Personal Data Processing Policy

TRANSPORTADORA DE GAS INTERNACIONAL S.A. ESP

Carrera 9 # 73-44
(57) 3138400
tgi.com.co

Heading I. Purpose, scope of application, recipients and definitions.

Article 1. Purpose. Transportadora de Gas Internacional S.A. ESP - TGI S.A. ESP (hereinafter the Company or TGI) in compliance with the constitutional and legal provisions that govern the protection of personal data, adopts this policy with the purpose of guaranteeing that the holders can know, include, update, rectify and exclude your personal information subject to processing in databases or files of the Company.

Article 2. Scope of application. The procedures and guidelines established in this policy will be applied to the processing of any database or files created, administered and / or under the custody of the Company, either as processing controller or processor.

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

Article 3. Recipients. This Policy is mandatory for:

a) Company representatives and administrators

b) All employees dependent on the Company.

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

d) The Information Holders who may refer to the procedure established to exercise their legal rights.

e) The others provided for in the regulations or any contractual provision.

Paragraph: The breach of the obligations by Company employees, as described in this Policy, will lead to disciplinary sanctions, in accordance with the Internal Work Regulations.

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

a). Area: Unit that integrates the administrative structure of the Company. In this sense, when an obligation is imposed on an area or it is requested to contact it under this Policy, its compliance will be the responsibility of the Head of each area, or whoever acts as such.

b). Authorization: Prior, express and informed consent of the Holder to process personal data.

c). Notice of Privacy: Verbal or written communication generated by the person controller, addressed to the holder for the processing of their personal data, whereby they are informed about the existence of the information processing policies that will be applicable, how to access them and the purposes of the processing to which personal data will be subjected.

d). **Database:** Organized set of personal data, subjected to processing.

e). **Automated Databases:** Those that are stored and managed with the support of computer and / or technological tools.

f). **Manual Databases:** These are the files whose information is physically organized and stored in a physical way.

g). **Transfer of Data.** Data processing that involves its disclosure to a person other than the owner of the data or other than the person who was authorized as assignee.

h). **Personal Data:** Any information linked to, or which may be associated with one or more specific or determinable natural persons, such as name, identification number, address, images captured of people, fingerprint, political affinity, membership in organizations union, worldview, academic training, sexual condition, among others.

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

j). **Public Data:** Data that is not semi-private, private or sensitive. They are considered data. Given their nature, public data may be contained, among others, in public records, public documents, gazettes and official bulletins, judicial rulings duly executed, not subjected to confidentiality.

k). **Semi-private Data:** Semi-private means data that is not intimate, reserved, or public in nature and whose knowledge or disclosure may be of interest not only to its holder, but to a certain sector or group of people or society in general.

l). **Sensitive Data:** This is the data that affects the intimacy of the holder or which undue use may give rise to their discrimination, such as those that disclose their race or ethnic background, political preference, religious or philosophical convictions, affiliation to unions, social, human rights organizations, or entities that guarantee the rights and guarantees of opposition political parties, as well as the data pertaining to health, sexual life and biometric data.

m). **The Company:** La Transportadora de Gas Internacional S.A. ESP – TGI S.A. ESP.

n). **Processor:** Natural or legal person, whether public or private, which by itself or together with others, processes personal data on behalf of the controller.

ñ). **Publicly Accessible Sources:** It refers to those databases containing personal data whose consultation can be made by anyone, which may or may not include the payment of a consideration in exchange for the access service to such data. Telephone directories, industry or sector directories, among others, are considered sources accessible to the public, as long as the information is limited to personal data of a general nature or that contains generalities of the law. The printed media, the official gazette and other media are considered accessible sources.

o). **Habeas Data:** The fundamental right that grants the power to the holder of personal data, to request to personal data administrators' access, inclusion, exclusion, correction, addition, updating and certification of the data, as well as the limitation in the possibilities of disclosure, publication or transfer thereof, in accordance with the principles pertaining to the personal database administration process.

p). **Negative Information:** It is one that reflects a condition that favorably impacts the image and good name of the holder.

q). **Positive Information:** It is one that reflects a condition that favorably impacts the image and good name of the holder.

r). **Confidential Information:** Information that is legally exempted from access to citizens because its disclosure is likely to cause damage to the rights of natural or legal persons or to public interests. It is understood that the former occurs when it affects privacy, the right to life, health or safety of natural persons or when it deals with commercial, industrial and professional secrets. The disclosure of information affects public interests and, therefore, is confidential in the cases provided for in article 19 of Law 1712 of 2014 (when it affects national defense and security; public security; international relations; prevention, investigation and prosecution of crimes and disciplinary offenses, as long as the security measure is not made effective or the statement of charges is formulated, as the case may be; due process and equality of the parties in judicial processes; effective administration of justice; rights of children and adolescents; the macroeconomic and financial stability of the country; public health; as well as the documents that contain the opinions or points of view that are part of the deliberative process of public servants).

s). **Regulation**: It refers to the Political Constitution of Colombia, laws, decrees, resolutions, ordinances, agreements, concepts of the National Authority for the Protection of Personal Data and case law.

t). **Personal Data Protection Official:** Person responsible for the attention of requests, queries and claims, for which the data holder can exercise its rights to know, update, rectify and delete the data and revoke the authorization. The Personal Data Protection Officer will support and guide the process of implementing the principle of proven responsibility. The Personal Data Protection Officer for TGI is Álvaro de Angulo Sanz and the contact channel is **datospersonales@geb.com.co.**

u). **Controller:** Natural or legal person, whether public or private, which by itself or together with others, decides on the database and/or data processing.

v). Holder: Natural person whose personal data are subjected to processing.

w). Transfer: The transfer of data takes place when the controller and / or processor of personal data, located in the Republic of Colombia, sends the information or personal data to a recipient, who in turn, is responsible for the processing and is located within the country or abroad.

x). Transmission: Processing of personal data that implies the communication thereof within or outside the territory of the Republic of Colombia, when the aim is for the processor to undertake the processing on behalf of the controller.

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

Heading II.
Principles

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

a). Principle of legality regarding data processing: The processing of personal data is a regulated activity that must be subject to the provisions of current regulations.

b). Principle of comprehensive interpretation of constitutional rights: The procedures and guidelines established in this policy will be comprehensively interpreted in the sense that constitutional rights are adequately protected, such as habeas data, the right to a good name, the right to honor, the right to privacy and right to information. The rights of the holders will be interpreted in harmony and maintaining balance with the right to information provided for in article 20 of the Constitution and with the other applicable constitutional rights.

c). Principle of Purpose: The processing of personal data will follow legitimate purposes in accordance with the Constitution and the law, which will be informed to the holder.

d). Principle of Freedom: The processing can only be exercised with the prior, express and informed consent of the holder. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that relieves consent.

e). Principle of Truthfulness or Quality: The information subject to processing must be truthful, complete, accurate, up-to-date, verifiable and understandable. The processing of partial, incomplete, fractioned or misleading data is prohibited.

f). Principle of Transparency: The Holder will be entitled to obtain from the Processing Controller or Processor, at any time and without restrictions, information about the existence of data that concerns him/her.

g). **Principle of Access and Restricted Circulation:** The processing is subject to the limits that derive from the nature of the personal data, the provisions on habeas data and the Constitution. In this sense, the processing can only be done by people authorized by the holder and / or by the people provided for in current regulations. Personal data, except for public information, may not be available on the Internet or other means of dissemination or mass communication, unless access is technically controllable to provide restricted knowledge only to the holders or authorized third parties in accordance with the law.

h). **Principle of Security:** The information subject to processing by the Company must be handled with the technical, human and administrative measures needed to grant security to the records avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access.

i). **Principle of Confidentiality:** All persons who intervene in the processing of personal data that are not public are obliged to guarantee the confidentiality of the information, even after the end of their relationship with any of the tasks comprised in the processing, being able to only supply or communicate personal data when this entails the development of the activities authorized in the regulations that addresses the right to habeas Data.

j). **Principle of Temporality of the Information:** The owner's information will not be provided to users or third parties when it ceases to serve the purpose of the data bank.

Heading III. Rights and legal conditions for data processing.

Article 6. Rights of the Holders. The holder of the personal data will have the following rights:

a) Know, update and rectify personal data. This right may be enforced, among others, with respect to partial, inaccurate, incomplete, split data inducing to error, or those whose treatment is expressly prohibited, or was not authorized.

b) Request evidence of the authorization granted, unless it is expressly exempted as requisite for processing, in accordance with the law.

c) Being informed, with prior request, with respect to the use given to personal data.

d) File with the Superintendency of Industry and Trade complaints for infractions to the provisions of this policy and the rules governing the matter, complying for this purpose with the procedural requirement consisting of having exhausted the consultation or claim process with the Company.

e) Revoke the authorization and / or request the deletion of the data when, in the processing, the constitutional and legal principles, rights and guarantees are not respected. The repeal and/or deletion will proceed when the Superintendence of Industry and Trade had determined that in the processing, conducts contrary to the law and the Constitution have been committed.

Notwithstanding the foregoing, the request to delete the information and the repeal of the authorization will not proceed when the Holder has a legal or contractual duty to remain in the database.

f) Freely access his personal data, subjected to treatment.

Article 7. Holder's Authorization. The Company will request, at the latest at the time of data collection, the holder authorization for the processing thereof and will inform the personal data that will be collected, as well as the specific purposes of the processing for which consent is obtained.

For this purpose, all the Company's workers, especially the Heads of the area (Vice Presidents, Directors and Managers) who are responsible for each process in which the processing of personal data is required, have the obligation to guarantee that prior to the processing thereof, the authorization of the owner is obtained in a free, express and informed manner, following the parameters established by Colombian regulations and this Policy.

For the authorization of the holder, technical means may be used to facilitate the declaration of the holder. It will be understood that the authorization complies with these requirements when it is expressed: (i) in writing, (ii) orally or (iii) through unequivocal conduct that allows to reasonably conclude that the authorization was granted, guaranteeing in any case that this is susceptible to subsequent consultation. In no case may silence be comparable to unequivocal conduct.

Paragraph I. Each area will keep support of the authorization for the processing of personal data.

Article 8. Authorization Content. Any authorization for the processing of personal data where the Company acts as processing controller or processor must contain at least the following:

a) The processing to which the personal data will be subjected, its purpose, the information storage period
b) The optional nature of the authorization related to sensitive data and minors.
c) The rights of the holder.
d) The identification, physical or electronic address and telephone number of the Company.

Article 9. Cases in which authorization is not necessary. The authorization of the holder will not be necessary in the event of:

a). Information required by a public or administrative entity in furtherance of its legal functions or by court order.
b). Data of a public nature.
c). Cases of medical or health emergency.

d). Processing of information authorized by law for historical, statistical or scientific purposes.
e). Data related to the civil status of people.

Article 10. Authorization for the processing of sensitive data. The authorization for the processing of sensitive data must be obtained expressly so that it contains, in addition to the requirements of the previous articles, the following:

a) Inform the holder that since this is sensitive data, the holder is not obliged to authorize the processing thereof.
b) Inform the holder which of the data that will be processed is sensitive and the purpose thereof.

Paragraph: No activity may be conditioned on the holder's provision of sensitive personal data.

Article 11. Notice of Privacy. In cases where it is not possible to make the information treatment policies available to the Holder, the Controller, through the privacy notice, will inform the Holder of the information regarding the existence of the personal data processing policy, the way to access it, the purpose thereof, the Company's contact details, the channels provided by it so that the holders of the information can exercise the rights provided for in this policy. Likewise, they will contain the rights of the holder, the mechanisms provided by the controller so that the owner becomes aware of the information processing policy and the substantial changes that occur therein or in the corresponding Notice of Privacy, how to access or enquire the information Processing policy.

When sensitive personal data is collected, the privacy notice must expressly indicate the optional nature of the response to the questions pertaining to this type of data.
In any case, the disclosure of the Notice of Privacy will not exempt the Controller from the obligation to inform the owners of the information processing policy.
The privacy notice is available to be consulted permanently on the Company's website: http://www.tgi.com.co/index.php/es/responsabilidad-global/proteccion-datos- personal

Paragraph: The Company reserves the right to modify the notice of privacy. In this sense, any change will be announced in due time on the website: http://www.tgi.com.co/index.php/es/responsabilidad-global/proteccion-datos-personales

Article 12. Personal data processing. TGI will conduct the processing, consisting of collecting, storing, using, circulating, registering, managing, reporting, processing, employing, evaluating, analyzing, confirming, updating and deleting, under standards of confidentiality, security, transparency, veracity, temporality, access and restricted circulation, in accordance with the regulating provisions and within the framework of the corporate purpose for administrative, operative, statistical, commercial purposes, and for everything deemed pertinent in furtherance of the functions, activities and operations comprised therein.

Article 13. Purpose. The Company's collaborators will only process personal data to fulfill a legitimate purpose related to their responsibilities. Consequently, the collection of personal data will be limited to those that are pertinent, adequate, necessary and useful for the purposes for

which they are collected or required in accordance with the Notice of Privacy.

Heading IV. Duties and Obligations

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

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

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

c) Properly inform the holder about the purpose of the collection and its rights by virtue of the authorization granted.

d) Inform at the request of the holder about the use given or that will be given to the data.

e) Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.

f) Process the queries and claims formulated in the terms set out in this policy, and carry out the update, rectification or deletion of the data in a timely manner.

g) Inform the Superintendency of Industry and Trade, in case of violations of the security codes and in case of risks in the administration of the information of the holders.

h) Comply with the instructions and requirements issued by the Superintendency of Industry and Trade.

i) Register in the database the legend "claim in process" when it is formulated by the holder of the information or "information in judicial discussion" once notified by the competent authority about judicial processes related to the quality of personal data.

j) Refrain from circulating information that is being objected by the holder and whose blocking has been ordered by the Superintendency of Industry and Trade.

k) Allow access to information only to people who are entitled to access it.

l) Guarantee that the information provided to the Processor is true, complete, exact, updated, verifiable and understandable.

m) Update the information, communicating in a timely manner to the Processor, all the news regarding the data that you have previously provided and adopt the other necessary measures so that the information provided thereto is kept up-to-date.

n) Rectify the information when it is incorrect and communicate the pertinent to the Processor.

o) Provide the Processor, as the case may be, only data whose Processing is previously authorized in accordance with the provisions of this law.

p) Demand the Processor, at all times, to respect the security and privacy conditions of the Holder's information.

q) Adopt an internal manual of policies and procedures to guarantee adequate compliance with this law and especially for the attention of queries and complaints.

r) Inform the Processor when certain information is under discussion by the Holder, once the claim has been submitted and the respective process has not been completed.

Article 15. Duties of the company towards those in charge of the processing. In the cases in which the Company, as controller, provides the processor personal information, it will do so in accordance with the following duties:

a) Provide, as the case may be, only data whose processing is previously authorized.

b) Guarantee that the information provided is true, complete, accurate, updated, verifiable and understandable.

c) Demand at all times, respect for the security and privacy conditions of the holder's information.

d) Demand compliance with the provisions set forth in the law and in this policy.

e) Inform when certain information is under discussion by the holder, once the claim has been submitted and the respective process has not been completed.

Article 16. Duties of the Processors. Processors must comply with the following duties, without prejudice to the other regulatory provisions that govern their activity:

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

b). Keep the information under the security conditions necessary to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access.

c). Timely update, rectify or delete the data in the terms of the regulations on the matter.

d). Update the information reported by the treatment controllers within five (5) business days from its receipt.

e). Process the queries and claims made by the holders in the terms indicated in the applicable regulations and this policy.

f). Adopt an internal manual of policies and procedures to guarantee adequate compliance with this law and, in particular, for the attention of inquiries and complaints from the holders.

g). Register in the database the legend "claim in process" in the manner in which it is set out in the regulations.

h). Insert in the database the legend "information in judicial discussion", once notified by the competent authority about judicial processes related to the quality of personal data.

i). Refrain from circulating information that is being objected by the holder and whose blocking has been ordered by the Superintendency of Industry and Trade.

j). Allow access to information only to those who can have access thereto.

k). Inform the Superintendency of Industry and Trade, in case of violations of the security codes and in case of risks in the administration of the information of the holders.

l). Comply with the instructions and requirements issued by the Superintendency of Industry and Trade.

Paragraph I. In cases where the Company acts as processing controller and processor, the duties provided for each one will be fulfilled.

Article 17. Obligations of the areas of the Company. For strict compliance of this policy on protection of personal data, each area of the Company must:

1. Make an inventory of the databases or files that it manages up to now, indicating the object, purpose and time of existence and report it to the Personal Data Protection Officer, within the term established thereby.

2. As of this date, if you need to create a database or file that contains personal information, the object, purpose and time of existence thereof must be established and reported to the Personal Data Protection Officer so that within ten (10) business days from the date of the request, a duly grounded concept is issued on its implementation and use. The negative concept of the Personal Data Protection Officer is equivalent to the prohibition of creating the requested database or file. However, if the area corrects the observations made by the Personal Data Protection Officer in its concept, if appropriate, a reconsideration of the decision may be requested thereto, with due grounds, in order for the officer to approve its constitution.

3. Prepare a detailed inventory of third personal data processors existing to date, explaining the activities carried out and analyzing the conditions of the processing, and submitting it to the Personal Data Protection Officer together with the contract or order, to study the contractual stipulations that regulate the legal relationship with the Company in the terms of this policy, as well as the criteria and methodology that the Company will use to carry out adequate supervision of compliance with the regulations on personal data protection by the third party processors. The Personal Data Protection Officer will announce the results of the study within the following fifteen business days.

4. Communicate to the Personal Data Protection Officer, should personal data processing be outsourced with a third processor, who must first inform the Personal Data Protection Officer of the activities to be carried out, the conditions in which the processing will be carried out, the methodology for this purpose, the manuals and policies for the protection of personal data obtained in market surveys, so that said Management determines that there is an adequate level of protection of personal data and that their invitation is endorsed.

5. Each time you need to modify the object, the purpose, the type of data, and the time of existence of a database or file, it must be reasonably justified through written communication or email, which will be sent to the Personal Data Protection Officer so that, within ten business days from the date the communication is received, the officer issues a favorable or unfavorable opinion for the implementation thereof. The negative concept of the Personal Data Protection Officer is equivalent to the prohibition of modifying the database or file. However, if the area corrects the observations made by the Personal Data Protection Officer in its concept, if appropriate, it may request a reconsideration of its decision with the due grounds, so that it approves its modification.

6. It must define the worker(s) who may exclusively process personal data and will inform the Personal Data Protection Officer so that, within ten business days from receipt of the communication, the officer prepares the content of the obligations to be included in the job profile. In turn, the Personal Data Protection Officer will send the requesting area the content of the obligations so that it can manage the update of the job profile and responsibilities with the Human Resources Management.

7. Ensure that databases or files containing only negative or adverse information will not be implemented.

8. Make the content of the notice of privacy known to the holder of the information before issuing the authorization, to guarantee that the holder knows all the purposes of the information.

9. Review in an informal and timely manner the notice of privacy prepared by the Personal Data Protection Officer and propose the inclusions or adjustments deemed pertinent.

10. Send the Personal Data Protection Officer the formats in which personal data available to date are collected, and which are part of the Integrated Management System, indicating the purpose thereof and the information to be collected, so that said Management, within ten business days from receipt of the communication, determines whether or not it is necessary to include the authorization for the processing thereof.

11. As of this date, each time formats are to be created to collect information, the Personal Data Protection Officer must be submitted the draft of said format indicating the purpose thereof and the information to be collected, so that said Management, within ten business days from receipt of the communication, determines whether or not it is necessary to include the authorization for the processing thereof.

12. It must adopt all measures that prevent unauthorized access to third parties, to protect the information, avoiding its manipulation, alteration or deletion and take into account that the personal information collected in databases or files is of restricted circulation; therefore, as a general rule, it will only be disclosed to third parties authorized by the holder according to the authorized or legitimate purposes to request such information.

13. Assist in the implementation and consolidation of the Personal Data Processing Policy and the principle of proven responsibility led by the Personal Data Protection Officer.

Article 18. Obligations of the bidders and contractors. All bidders and contractors of the Company will guarantee an adequate level of protection of personal data at all stages of the processing they carry out.

Likewise, they will guaranty that any personal information they are controlling, and which must be furnished to the Company in furtherance of the offer or the contract, is subject to due processing in accordance with the regulations on personal data protection and that there is prior authorization, consent and that it is susceptible to subsequent consultation.

Heading V
Procedure for the receipt and resolution of inquiries and claims.

Article 19. Legitimation for the exercise of the rights of the holder. The rights of the holder may be exercised by the following people:

1. By the holder, who must sufficiently prove its identity by the different means made available by the controller.
2. By its successors, who must prove such quality.
3. By the representative and / or attorney-in-fact of the holder, prior accreditation of the representation or power of attorney.
4. By stipulation in favor of another, or for another party.
5. The rights of children or adolescents will be exercised by persons empowered to represent them.

Paragraph I. The holder, its successors or the legitimized person must attach to the query or claim a copy of their identity document and the others deemed necessary to support their request.

Paragraph II. If the query or claim refers to a deceased owner, the spouse, permanent partner and / or successors in title must submit the request, attaching an authentic copy of the death certificate of the holder of the information and an authentic copy of the registry that proves the relationship (of marriage, birth, etc.) or an off-court declaration in cases of de facto marital union.

Article 20. Queries. The query will be made through the means authorized by the Controller or the Processor, as long as proof of this can be maintained. The person entitled to this effect will make queries through written communication or by email, in order to: i) determine his/(her identity (full name and personal identification number); ii) specify in a clear, specific, detailed and justified manner the object of the query; iii) establish and accredit the legitimate interest with which he/she acts, always attaching the pertinent supports, for example, power of attorney with a note of acknowledgment of content and signature before a notary public and, iv) report physical and / or electronic address to be served with notices.

The main subjects for queries include:

a) Request for information on access to personal data
b) Request for proof of authorization
c) Queries on the use that has been given to the information

Paragraph: The requested information may be provided by any means, including electronic, as required by the holder, so that it is easy to read, without technical barriers that prevent access and such information must entirely reflect the one that rests in the database.

Article 21. Claims. i). The claim will be formulated by means of a request addressed to the Controller or the Processor, with the identification of the Holder, the description of the facts that give rise to the claim, the address, and attaching the documents to be enforced. The holder, its successors in title or another person with a legitimate interest may submit a claim in writing or by email to the responsible area, which will contain: i) the determination of identity (full name and personal identification number; ii) a clear, specific, detailed and well-grounded statement of the object of the claim; iii) the manifestation of the legitimate interest with which it acts as well as its accreditation, always attaching the pertinent supports, for example, power of attorney with a note of acknowledgment of content and signature before a notary public and, iv) the physical and / or electronic address to be served with notices.

The main subjects for claims include: -

a) Correction or updating of the holder's personal data.
b) Partial or total revocation of the authorization of the processing.
c) Deletion of personal data.

Article 22. Correction or updating of the holder's personal data. The claim consisting of the correction of personal data must contain, in addition to the requirements established in the previous article, the specification of the corrections to be made and must include the documentation supporting the request.

Article 23. Partial or total revocation of the authorization of the processing. The holders of personal data are entitled to revoke the authorization when the principles, rights and constitutional and legal guarantees are not respected in the processing, which will proceed in those cases in which the Company has submitted the request or in which, the personal data protection authority so orders it.

However, if the Company considers that the revocation is not appropriate, it will inform it by means of a duly grounded communication, within the terms provided in number vii of article 28 of this Policy.

For its part, once the authorization is revoked, the Company will proceed to eliminate the information contained therein from the respective databases.

Article 24. Deletion of personal data. The holders of personal data are entitled to delete them when the principles, rights and constitutional and legal guarantees are not respected in the processing.

The claim consisting of the request for the deletion of personal data must contain, in addition to the requirements established in article 21 of this policy, the identification of the data whose deletion is intended and will proceed in those cases in which the Company so determines or in which the personal data protection authority orders it.

Article 25. Irrelevance of the request for deletion of the data or revocation of the authorization. The request to delete the information and the repeal of the authorization will not proceed when the Holder has a legal or contractual duty to remain in the database.

Article 26. Data of the Controller and Personal Data Protection Officer. The processing controller is Transportadora de Gas Internacional S.A. ESP- TGI SA ESP, whose NIT is 900.134.459-7 located in Carrera 9 No. 37-69 Piso 7, Bogotá, D.C. Telephone 3138400

The Personal Data Protection Officer who has the necessary powers to receive, attend and resolve inquiries and claims from holders of personal data or persons entitled to do so is Álvaro de Angulo Sanz, Director of Corporate Affairs of TGI S.A. ESP, a subsidiary of the Grupo Energía de Bogotá, email datospersonales@geb.com.co.

Article 27. Procedure to answer questions. When a query is presented, the following actions must proceed:

i). Documentary Management will deliver the query in physical and / or electronic form to the Personal Data Protection Officer, who will take care of the query.

ii). The Personal Data Protection Officer will review, within the following two business days, that the query has been submitted by the holder of the information or whoever is entitled to do so in accordance with the requirements established in article 20 of this policy.

iii). If the query does not meet all the requirements established in article 20 of this policy, it will not be addressed, and the reasons will be reported to the sender.

iv). If the query meets the requirements established in article 20 of this policy, the purpose thereof will be analyzed to determine if the provision of information and / or support from another area of the Company is required. If so, the Personal Data Protection Officer will send the query by email to the head of the respective area so that, within two (2) business days from receipt, he can pronounce on the merits and, if it is the case, to provide the relevant documentation to address the query.

v). Queries will be addressed within a maximum term of ten (10) business days as of the date of receipt thereof. When it is not possible to attend it within said term, the interested party will be informed, stating the reasons for the delay and indicating the date on which their query will be resolved, which in no case may exceed five (5) business days following the expiration of the first term.

Article 28. Procedure to attend claims. When filing a claim, the following procedure must be followed:

i). Documentary Management will deliver the claim in physical and / or electronic form to the Personal Data Protection Officer, who will immediately assign it to the professional in charge of the personal data protection policy.

ii). The Personal Data Protection Officer will review, within the following two (2) business days, that the claim has been submitted by the holder of the information or whoever is entitled to do so in accordance with the requirements established in article 21 of this policy.

iii). If the claim is incomplete, the interested party will be required within five (5) days after receiving it to correct the faults. If two (1) months elapse from the date of the requirement, without the applicant having submitted the information required, it shall be understood that the claim was waived.

iv). In the event that the Company is not competent to resolve the claim, it will transfer it to the corresponding person within a maximum term of five (5) business days and will inform the interested party of the situation.

v). Once the complete claim is received, a legend that says "claim in process" and the reason therefor will be included in the database, within a term not exceeding five (5) business days. Said legend must be kept until the claim is decided.

vi). The purpose of the claim will be analyzed to determine if the provision of information and / or support from another area of the Company is required. If so, the Personal Data Protection Officer will send the claim by email to the head of the respective area so that, within two working days from receipt, he can pronounce on the merits and, if applicable, to submit the pertinent documentation to address the query.

vii). The maximum term to address the claim will be fifteen (15) business days from the day following the date of receipt. When it is not possible to address the claim within said term, the interested party will be informed of the reasons for the delay and the date on which the claim will be resolved, which in no case may exceed eight (8) business days following the expiration of the first term.

Heading VI. Final Provisions

Article 29. Legal advisor. The Personal Data Protection Officer will provide advice to the areas and collaborators that request it.

Article 30. Compliance verification. The Internal Audit Department will verify strict compliance with this Policy in all the audits it carries out and will report the results thereof to the Personal Data Protection Officer.

Article 31. Induction and Re-Induction. The Human Management Department or the area acting as such will include, as a point of the program of each induction and reinduction, that pertaining to personal data protection, for which it will request the Personal Data Protection Officer to make the respective presentation.

Article 32. Confirmation of references. Only the Human Management Department or whoever acts as such is the area authorized to confirm employment references. For this purpose, the holder of the information must communicate in writing or by email to said area, the entity that will be contacted to confirm the references and authorize to proceed in this regard.

In the case of contractors, it will be the auditor or supervisor who will confirm the references. For this purpose, the owner of the information must communicate in writing or by email the entity that will be contacted to confirm the references and will authorize to proceed in this regard.

Paragraph. The confirmation of references will be made on positive information and never on negative or adverse data to the holder.

Article 33. Temporality of the processing. The processing of personal data by TGI will be carried out during the term of relevance of the data and, in any case, until the fulfillment of the purpose(s) for which it was authorized or when is appropriate by legal or contractual provision.

Negative or adverse information will remain for a period of five years, unless the law provides for a shorter period. Once the maximum term of permanence has expired, the negative data will be eliminated from the respective database or file, guaranteeing the data holders' right to be forgotten.

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

Article 35. Principle of proven responsibility. The Company will implement the principle of proven responsibility for which it will strive to have a high organizational culture in terms of personal data protection and the commitment of senior management on the matter, in accordance with the guidelines implemented by the Superintendency of Industry and Trade.

Article 36. Term. This policy for the processing of personal data applies from the date of issue.

Issued in Bogotá D.C., on 22 November 2016