TRAXIÓN
LIFE IN MOTION

PERSONAL DATA PROTECTION POLICY GRUPO TRAXIÓN, S.A.B. DE C.V.

August 2022

TABLE OF CONTENTS

1. INTRODUCTION

Information technologies, databases and electronic supports where information is stored have become an important part of the business process for the Responsible. As a consequence, information has been growing as an economic factor, however, the incorrect or abusive use of this information carries the risk of violating the rights of personal data holders or causing economic damage, which in some cases is irreparable.

The interests and values protected by data protection laws are a critical aspect to consider when the Responsible is dealing with employees, suppliers, customers and third parties with whom it has a legal relationship. In these relationships, it is essential that business processes comply with the legal requirements that protect such interests and values.

2. OBJECTIVE

The objective of this policy is to establish guidelines for the Protection of the Owner's Personal Data by the Responsible Party, in accordance with the provisions of the LFPDPPP and its Regulations.

3. SCOPE

This policy is obligatory and applies to all companies, affiliates and subsidiaries of Traxion and is mandatory for all officers, directors and collaborators of the company, as well as for third parties that have a contractual relationship with the company.

4. REFERENCES

4.1. Internal

- Code of Ethics
- Anti-Corruption and Integrity Policy
- Compliance Policy
- Information Security Policy
- Attention to Complaints and Disputes of Holders Policy
- Personal Data Department
- Privacy Notice Management Policy

- Information Classification Policy
- Personal Data Retention, Blocking and Deletion Policy
- Procedure for the Attention and Follow-up of ARCO Rights.

4.2. External

- Federal Law on the Protection of Personal Data in Possession of Private Parties (LFPDPPP)
- Regulation of the Federal Law on the Protection of Personal Data in Possession of Private Parties (RLFPDPPP).

5. DEFINITIONS

Term	Description
a. Privacy Notice	Physical, electronic or any other document generated by the Responsible Party that is made available to the Owner, prior to the Processing of their Personal Data, in accordance with the obligation established in the Law.
b. Data Base	The ordered set of Personal Data relating to an identified or identifiable natural person.
c. Consent	Manifestation of the will of the Owner of the Personal Data by means of which the Processing of the same is carried out.
d. Personal Data	Any information concerning an identified or identifiable natural person.
e. Sensitive Personal Data	Those Personal Data that affect the most intimate sphere of its Owner or whose improper use could give rise to discrimination or entail a serious risk for him/her. In particular, sensitive are those that may reveal aspects such as racial or ethnic origin, present and future state of health, genetic information, religious, philosophical and moral beliefs, trade union membership, political opinions, sexual preference.
f. Personal Property or Financial Data	Those that contain names, addresses, telephone numbers or email addresses, together with bank card or financial services numbers, account numbers, credit limits, balances, user identifiers or authentication information and passwords that allow the identification of the Account Holder.
g. ARCO Rights	These are the rights of access, rectification, cancellation and opposition that the Owner may exercise.

Term	Description
h. Person in charge	The natural or legal person who, alone or jointly with others, processes Personal Data on behalf of the Responsible.
i. INAI	National Institute of Transparency, Access to Information and Protection of Personal Data.
j. Law o LFPDPPP	Federal Law on the Protection of Personal Data in Possession of Private Parties, published on July 5, 2010.
k. Administrative Measures	Policies and standards that establish the rules that govern how security should be carried out within the organization in terms of systems and people.
l. Technical Measures	It is the implementation of security controls, previously established in the organization's policies and standards, on electronic media, telecommunications and information technology services and infrastructure, among others.
m. Obtaining	Collection of Personal Data that the Responsible Party carries out from the Owner.
n. Policy	It refers to this Personal Data Protection Policy that governs the Reponsible.
o. Personal Data Protection Program	The set of policies, measures, processes, procedures and safeguards aimed at ensuring the rights of the Data Subjects in the Processing of their Personal Data.
p. Regulation	The Regulations of the Federal Law on the Protection of Personal Data in Possession of Private Parties.
q. Remission	The communication of Personal Data between the Responsible Party and its Processors, inside or outside Mexican territory.
r. Responsible Party	Grupo Traxión, S.A.B. de C.V., a legal entity that decides on the processing of Personal Data that it collects.
s. Electronic support	Storage medium that can be accessed only through the use of an apparatus with electronic circuits that processes its contents to examine, modify or store personal data, including microfilms.
t. Fisical Support	Medio de almacenamiento inteligible a simple vista, es decir, que no requiere de ningún aparato que procese su contenido para examinar, modificar o almacenar los datos personales.
u. Third Party	The natural or legal person, national or foreign, other than the Owner or the Person Responsible for the Personal Data.
v. Owner	The natural person to whom the Personal Data corresponds.

Term	Description
w. Transfer	Any communication of data made to a person other than the Data Controller or Data Processor to a third party, the communication may occur, among other acts, by sending the data to the third party by physical or electronic means.
x. Treatment	The collection, use, disclosure or storage of Personal Data, by any means. Use includes any action of access, handling, use, transfer or disposition of Personal Data.

6. GUIDELINES

6.1. Regulatory Framework

The Responsible Party defines and formalizes the guidelines established in this document, based on what is established by the INAI, in relation to the LFPDPPP and its Regulations; The articles applicable to this policy are listed below.

6.1.1 Federal Law on the Protection of Personal Data in Possession of Private Parties

"Article 6.- Those responsible for the processing of personal data must observe the principles of legality, consent, information, quality, purpose, loyalty, proportionality and responsibility, provided for in the Law."

"Article 30.- Every person responsible shall designate a person, or department of personal data, who shall process the requests of the holders, for the exercise of the rights referred to in this Law. It will also promote the protection of personal data within society."

"Article 64.- Infringements of this Law shall be sanctioned by the Institute with: I. The warning for the responsible party to carry out the acts requested by the owner, in the terms provided for by this Law, in the case of the cases provided for in section I of the previous article. II. A fine of 100 to 160,000 days of the minimum wage in force in the Federal District, in the cases provided for in sections II to VII of the preceding article; III. A fine of 200 to 320,000 days of the minimum wage in force in the Federal District, in the cases provided for in sections VIII to XVIII of the preceding article, and IV. In the event that the infractions mentioned in the preceding paragraphs persist repeatedly, an additional fine shall be imposed ranging from 100 to 320,000 days of the minimum wage in force in the Federal District. In the case of infringements committed in the processing of data."

"Article 67.- A term of imprisonment of three months to three years shall be imposed on anyone who, being authorized to process personal data for profit, causes a breach of security to the databases in his custody. Article 68.- Any person who, for the purpose of obtaining undue profit, processes personal data by deception, taking advantage of the error in which the owner or the person authorized to transmit them is found, shall be punished with imprisonment of six months to five years."

"Article 69.- In the case of sensitive personal data, the penalties referred to in this Chapter shall be doubled."

6.1.2 Regulation of the Federal Law on the Protection of Personal Data in Possession of Private Parties

"Article 48.- In terms of Article 14 of the Law, the responsible party must adopt measures to guarantee due treatment, privileging the interests of the owner and the reasonable expectation of privacy.
Among the measures that the responsible party may adopt are at least the following:

I. Develop mandatory and enforceable privacy policies and programs within the organization of the controller.
II. Implement a program of training, updating and raising awareness of personnel on personal data protection obligations.
III. Establish a system of internal supervision and surveillance, external verifications or audits to verify compliance with privacy policies.
IV. Allocate resources for the implementation of privacy programs and policies,
V. Implement a procedure to address the risk to the protection of personal data due to the implementation of new products, services, technologies and business models, as well as to mitigate them.
VI. Periodically review security policies and programs to determine the modifications that are required.
VII. Establish procedures to receive and respond to doubts and complaints from the owners of personal data.
VIII. Have mechanisms in place to enforce privacy policies and programs, as well as sanctions for non-compliance.
IX. Establish measures for the securing of personal data, that is, a set of technical and administrative actions that allow the responsible party to comply with the principles and obligations established by the Law and these Regulations.

X. Establish measures for the traceability of personal data, that is, actions, measures and technical procedures that allow personal data to be traced during processing."

6.2. Responsibilities

All areas of the Responsible that, due to their functions and business processes, process personal data (collection, storage, transfer, remittance, blocking and cancellation) are responsible for complying with the provisions of this policy and for making good use of such information, and must meet the requirements in terms of controls, processes and information requested by the Personal Data Department. with respect to the applicable regulations. Likewise, it is the responsibility of each area to keep the inventory of Personal Data updated and to deliver changes and updates to the Personal Data Department.

In particular, the functions of each area of the Responsible are as follows:

6.2.1 Personal Data Department

In order to comply with the provisions of Article 3, section XIV and Article 6 of the LFPDPPP, Grupo Traxión, S.A.B. de C.V. will act as responsible in terms of said Law for the Personal Data that it obtains and processes. Therefore, they will decide on the Treatment of Personal Data in terms of the LFPDPPP, for which they will have a Personal Data Department to comply with the provisions of the applicable regulation.

6.2.2 Compliance Office (Compliance Audit)

Monitor the compliance of the areas that process personal data with the guidelines established in this Policy to ensure compliance with the LFPDPPP.

6.2.3 Legal

1. Document, formalize and collaborate with the Personal Data Department in monitoring and attending to the execution of ARCO Rights.

2. To pay attention to the official notices issued, inspection visits, fines, sanctions, requests for information by the INAI, and in the preparation of writings to that authority and to the holders; and;

3. Design data protection clauses in contracts, agreements, annexes, etc., assist in any requirement or query made by the Personal Data Department in accordance with the provisions established in the LFPDPPP, its Regulations and the Privacy Notice Guidelines released in the Official Journal of the Federation on January 17, 2013.

6.2.4 Human Resources

Train the Responsible Person's staff in relation to this Policy and the documents derived from it and ensure that the organization is aware of the procedures for attention and monitoring of the ARCO Rights for each Owner, the policies for retention, blocking and elimination of Personal Data, the information classification policy and the technical security measures, administrative and physical measures that must be followed to comply with the Law and its Regulations, and must sensitize the collaborators that, in case of non-compliance with the regulations established by the Responsible Party, they will be subject to sanctions and fines by the INAI.

6.2.5 Information Technologies

1. Establish, document, formalize and guarantee the procedures, guidelines, security measures (administrative and technical) for the protection and security of personal data found in electronic media.

2. Establish security policies to manage access to IT services and ensure that application access profiles are assigned according to the user's role and check if the user is authorized. Such user profiles shall be properly designed with a segregation of duties in application activities with business process activities.

6.3. Principles for Treatment

For the Processing of the Personal Data of the Owner, the Responsible will be based on the following principles:

a) At all times, the interests and rights of the Owner will be privileged;
b) In case of doubt, it is assumed that the Owner has the right to have their data treated confidentially and in accordance with this Policy;

c) All processing of personal data will be subject to the Consent of the Owner;

d) Personal Data will be processed for the purposes for which they were obtained, in terms of the corresponding Privacy Notices and in accordance with the consent obtained from their Owners with whom they have a legal and/or commercial relationship;

e) Personal Data may only be processed by the Responsible Party if it is legally permitted to do so, in terms of the Law and other applicable regulations;

f) Measures will be established to verify that the Personal Data contained in its Databases are relevant, correct and kept up to date;

g) Personal Data may only be kept for the time required by the purpose defined for the processing, so when they are no longer necessary for the fulfillment of the purposes, they must be deleted. Notwithstanding the foregoing, the mandatory storage period derived from a contractual relationship or applicable legislation and in particular, the regulations issued for the insurance sector will be respected;

h) Only Personal Data that is adequate, necessary and relevant for the determined purpose will be processed;

i) Sensitive Personal Data Databases may not be created, except in cases where their creation is justified for legitimate, specific purposes and in accordance with the activities or explicit purposes of the Responsible Party;

j) Technologies or practices that allow Personal Data to be obtained in a deceptive or fraudulent manner will not be used;

k) Personal Data Transfers will only be made to companies that comply with the Law and that offer similar protection standards to this Policy, as long as the Owner's Consent is obtained; and

l) All areas that use Personal Data to have direct contact or through a Third Party with the Data Subject by any means, whether for commercial prospecting, collection, collection reminders, advertisements, promotions, must be made known, within 5 (five) business days following the collection of the personal data, of the Personal Data Department before being released (communicate it within a term of no more than 5 business days) in order to have identified and inventoried these contacts with the Owner and to have control at the time that any blocking or cancellation requirement is generated by the Owner or the INAI, but to review the Privacy Notices or Consents implemented or to be implemented.

6.4. Submission of Evidence

The Personal Data Department is the figure in charge of implementing, executing, monitoring and promoting the protection of Personal Data within the Responsible Party and among its main responsibilities are the following:

a) Define guidelines to be followed by the areas for the proper treatment of Personal Data.
b) Evaluate and authorize the creation of new Personal Data Databases.
c) Define, design and elaborate the means of communication for the reception of ARCO Rights and tools to monitor these rights.
d) Issue statements emphasizing the risks of non-compliance with the LFPDPPP and its impact on the Responsible Party, as well as the importance of complying with the established activities.
e) To approve the model clauses that must be established in the contracts entered into with third parties in terms of personal data protection.
f) Analyze and Authorize Transfers or Submissions of Personal Data.
g) Receive, coordinate, attend and take the necessary measures in case of requirements, visits or procedures of the INAI in conjunction with the areas involved.
h) Review and propose changes or modifications to this Policy when appropriate.
i) Coordinate the areas that must participate in the execution of this Personal Data Protection Policy and Program within the organization and establish their responsibilities.
j) To be the function of internal consultation of all areas of the Responsible Party regarding the Processing of Personal Data.
k) Supervise the activities of the different areas in the field of Personal Data Protection.
l) Propose best practices in the field of Personal Data Protection.
m) To receive and monitor the exercise of the ARCO Rights of the Holders.
n) Establish criteria and guidelines regarding the processing of Personal Data, periods of conservation, blocking, deletion or destruction of information in conjunction with the areas that handle personal data.
o) Establish the guidelines for the correct implementation of privacy notices and obtaining consents for the various Owners with whom the Responsible Party has any type of legal and/or commercial relationship, or from which personal data has been obtained.
p) Immediately attend to notifications of information violations and establish a reaction protocol for these cases, in conjunction with the areas involved and Legal.
q) Establish the guidelines on data protection for the hiring of Third Parties.

r) In conjunction with the areas involved, design, elaborate and update the necessary policies, procedures and documents that regulate the activities, controls and security measures related to the processing of personal data, such as: delivery of privacy notices, safeguarding of information, blocking and cancellation of information, as well as any other activity or transaction related to the processing of personal data.

s) Prepare the corresponding Privacy Notices by type of Owner and channel of collection.

6.5. Guidelines for Treatment

6.5.1 Treatment

The collection and processing of personal data for the various processes and services of the Responsible Party will be subject to the following guidelines:

a) The creation of new products that involve the collection and processing of personal data of Owners must be notified to the Personal Data Department, for its analysis of privacy impact and approval.

b) Changes or updates to the products, where it implies the modification or new obtaining of personal data of the Holders, must be notified to the Personal Data Department, for review and approval. No modification or update may be released without prior approval from the Personal Data Department.

c) Changes or updates or new products may not be released unless the corresponding privacy notice considers it and is approved by the Personal Data Department.

d) Changes or updates to policies or procedures related to the processing of personal data or any other situation that impacts the processing of personal data must be notified to the Personal Data Department for analysis and approval.

e) It is the obligation of the areas that, for the execution of their operations, follow and establish the appropriate measures for the processing of the Sensitive Personal Data and Personal Patrimonial or Financial Data of the Owners that are described in this Policy and in the Personal Data Security Management System.

f) In cases where it is not necessary to identify the Owner, for statistical purposes, such information must be stored in a dissociated manner, among others.

g) The Owner must be informed about the treatment that will be given to their Personal Data, through the Privacy Notice, which will be limited to the fulfillment of the purposes set forth therein and which will be made available to them before the registration and/or any processing of their Personal Data.

h) Each of the areas that collect personal data must develop mechanisms, as well as manage the resources to collect and safeguard the evidence of the availability of the Privacy Notice to the Owner and the consents that were collected, according to the control guidelines established by the Personal Data Department.

6.5.2 Collection

a) The collection of Personal Data will be through secure means and/or those established by the Responsible Party.
b) Information on personal, sensitive and/or patrimonial data must not be handled or sent through unsecured means of transmission such as FTP, physical formats in folders or envelopes that are not closed or sealed, among others that are not defined in this policy or the Personal Data Security Management System.
c) Personal Data may not be obtained without making the corresponding Privacy Notice available to the Owner prior to Collection. Such Privacy Notices must comply with the provisions of section 6.7 of this policy.

6.5.3 Collection through Processors or Third Parties

In the event of obtaining Personal Data through a Processor or Third Party with whom a legal or commercial relationship is maintained and who act in the name and/or on behalf of the Responsible Party, the following must be verified and documented:

a) That the consent has been obtained in terms of the LFPDPPP for the Processing and, where appropriate, the Remittance of Personal Data to Third Parties with whom they rely to comply with contractual obligations or acquired by a claim, as well as for secondary purposes, including commercial prospecting.
b) The delivery of the privacy notice used by the Person in Charge is that of the Responsible, if applicable, the one used by the Third Party.
c) That the contract includes the obligation to indemnify the Responsible Party for damages caused by the Transfer, use, loss, misplacement, leakage or profit of Personal Data in contravention of the Consent granted by the Owner or the applicable legal provisions.

In addition, through guidelines issued by the Personal Data Department, the time and manner in which it must make its Privacy Notice known to the Owners and the

way in which it must obtain consent in response to the Personal Data collected and processed will be established.

The Personal Data Department will establish procedures to ensure that the data comply with the principles of quality, legality, proportionality and others established by the LFPDPPP, which must be complied with by the area that obtains the Personal Data.

In any case, the collection of Personal Data through Third Parties with whom a legal or commercial relationship is maintained must be subject to analysis and approval by the Personal Data Department.

6.5.4 Storage

a) The storage of Personal Data must be carried out on physical and electronic supports through secure mechanisms that allow the data to be protected from theft or loss, unauthorized access, alteration or unauthorized disclosure.
b) All physical documentation containing Personal Data will remain stored under lock and key or safeguarded in locked or locked places and access restricted to only authorized users.

6.5.5 Conservation

Physical and electronic repositories containing Personal Data will be kept for the period of time established in the Personal Data Retention, Blocking and Elimination Policy, which establishes the retention periods of such information, also considering the retention periods established in the legal provisions applicable to the sector or other applicable legislation.

6.5.6 Blocking

a) In cases where it is required to delete a record containing Personal Data, which is located in physical or electronic repositories, prior to its deletion, it will enter a blocking period in accordance with the provisions of the Personal Data Retention, Blocking and Elimination Policy. After that period, they may be eliminated.
b) During the period of blocking of Personal Data in physical or electronic media, such information may not be accessed, nor may it be modified or updated. In case of requiring a query to be made to said information, the authorization of the Personal Data Department must be requested and it will be validated that the integrity of the information is not affected during the consultation.

6.5.7 Cancellation

Physical and electronic repositories containing Personal Data will be preserved and deleted in accordance with the Personal Data Security Management System and the Personal Data Retention, Blocking and Elimination Policy, as well as the legal provisions applicable to the matter.

6.5.8 Treatment of Sensitive and Financial Personal Data

By virtue of the fact that the processing of Sensitive Personal Data and/or Personal Patrimonial or Financial Data are necessary for the operation of the areas, these must be treated in the manner established below:

a) Any procurement shall be subject to an exercise of minimisation and proportionality before being released within a business process.
b) The Consent of the Owners must be obtained in the formats authorized by the Department of Personal Data for this purpose, said consent must be obtained expressly and in writing by means of the handwritten signature, electronic signature or any authentication mechanism of the Owner that is established for this purpose.
c) The processing must only be carried out by the persons authorised to do so by virtue of the functions included in the job description within the Responsible Party.
d) They will be stored in electronic repositories and safeguarded with encryption methods.
e) The transfer or remittance of sensitive or patrimonial Personal Data must be carried out through authorized and secure means of communication, taking the necessary measures, such as data encryption, digital signatures, among others to avoid unauthorized access, loss or corruption of the information during its transmission.
f) The processing of Sensitive Personal Data and Personal Patrimonial or Financial Data must be carried out only by the persons authorized to do so by virtue of the functions included in the job description within the companies of the Responsible Party.

6.5.9 Personal Data Inventory

a) The Personal Data Department will draw up an inventory of Personal Data for the business processes they handle. As well as mapping the flow of the treatment given to Personal Data.

b) Each area will keep this inventory and flow of Personal Data processing updated annually. Any changes made to business processes in relation to the collection of Personal Data must be notified to the Personal Data Department.

6.6. ARCO Rights Attention Procedure

The Personal Data Department is in charge of attending and responding to requests for the exercise of ARCO Rights, revocation of Consent and refusal of commercial prospecting made by the Owners, with the support of the areas that handle personal data, for this it must consider the following:

a) Issue the forms that must be filled out by the Owners for their exercise.
b) In order to exercise the ARCO rights, the request must be submitted through the Responsible Party's email address in accordance with the provisions of the corresponding Privacy Notices and must be accompanied by the information and documentation necessary to prove the Owner's personality and make it easier to identify the Owner's Personal Data in accordance with the established ARCO Rights Procedure. In the event of revocation of Consent and refusal of commercial prospecting, it must be done through the email address of the Data Controller in accordance with the established procedure.
c) The Personal Data Department will issue the procedure for the attention of requests for the exercise of ARCO Rights, revocation of Consent and refusal of commercial prospecting.
d) Any response and attention to the ARCO Right, revocation of Consent and refusal of commercial prospecting will be kept registered and safeguarded in email and in the computer equipment of the legal representative of the Personal Data Department for such follow-up and will contain the documentation and evidence that supports the exercise of the ARCO Right or not. revocation of Consent and refusal to prospect for trade and its execution if applicable.
e) The attention and exercise of the ARCO Rights, revocation of Consent and refusal of commercial prospecting requested by the Owner, will be aligned with the times and guidelines established in the LFPDPPP and its Regulations.

6.7. Privacy Notice

The Personal Data Department is responsible for preparing the corresponding privacy notices to obtain the consent of the Owner. Such notices must comply with the provisions of Article 16 of the LFPDPPP, Article 26 of the Regulations and Article Twentieth of the Privacy Notice Guidelines, and must contain at least:

a) Name and address of the Responsible Party;
b) The data that are processed, expressly indicating those considered sensitive and patrimonial;
c) Indicate data that are obtained indirectly and through publicly available sources or transfers;
d) Describe the purposes of the Processing of personal data;
e) To expressly distinguish the secondary purposes;
f) Identify the third parties or types of third-party recipients to whom Personal Data may be transferred, as appropriate and necessary;
g) Indicate the purposes of the transfers of Personal Data;
h) Clause indicating whether or not the Owner accepts the transfer of Personal Data;
i) Information about remote or local means of electronic, optical or other technology, through which Personal Data is collected;
j) Options and means that the Controller offers to limit the use or disclosure of your Personal Data;
k) Mechanisms to revoke consent to the Processing of Personal Data;
l) The means for the Holders to exercise their ARCO Rights, and;
m) Mechanism for expressing refusal to process secondary purposes;
n) The procedure and means through which the Data Controller will notify the Data Controllers of the changes in the privacy notice.

Depending on the means or channel of obtainment, the Owner must be presented with the Privacy Notice in its integral, simplified or short format and attend to the information that in each case it must contain, in accordance with the LFPDPPP, its Regulations and the Privacy Notice Guidelines released in the Official Gazette of the Federation on January 17, 2013 and/or in accordance with the regulations and guidelines of Privacy Notices Current.

The Personal Data Department must ensure that the Privacy Notices contain all the information required by the LFPDPPP and give its approval for their release and use. The Personal Data Department will validate that the wording of the Privacy Notices complies with the following:

i. It does not persist with inaccurate, ambiguous or vague phrases;
ii. Take into account the profiles of the Owners;
iii. Do not include texts or formats that induce the holder to choose a specific option;
iv. In the event that it includes boxes for the Owner to grant their consent, it must not be previously checked, but on the contrary it is the Owner who marks the option as a sign of their consent;
v. Do not refer to texts or documents that are not available to the Owner;

vi. The Owner is expressly informed of the Personal Data that is collected from them and for what purposes;
vii. Are aligned with the Privacy Notice Guidelines released in the Official Journal of the Federation on January 17, 2013 or any other guideline or provision released by the INAI.

The consent of the Data Subjects to the Privacy Notices must be reliably obtained, as the burden of proof falls on the Data Controller. Consequently, the Personal Data Department will establish the necessary control mechanisms and support the areas that handle and collect personal data to, if necessary, demonstrate to the authorities the Privacy Notice that the Owner consented, reliably evidencing the way in which the Privacy Notice was made available to the Owner and which was in force at the time they will grant their consent.

In the case of Sensitive Personal Data, it will be necessary to obtain the prior, express and written consent of the Owner for its processing, in accordance with this policy.

The documents containing the consent of the Data Subjects for the processing of Personal Data will be stored indefinitely. These documents may only be destroyed once it is ensured that the Personal Data of the Owners is not available, either because it was requested by the Owner or at the end of the legal relationship or purpose for which they were collected, and evidence of the corresponding destruction must be left.

The business areas will refrain from creating, publishing and using Privacy Notices outside of those released by the Personal Data Department.

The Personal Data Department will maintain control over the released privacy notices, through the management of a version control and a record of the privacy notices published, their modifications and measures taken to notify such modifications.

6.8. Transfers

a) The Responsible Party must ensure that all Personal Data Transfers are reported through the corresponding Privacy Notices and will obtain the consent of the Owner, under the terms of the LFPDPPP, except when the Transfer is carried out under any of the exceptional cases established by the LFPDPPP.
b) The Transfers of Personal Data to a Processor or Third Party that will process the information for their own purposes and under their policies, must be

informed and consented to by the Owners in terms of the LFPDPPP and within the corresponding Privacy Notices.

c) Any transfer of the Personal Data repositories carried out by any area in the exercise of its powers will be notified to the Personal Data Department for its analysis and approval.

d) Transfers may only be made to Third Parties with the security standards established by the Responsible Party in the Personal Data Security Management System.

e) Any Transfer of Personal Data to Third Parties must be documented, detailing the terms, purposes, treatment and responsible persons who receive the Personal Data. Such transfer will be documented by the area responsible for carrying out and with the authorization of the Personal Data Department.

f) All Personal Data Transfer in electronic format must be carried out using authorized and secure means of communication, taking the necessary measures, such as data encryption, digital signatures, among others to avoid unauthorized access, loss or corruption of information during its transmission.

g) In case of requiring the acquisition of any technological resource for the secure transfer of information, the user area must manage the resources to carry it out and comply with this policy.

h) All the Transfer of Personal Data in physical format must be carried out through closed containers and executing a verification mechanism that the information was delivered in its entirety.

i) Personal Data may not be transferred to any Third Party, as long as a contract has not been entered into that regulates such Transfer in accordance with the LFPDPPP, in which the Third Party assumes compliance with the obligations that correspond to the Responsible Party and the responsibilities of the parties in terms of Personal Data Protection are specifically delimited. In case the treatment warrants it, a corresponding contract must be made.

j) Transfers may only be made to Third Parties that comply with the protection standards established by the LFPDPPP. In this regard, the corresponding contract must include the text of the data protection and confidentiality clauses that have been approved by the Responsible Party and the Third Party must declare that it complies with the provisions of the LFPDPPP.

k) The contract for the transfer of Personal Data to a Third Party must include the following minimum elements of Personal Data protection:

- Use and process Personal Data for the sole and exclusive purpose of complying with the purposes set forth in the Privacy Notice and for which the Owner gave his consent;
- The commitment to refrain from altering, using the Personal Data for its own interest or communicating it or allowing third parties to access it, as well as using it for purposes other than those for which it is transferred;
- The security measures that the parties must observe during the transfer of Personal Data;

- To keep the Personal Data confidential;
- To compensate the injured party for all those expenses, damages and losses caused by the breach of any of the obligations provided for in the contract as a result of a possible breach of the contract, as well as the lawsuits that may be promoted by the owners of the Personal Data;
- The prohibition of using Personal Data for personal purposes;
- The prohibition of making any type of Transfers or referrals to Third Parties;
- The exchanges of Databases owned by the Responsible Party and the manner in which they are made available to Third Parties;
- The obligation to abide by all policies, guidelines, manuals and procedures that the Data Controller determines in terms of data protection.

6.9. Referrals

a) The exchange of Personal Data that the Responsible Party makes to Third Parties that have the character of Processors are considered Referrals for the purposes of the Law and do not require to be informed in the Privacy Notice or consented to by the Owners.

b) The Responsible Party must make available and obtain a signature of knowledge from the Processor the corresponding Privacy Notice for the processing of Personal Data. In any case, the actions of the Processor in relation to the processing of Personal Data must be in accordance with the Privacy Notice that has been consented to by the Owners and with the provisions of this Policy.

c) Any Submission of Personal Data repositories made by any area in the exercise of its powers will be notified to the Personal Data Department for analysis and approval.

d) Referrals may only be made to Third Parties with the security standards established by the Responsible Party in the Personal Data Security Management System.

e) Any Submission of Personal Data to Third Parties must be documented, detailing the terms, purposes, treatment and responsible persons who receive the Personal Data. Such Submission will be documented by the area responsible for carrying out and with the authorization of the Personal Data Department.

f) The Responsible Party must make available to the processor the corresponding Privacy Notice for the processing of Personal Data.

g) Submissions to Processors must be covered by a legal instrument or contract, which shall contain the following minimum elements for the protection of Personal Data:

- Purposes of the referral;

- Consent to process Personal Data in accordance with the instructions of the Responsible Party;
- To keep the Personal Data confidential;
- Inform the Responsible Party if any Personal Data breach occurs;
- Notify in case a subcontracting is required for the approval of the processing of the Personal Data for which they were sent;
- Delete or return the Personal Data subject to processing once the legal relationship has ended;
- The terms for blocking and deleting Personal Data;
- The delivery of evidence of the deletion of Personal Data;
- Restrict employees, agents and collaborators from accessing and using Personal Data to those that are absolutely essential for the development of the object of the legal instrument;
- The obligation of the Processor to establish in the contracts with its employees and service providers, clauses regarding the protection of Personal Data and confidentiality in accordance with the policies of the Responsible Party on the matter;
- The obligation of the Processor to respond to the damages caused to the Controller and/or the Data Controllers derived from their negligence or breach of the Responsible Party's data protection policies;
- The obligation of the Processor to reimburse the Controller for all amounts that the latter has to pay as a result of the proceedings and/or lawsuits filed against it due to the violation of the rights of the Data Controllers in terms of personal data protection;
- The delimitation of the Processor's actions as Responsible Party with respect to the Personal Data that it collects and processes for its own purposes.
- The obligation of the Processor to carry out, or allow the Controller to carry out compliance audits with the obligations regarding the protection of Personal Data.

6.10. Security of Personal Data

a) The Personal Data Department, in accordance with the Personal Data Security Management System, will be in charge of carrying out the following activities:

- Preparation of a Catalogue of Personal Data Systems, including the processing systems involved and the types of Personal Data they contain. For more information, please consult the Personal Data Security Management System of the Responsible Party.
- Annually, carry out an analysis of the security measures applicable to the processing of the data, considering the following factors:

1. Inherent Risk in the type of personal data.
2. Sensitivity of the Personal Data processed.
3. Technological development.
4. Consequences of a violation for holders.

- Perform a breach analysis to determine the security measures necessary for the protection of personal data. Review and update annually the security measures applicable to Personal Data in accordance with the provisions of the Information Technology Policies and Narratives and the Personal Data Security Management System Document or in the event of any event such as:

    1. Continuous improvement of security measures or processes.
    2. Change in the level of risk of data processing.
    3. There is a violation of the treatment systems.

- Immediately attend to notifications of information breaches and establish a reaction protocol for these cases.

b) The Personal Data Department will be responsible for risk analysis, as well as for managing vulnerabilities and risks related to the processing of Personal Data. Likewise, the procedures and policies to be followed for the analysis of vulnerabilities of the systems that process Personal Data will be followed as described in the Personal Data Security Management System.

c) A breach of the security of Personal Data is considered as the unauthorized acquisition of data or any action that compromises the security, confidentiality and integrity of said Personal Data on any physical or electronic medium in which it is found during any phase of processing.

d) According to Article 64 of the LFPDPPP Regulations, a Personal Data security breach is considered to be those that occur at any stage of its processing and are:

- Unauthorized loss or destruction;
- Theft, loss or unauthorized copying;
- Unauthorized use, access, or processing; or
- Damage, alteration or unauthorized modification.

e) If at any time a loss of Personal Data or a breach of the security with which Personal Data is protected is detected, the Responsible Party, at the time

of becoming aware of the situation, will decide the specific actions to be followed, which will be aimed at minimizing the risk and correcting the deficiency detected.

Any damage or loss in the provision of the service, the Responsible Party proceeds to draw up a report before the corresponding Public Prosecutor's Office so that an investigation folder number is assigned and the necessary required data is indicated.

f) In the event of any vulnerability, the Controller must notify the Owner within the period of time established by the Controller in its incident management processes. The response time to address a vulnerability will be immediate and immediate corrective measures will be carried out to mitigate the vulnerability to the system, during the period that the appropriate solutions are implemented to mitigate or eliminate said vulnerability. In the event that the vulnerability scanner is a Third Party, it is the contractual obligation of the service provider to comply with the provisions of this policy.

7. SANCTIONS

Traxión's collaborators who fail to comply herewith will be subject to disciplinary measures as determined by Traxion and/or business unit management; which, depending on the severity, may be as follows:

1. Warning call.
2. Issuance of administrative record.
3. Suspension from work without pay.
4. Termination of employment agreement.
5. Criminal complaint or appropriate legal action.

8. LIABILITY / TITLE

The Legal Department of Grupo Traxión, S.A.B. de C.V., is the assigned owner of this Policy and is primarily responsible for its content, updating and submission for approval to the Corporate Management of the Comptroller's Office.

This policy is illustrative but not limited to, so it is the responsibility of officers, employees, business partners to contact the Compliance Office (oficina.cumplimiento@traxion.global) to incorporate specific guidelines not included in this document.