Personal Data
Processing Policy

GrupoEnergíaBogotá

Title I. Object, Scope of Application, Addressees and Definitions.

Article 1. Object. Grupo Energía Bogotá S.A. ESP (hereinafter the Company or GEB S.A. ESP), in compliance with the constitutional and legal provisions that govern the protection of personal data, does hereby adopt this policy for the purpose of ensuring that owners of said data can review, include, update, rectify or exclude personal data that is subject to processing in the Company's databases or files.

Article 2. Scope of application. The procedures and guidelines established in this policy will apply to the processing of any database or files created, managed and/or guarded by the Company, either as the data controller or processor.

Paragraph. Similarly, this Policy will be applicable to all addressees provided for in the following article.

Article 3. **Addressees.** This Policy is mandatory for:

a) Company representatives and administrators.

b) All dependent workers of the Company.

c) Natural or legal persons linked through any of the contractual modalities established in the Company's Contracting Manual.

d) Data owners, who will be able to consult the process set forth for the exercise of their legal rights.

e) Other regulatory or contractual provisions.

Article 4. Definitions. For the purposes of this policy, the following are defined:

a) **Area:** Unit that integrates the administrative structure of the Company. In that sense, when the Policy imposes an obligation on a department, or said department is contacted, the department's manager or whomever acts on his behalf shall be responsible for compliance.

b) **Authorization:** Express and informed prior consent by the data owner to process the personal data.

c) **Privacy notice:** Verbal or written communication generated by the data controller directed at the data owner to process their personal data, notifying them of the existence of the personal data processing policies that will be applied, how to access them and the purpose of processing said data.

d) **Database:** Organized set of personal data that is subject to processing.

e) **Automated databases:** Those databases stored and managed with the help of IT tools.

f) **Manual databases:** Files with information that is organized and stored physically.

g) **Data transfer:** Processing data with the intent to disclose it to a person other than the data owner or someone who is authorized as transferee.

h) **Personal data:** Any information connected to or that could be associated with one or several certain or ascertainable natural persons, including name, identification number, address, images taken of said persons, fingerprints, political affinity, membership in labor unions, world view, academic training, sexual orientation, etc.

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

j) **Public data:** Data that is not semi-private, private or sensitive. They are considered data. Given its nature, public data may be contained in public records, public documents, official gazettes and bulletins, and duly executed court judgments not subject to reserve.

k) **Semi-private data:** Semi-private data is that which has no intimate, classified or public nature, and whose knowledge or disclosure may interest not only its data owner but a certain sector or group of people or society in general.

l) **Sensitive data:** 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.

m) **The Company:** Grupo Energía Bogotá SA ESP – GEB SA ESP.

n) **Data processor:** Natural or legal person, public or private, that on its own or in association with others, is responsible for processing the personal data at the request of the data controller.

o) **Publicly accessible sources:** Refers to those bases that contain personal data that can be consulted by anyone and may or may not include payment of compensation in exchange for access to said data. Sources accessible to the public include telephone directories and industry or sector directories, as long as the information is limited to personal data that is general in nature or contains general legal information.

Print media, official newspaper and other media will be classified as such.

p) **Habeas data:** The fundamental right that entitles the data owner to petition managers of personal data to access, include, exclude, correct, add, update and certify the data, as well as to limit the possibilities of disclosing, publishing or transferring said data, pursuant to the principles that guide the process of managing personal databases.

q) **Negative information:** That which reflects a condition that unfavorably impacts the data owner's image and good name.

r) **Positive information:** That which reflects a condition that favorably impacts the data owner's image and good name.

s) **Classified information:** Information that is legally excluded from access by the citizenry because its disclosure is likely to cause harm to the rights of natural or legal persons or to the public interest. It is understood that the former occurs when it affects the intimacy, right to life, health or safety of individuals, or when it is related to commercial, industrial or professional secrets. Disclosure of information affects the public interest, so it is confidential in the cases stipulated in Article 19 of Law 1712 of 2014 (when it affects national security and defense; public safety; international relations; prevention, investigation and prosecution of crimes and disciplinary infringements, as long as the arraignment is not enforced or charges are filed, as the case may be; due process and equality between the parties in legal proceedings; effective delivery of justice; children and adolescent's rights; macroeconomic and financial stability of the country; public health; as well as documents that contain opinions or points of view that are part of the deliberative process of public servants).

t) **Regulation:** Refers to the Political Constitution of Colombia, laws, decrees, resolutions, ordinances, agreements, and opinions by the National Authority for Personal Data Protection and jurisprudence.

u) **Personal Data Protection Official:** Person responsible for addressing petitions, inquiries and claims submitted by the data owner in the exercise of its rights to review, update, rectify and delete the data and revoke the authorization. The Personal Data Protection Official will support and guide the implementation of the principle of proven responsibility. The Personal Data Protection Official for the GEB S.A. ESP is Álvaro de Angulo Sanz, and the contact information is datospersonales@geb.com.co.

v) **Data controller:** Natural or legal person, public or private, that by itself or in association with others, decides on the database and/or data processing.

w) **Data owner:** Natural person whose personal data is subject to processing.

x) **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.

y) **Transmission:** Processing personal data that implies communication thereof inside or outside of the Colombian territory when the purpose is for the data processor to do processing at the behest of the controller.

z) **Processing:** Any operation or set of operations on personal data such as collection, storage, use, circulation or deletion.

Title II. Principles

Article 5. Principles. The following principles shall be applied harmoniously and comprehensively in processing personal data, as well as in the development, interpretation and implementation of this policy:

a) **Principle of legality in matters of data processing:** Personal data processing is a regulated activity that must be subject to current legislation.

b) **Principle of comprehensive interpretation of constitutional rights:** The procedures and guidelines set forth in this policy shall be interpreted in a comprehensive manner, in the sense that the constitutional rights are adequately protected. Said rights include habeas data, the right to a good name, the right to honor, the right to intimacy and the right to information. The data owner' rights shall be interpreted in harmony and in a plane of equilibrium with the right to information stipulated in Article 20 of the Constitution and other applicable constitutional rights;

c) **Principle of finality:** Personal data processing shall obey legitimate purposes pursuant to the Constitution and the law, which shall be made known to the data owner.

d) **Principle of freedom:** The processing may only be exercised with the prior, express and informed consent of the data owner. Personal data may not be obtained or disseminated without prior authorization, or in the absence of a legal or judicial mandate which discloses the consent.

e) **Principle of veracity or quality:** The data subject to processing must be true, complete, exact, up to date, verifiable and understandable. Processing data that is partial, incomplete, fragmented or can lead to error is prohibited.

f) **Principle of transparency:** The data owner is guaranteed to obtain from the data Processor or Controller, at any time and without restrictions, information about the existence of relevant data. .

g) **Principle of restricted access and circulation:** Processing is subject to the limits that derive from the nature of the personal data, provisions pertaining to habeas data

and the Constitution. In that regard, the process may only be carried out by persons authorized by the data owner and/or persons stipulated in current legislation. Personal data, except for public information, 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 the data owners or third parties authorized according to law.

h) **Principle of security:** Information subject to processing by the Company shall be handled with the technical, human and administrative measures necessary to convey security to the records, avoiding corruption, loss, query, unauthorized or fraudulent use or access.

i) **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.

j) **Principle of timeliness of the information:** The data owner's data shall not be furnished to other users or third parties when it ceases to be useful for the purpose of the database**.**

Title III. Rights and Legal Terms for Processing Data.

Article 6. Data owner's rights. The personal data owner is entitled to the following rights:

a) Know, update and rectify their personal data. This right may be exercised over data that are partial, inaccurate, incomplete, fragmented, or leading to error, among others, or data expressly forbidden or not authorized to be processed.

b) Request proof of authorization granted, except when expressly exempted as a requirement for processing in accordance with law.

c) Be informed, upon request, of the use given to the personal data.

d) Appear before the Superintendence of Industry and Commerce to file claims for infringements to the provisions of this policy and the regulations that govern the matter, to that end complying with the requirement of procedure consisting of having exhausted the process of consultations or claims with the Company.

e) Revoke the authorization and/or request deletion of the data when the process fails to respect constitutional and legal principles, rights and guarantees. The revocation and/or deletion will proceed when the Superintendence of Industry and Commerce has determined that the process incurred in conducts contrary to the law and the Constitution. Notwithstanding the foregoing, the requests to delete the information and revoke the authorization shall not proceed when the Data owner has a legal or contractual duty to remain in the database.

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

Article 7. Data owner's authorization. The Company will request authorization from the data owner no later than at the time of data collection to process and report the personal data gathered, as well as the specific objectives of the process for which it obtained consent.

To that end, all Company employees, particularly department heads (vice presidents, directors, managers) responsible for each process that requires processing personal data, have the obligation of ensuring that, prior to processing the data, they obtain authorization from the data owner. Said authorization must be freely and expressly given in writing, following the parameters set forth by Colombia regulations and this Policy.

The data owner's authorization may be issued via technical means that facilitate the data owner's statement. It shall be understood that the authorization complies with these requirements when it is stated: (i) in writing, (ii) verbally or (iii) through unequivocal conducts that lead to the reasonable conclusion that the authorization was granted, guaranteeing in every case that it may be subject to further consultation. In no case shall silence be understood as an unequivocal conduct.

Paragraph I. Each department will keep supporting documentation of the authorization to process personal data.

Article 8. Content of the authorization. Any authorization to process personal data in which the Company is acting as the controller or processor must contain no less than the following:

a) The process to which the personal data shall be submitted, its purpose, and how long the information will be stored.
b) The optional nature of the authorization as it relates to sensitive data or minors
c) The rights of the data owner.
d) The Company's identification, physical or electronic address and telephone number

Article 9. Cases in which authorization is not necessary. Data owner's authorization is not necessary when it deals with:

a) Information requested by a public or administrative entity in the exercise of its legal duties or by court order
b) Information of 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 people's civil registry

Article 10. Authorization to process sensitive data. Authorization to process sensitive data shall be obtained expressly, ensuring that in addition to the requirements of the previous article, it also contains the following:

a) Notification to the data owner that because these are sensitive data, the data owner is not obligated to authorize the process.
b) Notification to the data owner that the data subject to processing are sensitive, and the purpose of the process.

Paragraph: No activity may be conditioned on the data owner providing sensitive personal data.

Article 11. Privacy notice. In the event that it is not possible to make available to the Data owner the policies regarding data processing, the data controller, through the privacy notice, will furnish the Data owner information pertaining to the existence of the personal data processing policy, how to access it, its purpose, the Company's contact information, and any channels provided by the Company for data owners to exercise their rights as per this policy. Similarly, it shall contain the rights of the data owner, the mechanisms provided by the data controller for the data subject to review the data processing policy and any substantial changes that may result in it or in the corresponding privacy notice, how to access or consult the data processing policy.

When sensitive personal data are collected, the privacy notice shall expressly indicate the optional nature of the response to the answers related to this type of data.

In any case, disclosure of the Privacy Notice shall not exempt the data controller from the obligation of making data owners aware of the data processing policy.

The privacy notice is available for permanent consultation on the Company's website: https://www.grupoenergiadebogota.com/eeb/index.php/datos-personales

Paragraph: The Company reserves the right to amend the privacy notice. Accordingly, changes will be notified in a timely manner on the web page https://www.grupoenergiadebogota.com/eeb/index.php/datos-personales

Article 12. Personal data processing. GEB S.A. ESP will carry out a process to collect, store, use, circulate, record, manage, report, process, employ, assess, analyze, confirm, update and delete data under standards of confidentiality, security, transparency, accuracy, timeliness, restricted access and circulation, pursuant to regulatory provisions and in the framework of its corporate purpose for administrative, operating, statistical and commercial ends, and for all that is considered pertinent in the development of the functions, activities and operations understood therein.

Article 13. Purpose. Company employees will only process personal data to comply with a legitimate purpose related to the responsibilities of their position. Consequently, personal data collection shall be limited to that which is pertinent, adequate, necessary and useful for the purpose or purposes for which it is collected or required in accordance with the privacy notice.

Title IV. Duties and Obligations

Article 14. Duties of the company as data controller. The Company, as data controller or processor, will comply with the following duties, without prejudice to the other provisions provided by law:

a) Guarantee the data owner, at all times, the full and effective exercise of the right of habeas data.

b) Request and keep a copy of the respective authorization granted by the data owner.

c) Duly notify the data owner of the purpose of the data collection and the rights the data owner is entitled to in virtue of the authorization granted.

d) At the request of the data owner, report on the use that was or will be given to the data.

e) Maintain the information under the conditions necessary to prevent corruption, loss, consultation, unauthorized or fraudulent use or access.

f) Process any consultations and claims formulated in the terms indicated herein and complete any update, correction or deletion of the data in a timely manner.

g) Notify the Superintendence of Industry and Commerce in the event of violations of the security codes or risks when managing the data owners' data.

h) Comply with any instructions and requirements made by the Superintendence of Industry and Commerce.

i) Record the caption "claim in process" in the database when it is formulated by the data owner, or "information under legal discussion" once it has been notified by a competent authority of legal proceedings related to the quality of the personal data.

j) Abstain from circulating information that is being challenged by the data owner and has been ordered blocked by the Superintendence of Industry and Commerce.

k) Allow access to the information only to persons legitimately allowed to do so.

l) Guarantee that the information provided to the data processor is true, complete, exact, up to date, verifiable and understandable.

m) Update the information, notifying the data processor, in a timely manner, of any developments regarding the data that have been already provided and adopt other measures necessary to maintain the information up to date.

n) Rectify the information when it is incorrect and notify the data processor as needed.

o) Provide the data processor, as the case may be, only data that has been authorized for processing pursuant to legal provisions.

p) Require that the data processor abide by the conditions of security and privacy of the data owner's information at all times.

q) Adopt an internal manual of policies and procedures to guarantee adequate compliance of this law and especially, to handle consultations and claims.

r) Notify the data processor when certain information is under discussion by the data owner once the claim has been filed and the respective process has not been finalized.

Article 15. Duties of the Company with regard to data processors. In cases when the Company, as the data controller, provides personal information, it will do so according to the following duties:

a) Provide, as the case may be, only data that has already been authorized for processing.

b) Guarantee that the information provided is true, complete, exact, up to date, verifiable and understandable.

c) Require respect for the conditions of security and privacy of the data owner's information at all times.

d) Require compliance of the provisions stipulated by law and in this policy.

e) Notify when certain information is under discussion by the data owner once the claim has been filed and the respective process has not been finalized.

Article 16. Duties of data processors. Data processors shall comply with the following duties, notwithstanding any other regulatory provisions that govern their activity:

a) Guarantee the data owner, at all times, the full and effective exercise of the right of habeas data.

b) Maintain the information under the conditions necessary to prevent corruption, loss, consultation, unauthorized or fraudulent use or access.

c) Make timely data updates, corrections or deletions under the terms of regulations pertaining to the matter.

d) Update the information reported by the data controllers no later than five (5) business days from receipt.

e) Process consultations and claims formulated by the data owners under the terms indicated in applicable regulations and herein.

f) Adopt an internal manual of policies and procedures to guarantee adequate compliance of this law and especially, to handle consultations and claims made by data owners.

g) Record the caption “claim in process” in the database as set forth in the regulations.

h) Insert the caption “information under legal discussion” in the database when it has been notified by a competent authority of legal proceedings related to the quality of the personal data.

i) Abstain from circulating information that is being challenged by the data owner and has been ordered blocked by the Superintendence of Industry and Commerce.

j) Allow access to the information only to persons that are allowed access to it.

k) Notify the Superintendence of Industry and Commerce in the event of violations of the security codes or risks when managing the data owners’ data.

l) Comply with any instructions and requirements made by the Superintendence of Industry and Commerce.

Paragraph I. When the Company is the data controller and processor, it will comply with all the duties set forth to that end.

Article 17. Obligations of Company areas. In order to give strict compliance to this personal data protection policy, each department in the Company shall:

1. Complete an inventory of the databases or files it manages up to that point, indicating the subject, purpose and time of existence, and report it to the Personal Data Protection Official in the term established thereby.

2. As of that date, if there is a need to create a database or file that contains personal information, the Company will establish the subject, purpose and time of existence of said file and report it to the Personal Data Protection Official so it can issue a decision about its implementation and use in a period of ten (10) business days from the date of said request. A negative decision by the Personal Data Protection Official means the creation of the database or file requested is forbidden. However, if the department can correct the issues indicated by the Personal Data Protection Official in its decision, and if pertinent, it may petition the official to reconsider its decision in order to approve the process.

3. Prepare a detailed inventory of third parties acting as data processors to date, explaining the activities conducted and analyzing the terms of data processing, which will be submitted to the Personal Data Protection Official with a contract or order to study the contractual stipulations that govern the legal bond with the Company under the terms of this policy, as well as the criteria and methodology the Company will use to make sure the personal data protection regulations are complied with by the third parties involved.

The Personal Data Protection Official will report the outcome of the study within the next fifteen business days.

4. If the personal data processing will be handled by a third party, notify the Personal Data Protection Official of the activities that will be undertaken, the conditions under which the process will take place, the methodology used to that end, and the personal data protection manuals and policies obtained in market surveys, so that Management can determine if there is an adequate level of personal data protection and approve the request.

5. Every time a modification is required of the subject, purpose, type of data and time of existence of a database or file, reasonable justification must be provided in writing or via email addressed to the Personal Data Protection Official for the approval and rejection of the corresponding implementation, within ten business days after the communication is received. A negative decision by the Personal Data Protection Official means the modification to the database or file is forbidden. However, if the department corrects the issues indicated by the Personal Data Protection Official in its decision, and if pertinent, it may request the Official to reconsider its decision in order to approve the modification.

6. Define the employee or employees who will work exclusively to process the personal data and notify the Personal Data Protection Official to formulate the content of the obligations to be included in the job description within ten business days from date of receipt. In turn, the Personal Data Protection Official will submit to the requesting department the content of the obligations so that it can provide Human Resources management the updated job description and responsibilities.

7. Guarantee that no databases or files containing only negative or adverse information will be implemented.

8. Notify the data owner of the privacy notice's content prior to making the authorization to guarantee that it knows all the purposes of the information.

9. To timely and unofficially review the privacy notice prepared by the Personal Data Protection Official and recommend any inclusions or adjustments deemed pertinent.

10. Send the Personal Data Protection Official the forms containing the personal data that exist to date and are part of the Integrated Management System, indicating their purpose and that of the information to be collected, so that within ten business days from receipt, Management can determine whether or not it is necessary to include authorization to process the data.

11. From that date, every time it needs to create forms that collect personal data, it must send the Personal Data Protection Official the project of said form, indicating their purpose and that of the information to be collected, so that within ten business days from receipt, Management can determine whether or not it is necessary to include authorization to process the data.

12. Adopt all measures that prevent unauthorized access by third parties in order to protect the information, avoiding its manipulation, alteration or deletion, and taking into consideration that the personal data compiled in databases or files is of restricted circulation, therefore and as a general rule, it will only be disclosed to third parties authorized by the data owner in accordance with the authorized purposes, or to those entitled to request said information.

13. Assist in the implementation and consolidation of the personal data processing policy and the principle of proven responsibility managed by the Personal Data Protection Official.

Article 18. Obligations of bidders and contractors. All Company bidders and contractors shall guarantee an adequate level of personal data protection at every stage of the process they conduct.

Similarly, they shall guarantee that any personal information for which they are responsible and that have to be submitted to the Company as a result of the bid or contract is subject to proper processing in accordance with the personal data protection regulation, and has prior agreed authorization, which may be subject to further consultation.

Title V
Procedure to Receive and Resolve Consultations and Claims.

Article 19. Legitimacy to exercise the data owner's rights. The rights of the data owner may be exercised by the following persons:

1. By the data owner, who must sufficiently verify their identity through the various means made available by the data controller.
2. By its assigns, who must verify said condition.
3. By the data owner's representative and/or proxy, upon accreditation of the representation or power of attorney.
4. By stipulation in favor of another or for another.
5. The rights of children and adolescents shall be exercised by the persons authorized to represent them.

Paragraph I The data owner, their assigns or representatives must attach a copy of their identification document and others deemed necessary to substantiate the request for consultation or claim.

Paragraph II. If the consultation or claim is in reference to a deceased data owner, the spouse, permanent partner and/or assigns, must submit the request, attaching a true copy of the civil registry of

death of the data owner and a true copy of the civil registry that proves the relationship (marriage, birth, etc.) or an out of court statement in cases of de facto marital union.

Article 20. Consultations. The consultation shall be formulated through channels enabled by the data processor or data controller, as long as it can keep a copy thereof. The representative will make the consultations in writing or by email in which it: i) establishes its identity (full name and personal identification number);
ii) ii) clearly, specifically and factually specifies the purpose of the consultation; iii) establishes and accredits the legitimate interest that drives their actions, always attaching supporting documentation, such as a power of attorney acknowledging the content and signature before a public notary and, iv) reports the physical and/or electronic address to receive communications.

The main topics of consultation are:

a) Request for information on access to personal data.
b) Request for proof of authorization
c) Consultation of the use given to the information.

Paragraph: The information requested may be furnished by any means, including electronic, as required by the data owner, so that it can be read easily without technical barriers that prevent its access and correspond totally to that which resides in the database.

Article 21. Claims. i). The claim is formulated through a request addressed to the data controller or processor, with the data owner's identification, description of the events that resulted in the claim, the address and supporting documentation as needed. The data owner, their assigns or any other person with a legitimate interest may file a claim in writing or by email with the responsible department, in which it: i) establishes their identity (full name and personal identification number); ii) in detail, clearly, specifically and factually specifies the purpose of the consultation; iii) states and accredits the legitimate interest that drives their actions, always attaching supporting documentation, such as a power of attorney acknowledging the content and signature before a public notary and, iv) the physical and/or electronic address to receive communications.

The main topics of claim are:

a) Corrections or updates of the data owner's personal data.
b) Partial or total revocation of the authorization to process.
c) Deletion of personal data.

Article 22. 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 in the previous article, contain the specification of the corrections to be made and supporting documentation for the request.

Article 23. Partial or total revocation of the authorization to process Data owners have the right to revoke the authorization when the constitutional and legal principles, rights and guarantees are not respected in the process, which shall prevail in cases in which

the Company makes a determination after the claim is filed, or the personal data protection authorities so deem.

Nevertheless, if the Company decides that the revocation is not appropriate, it will report it by means of a substantiated communication as per the terms set forth in section vii of article 28 herein.

Once the authorization has been revoked, the Company can proceed to delete information contained in the respective databases.

Article 24. Deletion of personal data. Personal data owners have the right to delete them when the process fails to respect constitutional and legal principles, rights and guarantees.

In addition to the requirements established in article 21 herein, the claim consisting of the request to delete personal data must contain identification of the data to be deleted, and proceed as deemed by the Company or in cases in which the personal data protection authority so orders.

Article 25. Inadmissibility of the request for deletion of the data or revocation of the authorization. The requests to delete the information and revoke the authorization shall not proceed when the data owner has a legal or contractual duty to remain in the database.

Article 26. Data of the data controller and Personal Data Protection Officer. The data controller is Grupo Energía Bogotá S.A. ESP – GEB S.A. ESP, with TIN 899.999.082-3, located at Carrera 9 No. 73 – 44 Piso 6 of Bogotá D.C., telephone number +57 (1) 326-8000.

The Personal Data Protection Official with the powers necessary to receive, address and resolve consultations and claims made by personal data owners or persons authorized to do so is Álvaro de Angulo Sanz, Director of Corporate Affairs of TGI S.A. ESP, a subsidiary of Grupo Energía Bogotá, email **datapersonales@geb.com.co.**

Article 27. Procedure to address consultations. A consultation will be processed as follows:

i. Documentation Management will submit (in physical or electronic format) the consultation to the Personal Data Protection Official, who will address the consultation.

ii. In the next two business days, the Personal Data Protection Official will ensure that the consultation was submitted by the data owner or its representative in compliance with the requirements established in article 20 herein.

iii. If the consultation does not meet all the requirements established in article 20 of this policy, it will not be processed, and the sender will be notified of the reasons.

iv. If the consultation meets all the requirements of article 20 of this policy, its subject will be analyzed in order to determine if it requires information and/or support from another Company department. If so, the Personal Data Protection Official will forward the consultation via email to the head of the respective department so that in two (2) business days from receipt it can decide, and as appropriate, provide the documentation needed to address the consultation.

v. 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 for the delay and indicating the date in which the consultation will be resolved, which under no circumstances may exceed five (5) business days following expiration of the first term.

Article 28. Procedure to address claims. When a claim is filed the following procedure will be adhered to:

i. Document Management shall provide a physical and/or electronic copy of the claim to the Personal Data Protection Official, who will immediately assign it to the professional in charge of the personal data protection policy.

ii. In the next two business days, the Personal Data Protection Official will ensure that the claim was submitted by the data owner or its representative in compliance with the requirements established in article 21 herein.

iii. If the claim is incomplete, the interested party will be asked to make the necessary corrections no later than five (5) days after receipt thereof. Two (2) months after the date of requirement, if the petitioner has not presented the information required, the claim will be considered relinquished.

iv. If the Company is not competent to resolve the claim, it will be transferred to whom it corresponds in a period of no more than five (5) business days and notify the interested party of the situation.

v. Once the completed claim is received, a caption will be included in the database stating “claim in process” and the reason for it, in a period of no more than five (5) business days. Said caption shall be kept until the claim is resolved.

vi. The object of the claim will be analyzed to determine if it requires further information and/or assistance from another Company department. If so, the Personal Data Protection Official will forward the claim via email to the head of the respective department so that in two business days from receipt it can decide, and as appropriate, provide the documentation needed to address the claim.

vii. The maximum period to address the claim will be fifteen (15) business days from the date of receipt. When it is not possible to address it within said term, the interested party will be informed of the reasons for the delay and the date on which their claim will be resolved,

which in no case may exceed eight (8) business days following the expiration of the first term.

Title VI. Final Provisions

Article 29. Legal guidance. The Personal Data Protection Official will provide guidance to any departments or employees that request it.

Article 30. Verification of compliance. The Internal Audit Department will verify strict compliance with this Policy in all audits performed and report the results to the Personal Data Protection Official.

Article 31. Orientation and retraining. Human Resources Management or the department acting as such shall include as a point of the program for each new hire orientation and retraining the topic of personal data protection. To that end, it will ask the Personal Data Protection Official to make the corresponding presentation.

Article 32. Confirmation of references. Only Human Resources Management or the department acting as such is authorized to confirm job references. For that purpose, the data owner shall communicate in writing or via email with said department, notifying the entity that is going to contact them to confirm the references, and authorize the department to proceed in that regard.

In the case of contractors, it will be the auditor or supervisor who confirms the references. For that purpose, the data owner shall communicate in writing or via email with them, notifying the entity that is going to contact them to confirm the references, and authorize the department to proceed in that regard.

Paragraph. Confirmation of references shall be made on positive information, and never on negative data or information that is adverse for the data owner.

Article 33. Timeliness of processing. Processing personal data by GEB S.A. ESP is carried out during the period of pertinence of the data, and in every case, until compliance with the purpose or purposes for which it was authorized, or when appropriate by legal or contractual provision.

Negative or adverse information will remain for a period of five years, unless a law provides for a shorter term. Once the maximum permanence period expires, the negative data will be eliminated from the respective database or file, guaranteeing the right to privacy by default.

Article 34. Integration. The privacy notice is an integral part of this policy.

Article 35. Principle of proven responsibility. The Company shall implement the principle of proven responsibility, for which it will aim to have a high organizational culture in matters of personal data protection, as well as the commitment from senior management to it, in accordance with the guides implemented by the Superintendence of Industry and Commerce.

Article 36. Validity. This personal data processing policy is in effect as of the date it was issued.

It was approved on August 12, 2016, and taking into consideration the change of corporate name, it was adjusted on December 18, 2017.