection, the Data Controllers, by virtue of the principle of demonstrated responsibility, must be able to demonstrate that they have implemented appropriate and effective measures to guarantee the adequate processing of any personal data they transfer to another country and to grant security to the records at the time of making said transfer.*

*PAR. 2nd—When the transfer of personal data is going to be carried out to a country that is not within those listed in this numeral, it will correspond to the data controller that will carry out the transfer to verify if the operation is included within one of the exception causes established in Article 26 of Law 1581 of 2012, or, if that country meets the standards established in number 3.1 above, cases in which the transfer may be made, or, if none of the above conditions are met, request the respective declaration of conformity from the Superintendency.*

*PAR. 3rd—The simple cross-border transit of data does not entail a transfer of data to third countries. Cross-border data transit refers to the simple passage of data through one or several territories using*

*the infrastructure made up of all the networks, equipment and services required to reach its final destination.*

*PAR. 4th—It is possible to transmit personal data to countries that have an adequate level of personal data protection, under the terms that govern the transfer of personal data.*

Taking into account the modification to the list of countries that have an adequate level of data protection incorporated by Newsletter 002/2018, the countries considered safe for the international transfer of personal data are:

| List of countries that have an adequate level of data protection | | | | |
|---|---|---|---|---|
| **Germany** | Australia | Austria | Belgium | Bulgaria |
| **Cyprus** | Costa Rica | Croatia | Denmark | Slovakia |
| **Slovenia** | Estonia | Spain | United States of America | Finland |
| **France** | Greece | Hungary | Ireland | Iceland |
| **Italy** | Japan | Latvia | Lithuania | Luxembourg |
| **Malta** | Mexico | Norway | Netherlands | Peru |
| **Poland** | Portugal | United Kingdom | Czech Republic | Republic of Korea |
| **Romania** | Serbia | Sweden | | |

Taking into account the aforementioned legal framework, GEB will validate prior to any international transfer of personal data:

**a)** If the transfer operation is framed within the exceptions established by Article 26 of Law 1581 of 2012.

**b)** If the receiving country is on the list of countries with adequate levels of personal data protection, and established in Newsletter 002/2018 of the SIC.

**c)** If the receiving country offers an adequate level of protection, it must be validated that it offers an adequate level of protection in accordance with the standards set by the Superintendence of Industry and Commerce, which may not be less than those provided by law.

If as a result of the verification of the requirements mentioned above, the outcome of GEB is that they are not met, it must request the SIC to rule on the international transfer of personal data processed before this entity in the exercise of its legal powers a request to be issued a Declaration of Conformity must be processed with this entity.

The request for Declaration of Conformity must not be made by GEB in the case set out in the first paragraph of numeral 3.3 of Circular 005 of 2017, which provides:

*"(…) **PAR. 1st—** When the data processors that, in order to comply with the principle of demonstrated responsibility, sign a contract with the data controller or implement another legal*

*instrument through which they indicate the conditions that will govern the international transfer of personal data and through which they will guarantee compliance with the principles that govern the processing, as well as the obligations they are responsible for, it will be presumed that the operation is viable and that it has a declaration of conformity.*

*Consequently, data processors may carry out said transfer, after sending notification to the delegation for the protection of personal data of the Superintendence of Industry and Commerce, through which they report on the operation to be carried out and declare that they have signed the transfer contract or other legal instrument that guarantees the protection of the personal data transferred, which may be verified at any time by this superintendence and, in the event that a breach is demonstrated, it may put forward the respective investigation and impose the corresponding sanctions and order the necessary measures (…)".*

Therefore, if GEB signs an International Personal Data Transfer Agreement with the recipient that includes the conditions that will govern the international transfer of personal data and which will guarantee compliance with the principles that govern the processing, as well as the obligations associated therewith, our Organization may benefit from the exception of the aforementioned paragraph, and will only notify the SIC of the operation to be carried out and the declaration of the signing of the International Personal Data Transfer Agreement.

### Processing of personal data transmitted or transferred by third parties

GEB, in compliance with its corporate purpose, may process personal data transmitted or transferred by third parties within the framework of strategic partnerships, service provision contracts and operations between related companies, among others.

Our Organization, as a Data Processor, and in compliance with the provisions of Law 1581 of 2012, will carry out all activities necessary to be certain about the legal legitimacy regarding the collection, use and circulation of personal data. transmitted or transferred by third parties on its behalf.

Given the foregoing, GEB will not process personal data transmitted or transferred to it by third parties without complying with the following assumptions:

**a)** Any Third Party that transfers or transmits personal data to GEB must have express, informed, advanced authorization by the data owner to: (i) Transmit or transfer your personal data to third parties; (ii) Said transfer or Transmission must be authorized so that the third party recipient of the information can process it.

**b)** In the event that personal data is transmitted or transferred by Third Parties so that GEB uses them for advertising, merchandising, marketing or marketing purposes, the Organization will verify that the Third Party is duly authorized by the data owner for such purposes. This review must be carried out by the owner of the alliance/contract/relationship and supported by the Personal Data Protection Officer.

In order to comply with the aforementioned budgets, GEB may use different mechanisms that allow it to effectively verify that the Third Party does, in fact, have express, informed, advanced authorization by the data owner for the processing of personal information. The mechanisms that GEB may use to verify the above include:

**a)** Requests to Third Parties for the authorizations for the processing of personal data granted on their behalf by the data subjects that are the object of the transmission or transfer. GEB will be able to verify that the authorizations provided comply with the aforementioned assumptions.

**b)** Audits of Third Parties in which it is verified that they comply with the Personal Data Protection Regime - Law 1581 of 2012-, especially the requirements for the collection and circulation of personal data.

**c)** Contractual statements or certifications issued by Third Parties expressing their full compliance with the Personal Data Protection Regime - Law 1581 of 2012-, especially the requirements for the collection and circulation of personal data transmitted or transferred to GEB .

In the event in which the owner of data transferred or transmitted to GEB by Third Parties informs GEB of their request to revoke the authorization granted, our Organization will process the request in accordance with our Personal Data Processing Policy and will guarantee the data owner the exercise of their rights.

Additionally, GEB may implement contractual measures in all those contracts, agreements or partnerships signed with Third Parties that support compliance with the Personal Data Protection Regime - Law 1581 of 2012 - during and once the contractual or commercial relationship has ended.

### Compliance with Law 1581 of 2012 by third parties that transmit or transfer personal data

The GEB Personal Data Protection Officer will carry out an analysis of those contracts, agreements or commercial partnerships signed by GEB that entail the transmission or transfer of personal data of the data owners, for which the following will be taken into account: the type of processing carried out, nature of the personal data, volume of personal information and means of transfer or transmission.

In particular, the following will be verified:

- The existence of a Personal Data Protection Policy.
- The existence of service channels set up for the exercise of the rights of access, rectification, cancellation or opposition (ARCO) of the data subjects.
- The existence of guidelines or procedures to guarantee the security of the information.
- The existence of guidelines or procedures to guarantee the management of consultations and claims regarding the protection of personal data.

In the event that, as a result of the verification of the third party's compliance, it is evident that the third party does not meet the minimum standards in personal data protection, the Personal Data Protection Officer will design an action plan with the owner of the contract/partnership/relationship with the purpose of achieving adequate compliance.

## 4. GUIDELINE FOR THE STORAGE OF PERSONAL DATA

### Scope of application

Manage personal information stored in physical and digital repositories with achievable measures that substantially reduce the privacy risks to which the Organization is exposed in the course of its daily work. This will guarantee compliance with the security principle enshrined in Law 1581 of 2012.

### Storage in physical repositories

All employees of the Organization must fully comply with the provisions of the *Document Management Process through the procedures* **GDO-PRO-009 Preparation and updating of document retention tables (TRD)** and the **GDO-PRO-014 Monitoring and control of the application and implementation of document retention tables**. However, in addition to the measures imposed in said program, compliance with the following recommendations must be guaranteed in order to fully comply with Law 1581 of 2012.

**Access to physical filing cabinets.** All filing cabinets or physical information repositories (meaning cabinets, shelves, rolling filing cabinets) must be located in areas whose access is protected with doors equipped with opening systems using a key or other equivalent device. These spaces must remain closed when access by authorized personnel to the documents found inside is not necessary. Archive will be understood as the space (classroom, hall, room, warehouse or equivalent) where the physical file cabinets are located.

**Not open to the public.** The physical filing cabinets or information repositories will be located in spaces or areas of GEB that do not allow access to the public, understood as all personnel other than those who directly handle the information.

**Responsible for the physical files.** The area in charge of the physical repositories will provide for a person to control the entry and exit of the documents deposited in the physical repository.

The person in charge must have an inventory in their custody of the documents that are kept in the file, as well as warn the document administration area of the risks of loss or deterioration thereof.

This task must be controlled by the organization's document management area.

**Management of information outside the file.** When the documents containing personal data are not stored in their respective physical files, the person in charge of them must safeguard them and prevent them from being obtained or consulted by unauthorized persons at all times. In the event that the temporary person in charge of the custody of the information outside the file suffers a mishap from handling them, he will be obliged to make a report of what happened which must indicate the following:

**a)** Date of occurrence of the mishap.

**b)** The documents/folders or texts involved.

**c)** Factual account of what happened, being as concrete as possible.

Any loss of confidential information must be reported to the document administration area, so that the corresponding actions can be taken.

Additionally, the Document Management area must report the incident to the Mailbox datospersonales@geb.com.co, which belongs the Personal Data Protection Officer.

**Transitory information.** Transitory Information (transitory documents) can be kept for the term established by the Document Management Area. Transitory records which are cataloged as supporting documents for the process carried out in the areas are not registered in the document retention tables. Therefore, it is the responsibility of the Document Administrator of the area to manage them; this information is kept by the users without applying the retention table.

### Storage in digital repositories

All employees of the Organization must fully comply with the provisions of the Program *GEB Information Security.* However, in addition to the measures imposed in said program, compliance with the following recommendations must be guaranteed in order to fully comply with Law 1581 of 2012.

**Responsibility of the users.** All users of the information services -software- are responsible for handling their authentication data for the use and access to GEB's computer resources. Users must keep their authentication information secret from systems.

**a)** Users are responsible for all activities carried out with their identifier on the ID network.
**b)** Users must make correct use of the information to which they have access.
**c)** Users must not disclose the access codes or passwords of the entity's computer systems and devices.
**d)** Users may use the data and information contained in the entity's computer resources only for business purposes.

**Access management.** The information security area must limit and control the use of access and privileges to users through formal authorization processes to avoid the inappropriate use of privileges and prevent failures in the operation of information systems.

The information security area must review that the privileges assigned are aligned with the needs of the role and the user's responsibilities.

**Clean screens.**

**a.** Fixed workstations and laptops must have a screen saver standard configured so that it is activated after a certain period of time without use.
**b.** The authentication screen for access to the entity's network should only request the user ID and password.
**c.** When the employee is absent from their workstation, they must lock their workstation in such a way as to protect access to the applications, entity services and files.

### Information Repositories

GEB has the following storage spaces for personal databases:

| Storage | |
|---|---|
| **Storage Form** | **Storage place** |
| **Physical** | Area management archive<br>Central management archive |
| **Digital** | Abox, OneDrive and Corporate SharePoint |

## 5. GUIDELINES FOR THE DELETION OF PERSONAL DATA

### Scope of application

Through this guideline, GEB mitigates the legal, financial and operational risks associated with the custody of personal information, guaranteeing to data subjects, in the applicable events, the performance of activities for the deletion of their personal information from the Organization's databases.

### Requests for deletion of personal data

Requests for information deletion are considered, without being limited thereto, the following:

**a)** Those carried out by the data subjects in the exercise of their rights on the information that rests on them in the physical or digital files of GEB.
**b)** Those requested by the directors of the Organization.
**c)** Those requested by process or area leaders.
**d)** Those that must be carried out to eliminate historical files that have already completed their life cycle in the Organization, in accordance with current legislation regarding physical or digital files and GEB document retention tables.

The deletion of personal information is required by law for personal data for which there is no legitimate purpose to remain stored within the Organization. When documents containing personal data are eliminated, a procedure must be carried out that ensures:

**a)** The method used must prevent the reconstruction and subsequent use of the deleted data.
**b)** The method must be safe and intended to be eco-friendly.
**c)** The method may follow standards established in custom and consider whether information of a physical or electronic nature is to be eliminated. For this purpose, crushing, pulverizing, fusion, incineration, disintegration, overwriting, demagnetization, etc. mechanisms may be used.
**d)** The information to be deleted must have security measures that prevent it from being consulted or copied later. For example, not being available and/or visible in corridors, spaces open to the public, etc.
**e)** An act of destruction must be prepared by means of which a general reference is made to the type of information that is being eliminated, the method used, the date, identification and signature of the attendees.

### Deletion or elimination of negative information

Personal data containing negative information must be deleted or eliminated by GEB within a reasonable time and in proportion to the characteristics and elements of the content of the negative information.

### Validity of the Databases

The GEB Databases will have whatever period of validity that corresponds to the purpose for which their processing was authorized and the special rules that regulate the matter.

### Term of Conservation of Personal Data

GEB may only process personal data for as long as is reasonable and necessary, in accordance with the purposes that justified the processing, taking into account the provisions applicable to the matter in question and the administrative, accounting, tax, legal and historical information aspects.

Once the purposes of the Processing have been fulfilled and without prejudice to the legal obligations that require otherwise, GEB must proceed to the deletion of the Personal Data.

Additionally, the Personal Data must be deleted when required by the Data Subject.

### Deletion requested by the Data Subject

The Data Owner has the right to request the deletion (elimination) of their Personal Data from GEB when:

a) Consider that they are not being processed in accordance with the principles, duties and obligations set forth in Law 1581 of 2012.

b) They are no longer necessary or relevant to the purpose for which they were collected.

c) The period necessary for the fulfillment of the purposes for which they were collected has been exceeded.

This deletion implies the total or partial elimination of the personal information in accordance with the request of the Data Subject in the records, files, databases or processing carried out by GEB.

It is important to keep in mind that the right of deletion is not absolute and that GEB can deny the exercise of it when:

a) The Data Subject has a legal or contractual duty to remain in the Database.

b) The elimination of data hinders judicial or administrative actions related to tax obligations, the investigation and prosecution of crimes or the updating of administrative sanctions.

c) The Personal Data is necessary to protect the legally protected interests of the Data Subject,

to carry out an action based on the public interest, or to comply with an obligation legally acquired by the Data Subject.

When you become aware of this type of request, you must immediately notify the GEB Personal Data Protection Officer, who will carry out the pertinent analysis and determine if the deletion is appropriate.

### Deletion due to the termination of legal validity

When the Data is processed in compliance with a legal obligation, it must be deleted when the term of conservation required by law is fulfilled. The following conservation periods have been provided by law:

### Preservation of merchant documentation

In accordance with the provisions of Article 60 of the Commercial Code, merchants have the obligation to keep their books and papers for a period of 10 years. Once this term has expired, the information may be destroyed.

The Superintendency of Companies has specified that this obligation includes the following documents:

a) Accounting books.

b) Assembly Minutes and Boards of Directors books.

c) Registration of Shareholders and partners.

d) Accounting vouchers.

e) Documents that justify the previous receipts.

f) Any receipts that are issued.

g) Account vouchers.

h) Correspondence related to the business carried out by the company (Article 51 of the Commercial Code and 123 and 124 of Decree 2649/1993).

Note that the obligation provided for in the standard is the conservation of information. The foregoing is relevant because, from the perspective of the Personal Data protection regulations, the only Legally Enabled Processing in accordance with the provisions of Article 60 of the Commercial Code is conservation. In other words, any Processing other than storage, such as the disclosure, circulation and transfer of information, among others, would not have Legal Authorization for more than 10 years.

### Preservation of information required by tax regulations

The supporting information and evidence of the returns filed with the tax authorities must be kept for

the periods provided for in Article 632 of the Tax Statute, in accordance with Article 46 of Law 962 of 2005.

### Preservation of information as obliged by labor regulations

According to the Substantive Labor Code, the employer's obligations are: to give the worker who requests it, at the expiration of the contract, a certification stating the length of service, the nature of the work and the salary earned; and likewise, carry out exit exams and give certification on the matter, if the worker requests it and if upon being hired or during his stay at work he has been subjected to a medical examination.

Additionally, companies required to pay retirement benefits must keep in their files the data that allows them to accurately establish the length of service of their workers and the wages earned. When the files have disappeared or when it is not possible to use them as proof of the time of service or the salary, any other evidence recognized by law is admissible to approve them, which must be produced before the competent labor judge at the written request of the interested party and with the participation of the respective company.

Consequently, GEB must keep the aforementioned information so that it can comply with the obligations of the Substantive Labor Code.

### Deletion ordered by competent authority

Authorities in compliance with a legal function may order the suppression of certain information. The main case in which this can occur is when there is an administrative investigation by the SIC in which the elimination of Personal Data is ordered. In this case, the merits indicated by the authority to carry out the suppression must be evaluated and then to proceed to carry out said elimination, in the event it is considered duly justified.

## DOCUMENTARY CONTROL

| Version No. | Version date | Reason for update |
|---|---|---|
| ***1*** | Feb/05/2021 | In accordance with Law 1581 of 2012 and Decree 1377 of 2013 that develops the Statutory Law, every Data Controller must have an internal personal data protection manual |
| **2** | Sept/23/2021 | Content items are updated and a new form CUM-MAN-004-F-003 Contract for the transmission of personal data V1 is created |

| | | |
|---|---|---|
| **3** | May/17/2022 | Restructuring of form and substance of the Manual, in order to align it with the regulatory requirements established in the Colombian Personal Data Protection Regime. This document replaces the second version. *The name of the manual for the protection of personal data is changed to Manual of Policies and Procedures for the Protection of Personal Data.* |
| **4** | 03/29/2023 | Interactions with procedures CUM-PRO-038 Assessment of the Impact of Personal Data Protection and CUM-PRO-037 Management of Personal Data Protection Incidents are included.<br>Additionally, the following forms are included:<br>CUM-MAN-004-F-004 Authorization for the processing of personal data, use of image and the assignment of rights. |
| | | CUM-MAN-004-F-005 Authorization for the processing of minors' personal data.<br>Finally, the manual removes the form CUM-MAN-004-F-003 Contract for the transmission of personal data. |

| | Name | Role | Area |
|---|---|---|---|
| **Prepared by:** | Maria Claudia Alvarez | Advisor I Personal Data Protection Officer | Response and Detection Management |
| **Reviewed by:** | Luis Rodolfo Hernández | Detection and Response Manager | Corporate Compliance Department |
| **Approved by:** | Luz Elena Diaz | Corporate Compliance Director | Legal and Compliance Vice Presidency |