COMPLIANCE

Personal Data Management Directive Procedure

Objective

Guarantee the correct implementation, development, maintenance, continuous improvement and follow up of the Organization's Personal Data Management System, by strengthening the mechanisms and good practices for personal data protection and processing, therefore thoroughly complying with the principles, duties and obligations established in the Federal Law for Personal Data Protection Controlled by Individuals (LFPDPPP), its Regulation and other applicable laws; as well as communicating the directive Procedure to all personnel participating as data controllers.

Scope

All of Industrias Peñoles S.A.B. de C.V. and subsidiary companies' personnel.

Input	Output
• Personal Data subjects • Personal Data Incidents	• Adequate personal data management

Operational Norms

Integral Aspects

This is a general compliance directive procedure for all personnel and especially for those processing personal data. This procedure is communicated to all the personnel in the Organization through the most effective institutional channels for the purpose.

The Manager oversees the administration, safekeeping and protection of the personnel's, contractors', suppliers' and visitors' personal data. He/she also acts as contact with the regulatory authority, and his/her functions include fulfillment of the following duties:

I. Address the requests to exert the right of access, correction, cancelation and opposition, as well as reception of complaints of the personal data subjects.

II. Coordination of actions and collaboration with other areas of the Organization, like legal, technology, information security, human resources, environment, safety and health, contractors, among others; in order to ensure de proper fulfillment of this procedure and privacy practices of their internal processes, formats, notices, resources and arrangements made.

III. Comply with the normativity related to personal data management established by the Organization.

IV. Provide the necessary information for evaluation and compliance with the established normativity.

V. Coordinate and monitor the compliance relative to obtaining, use, conservation, cancelation, transference and destruction of personal data, in order to ensure that the information is protected and treated according to the internal normativity principles and the pertaining law.

Personal Data Processing

Regarding personal data process:

- It is subject to the consent of its holder, who will be able to request its termination at any moment. In case of termination, the Data Controller has to follow the mechanisms and procedures published in the Privacy Notice.
- Considers different purposes for the use of data that, in no limited manner are of Human Resources, supplies and materials trading, occupational health, industrial safety, physical safety and relationships with third parties, according to the processes of the Data Controller.
- Adequate and relevant data is necessary according to the purposes of the Privacy Notice. If the data were intended for a different use or to be transferred, a new consent from its subject will be required.

The Data Controller must:

- Guarantee the resources to establish and maintain the administrative, technical and physical safety

measures that allow the personal data protection from damage, loss, changes, destruction or non-authorized access or use.

- Maintain confidentiality regarding the personal data with other Data Processors who also handle the information in any other phase.

Actions to comply with the principles, duties and obligations established in the LFPDPPP

For the fulfillment of the LFPDPPP, its Regulation and other applicable legal provisions, the Organization:

a) Has a Personal Data Management System (SGDP) that includes the detailed elements and activities for the process directivity, operation and control which allow continuous and systematic protection of personal data under its possession.

b) Even when making a textual reference to the law, the Organization has a member of the directive team, represented by the Compliance President in order to plan, implement and develop the SGDP. Other responsibilities include:

I. Coordinate and develop the SGDP and the personal data management directive Procedures.

II. Perform the necessary action to ensure the implementation, compliance and improvement of the SGDP and directive procedure.

c) It has a Personal Data Protection Committee; whose function is to guarantee the commitment and compliance of the Organization to the directive Procedure and the SGDP. The conformation of the committee is outlined in Annex 1. The structure and responsibilities of the people that conform the Committee are:

Committee's Personal Data Protection Obligations:

I. Participate in the development of the SGDP and directive procedure to be approved by the directive team,

II. Monitor implementation and compliance of the SGDP and directive procedure on a daily basis with the Data Controller,

III. Perform administrative reviews and audits of the SGDP and directive procedures in order for them to reflect practical and technologic regulatory updates,

IV. Being in charge of the definition and implementation of the program to promote and protect personal data internally with the Data Controller or Data Processor, including training and sensitization of the SGDP and directive procedure,

V. Coordinate the regulatory compliance, risk management and safety aspects internally with the Data Controller or Data Processor,

VI. Deliver technical counseling regarding personal data protection and performance of projects related to the Data Controller or Data Processor,

VII. Perform and manage required notifications to the Institute and other authorities, according to the Law, its Regulation and other applicable normativity, including the ones related to the existence, modification and termination of the self-regulatory guidelines,

VIII. Perform and manage the required communication with the interested parties regarding the SGDP, the directive procedure and framework, including relevant modifications,

IX. Address the requirements made by the National Institute of Transparency, access to the Personal Data Protection and Information, and the competent sectoral authorities; and

X. Consider the regulation and good existing sectoral practices in this matter for the SGCP.

d) Implement in each Company of the Organization, the adequate measures and mechanisms to guarantee the fulfillment of the following principles for personal data protection:

- ***Legality***
  - Personal data must be collected and treated legally and accordingly to the applicable laws, dispositions and normativity.
  - Only personal data information given to the companies of the Organization can be used, according to the agreement with the subject in the Privacy Notice and other applicable

legal instances.

- ***Consent***
  - Broadcasting the privacy notice is mandatory, as well as providing the information that is being collected to the subject. This notice must be available to the subject of the personal data, through the formats established by the Personal Data Protection Committee.
  - The privacy notice consent can be expressed or tacit, based on the legal disposition applicable in the data protection subject and the guidelines that outline this directive procedure.
- ***Information***
  - Essential features of the personal data processing must be informed to the subject who is giving such information to the companies of the Organization through the Privacy Notice.
- ***Quality***
  - The companies of the Organization have to verify that the information regarding the personal data, is precise, complete, relevant, correct and up to date, in order for the truth not be altered, nor that the subject be affected because of such situation.
  - The period for the use of the information is strictly the necessary one (established in the procedures Manual for the LFPDPPP compliance). Once this period is over, the data should be blocked in order to determine possible responsibilities regarding its process, until the legal or contractual prescription period ends, in order to proceed to cancel.
  - In case that the data is no longer required for the intended purpose for which it was collected, the information must be eliminated from the data bases and from the Group's systems, leaving also proof of such procedure.
- ***Purpose***
  - The personal data collected by the companies of the Organization can only be used to fulfil the purpose or purposes specifically defined in the Privacy Notice.
- ***Loyalty***
  - At all moments the protection of the subject's interests and the reasonable expectation of privacy must be privileged.
- ***Proportionality***
  - Only necessary personal data that is adequate and relevant for the functions, purposes and process intended is collected, and in all cases must be justified.
  - The confidentiality clause and personal data caution approved by the Personal Data Protection Committee must be included in the contracts and agreements.
- ***Responsibility***
  - The companies of the organization must safeguard and account for the treatment of the personal data under their custody or care, or for the personal data communicated to a Data Processor. In this sense, the fulfillment of this directive procedure, as well as the laws and internal rules with which it's interrelated, becomes relevant for the Organization's integral compliance.

SGDP Development, Implementation, maintenance and improvement

The Data Controller has a Personal Data Management System, and its planning, implementation, and development is in the hands of the head of the Compliance Presidency. This System is focused on establishing, implementing, operating, monitoring, reviewing, maintaining and improving the personal data protection according to the risk of the assets and principles, duties and obligations foreseen in the laws and regulations applicable, as well as good practices relevant to the personal data protection.

The SGDP has the necessary personnel, mechanisms and elements to:

- Define the necessary directives, objectives, plans, processes and procedures to obtain the expected result of the Personal Data Protection Committee.
- Implement and operate the directives, objectives, plans, processes and procedures established in the previous phase.
- Measure and evaluate the implemented results in order to verify the adequate function of the SGDP and the achievement of the improvement expected based on the administrative review.
- Take preventive and corrective measures based on the results of the review, or otherwise on other relevant information in order to obtain continuous improvement.

Good practices adoption

The Data Controller monitors compliance with the LFPDPPP, its regulation and other applicable dispositions, as well as always looking to implement best practices regarding personal data protection according to the national and international experience and the sector's characteristics.

Compliance systemic approach

This directive approach is inter-related regarding compliance included but not limited to:

- Federal Law for Personal Data Protection Controlled by Individuals.
- Federal Regulation for Personal Data Controlled by Individuals.
- Self-regulation parameters Regarding Personal Data Protection.
- Privacy Notice guidelines.
- Guidelines to implement compensatory measures – INAI.
- Applicable internal normativity, especially with:
  - Directive procedure for safety information.
  - Management procedures for IT's safety incidents.
  - Procedure to classify information.
- Procedures manual to comply with the Federal Law for Personal Data Protection Controlled by Individuals:
  - Personal data administrative procedure.
  - Procedure to address applications for ARCO rights.
  - Procedure to address personal data safety incidents.
  - Internal audit procedure for personal data.
  - Procedure for sensitive personal data treatment.
  - Procedure for personal data referral and transference.
  - Procedure for personal data administrative procedures.
  - Procedure for personal data destruction.
- Training program for all personnel, especially those who process personal data.

Definitions

Asset: Information, knowledge about the processes, personnel, hardware, software and any other resource involved in the process of personal data that has value for the organization.

Manager: Human Resources area leader in the Data Controller company.

Privacy Notice: Physical, electronic or a document in any other format generated by the Data Controller company that is made available to the subject, previous to the process of his personal data.

Personal Data Protection Committee: Entity that has the function to guarantee the commitment and compliance of the Organization with the Directive Procedure and Personal Data Management System.

Consent:	Declaration of the personal data subject's willingness through which the process of the personal data is carried out.
Personal Data:	Any information regarding an identified or identifiable individual person.
Sensitive Personal Data:	Personal data that affect the most intimate sphere of the subject, or which misuse can originate discrimination or could involve a grave risk for the subject. Particularly, sensitive data is the one considered to reveal aspects like racial or ethnic origin, present and future health incidents, religious, philosophical and moral believes, union affiliation, political opinions, sexual preferences.
ARCO rights:	The rights to access, rectify, cancel and oppose.
LFPDPPP:	Federal Law for Personal Data Protection Controlled by Individuals.
Data Processor:	A natural or legal person external to the data controller of the organization, who alone or in conjunction with others, processes personal data on behalf of the data controller.
Regulation:	Federal Regulation for Personal Data Protection Controlled by Individuals
Referral:	Personal data communication between the data controller and the data processor, inside or outside Mexican territory.
Data Controller:	Natural or juridical person who decides about the personal data process.
SGDP:	Personal Data Management System.
Subject:	Natural person's personal data.
Transference:	All data communication made to other people different to the data controller or data processor for its process.
Process:	Personal data collection, use, disclosure or storage through any means. Personal data use includes any action to access, utilize, transference or provisions.

	Procedures Flow	Formats
Annexes	• N/A	• Annex 1 – Personal Data Protection Committee Certificate. • Annex 2 – Fundamental rules for Personal Data Management Directive Procedure.

Information to update document

Issuance date	Next revision	Version
June 2020	June 2023	0