Perez

Privacy and Personal Information Confidentiality Policy – September 2023

Introduction

This policy deals with the management and protection of confidential information within Perez inc. In particular, it processes information related to the company's activities, customers, suppliers and employees.

It defines the principles and practices that guide the collection, use and management of data and includes technical and behavioral standards and guidelines for quality, integrity, security, confidentiality, compliance, retention and data archiving, regardless of the location or format of the data.

This policy applies to personal information found on documents of all formats (paper, digital or audiovisual), whether recorded files, working documents, electronic documents, emails, online transactions, data stored in databases or on tape or disk, maps, plans, photographs, sound and video recordings.

Goals

The policy pursues the following objectives:

- Ensure respect for the privacy of individuals and the security of personal information held by Perez;
- Give guidelines regarding the exchange of information.

Definitions

- Privacy incident

  Any access not authorized by law to personal information, its use or its communication, as well as its loss or any other form of attack on its protection.

- Serious risk of prejudice

  The risk assessed following a confidentiality incident which could harm the people concerned. This risk is analyzed by the person responsible for personal information. For any confidentiality incident, the responsible person assesses the seriousness of the risk of prejudice to the persons concerned by estimating "the sensitivity of the information concerned", "the anticipated consequences of its use" and "the probability that it will be used for purposes harmful".

- Confidential information

  Any information provided or communicated to Perez in any medium whatsoever (verbal, written, audio, video, computerized or other) which concerns a person and which can be used to identify them, including: their name, their telephone number , their address, email, gender, sexual orientation and any information concerning their health.

  For greater certainty:

  - Information that does not allow an individual to be identified in the context of a testimony is not confidential information;
  - Statistical data is not confidential information since it does not allow an individual to be identified;
  - Photographs or recordings that do not allow an individual to be identified do not constitute confidential information relating to that individual. Photographs or recordings that identify an individual as an employee do not constitute confidential information relating to that individual.

Roles and responsibilities

Executive Committee

- Approves this policy and its modifications, if applicable;
- Designates a governance committee responsible for the application of this policy.

Management Committee

- Examines and recommends this policy and its modifications, if necessary, to the executive committee;
- Designates the person who will act as Personal Information Protection Officer;
- Approves the directives related to the policy on the protection of personal information.

Responsible for the protection of personal information

- Acts as the person responsible for this policy;
- Manages the application of this policy and the resulting directives;
- Acts as responsible for the management of any incident related to the protection of personal information in accordance with applicable laws;
- Reports periodically to the Managment Committee on the management of this policy;
- Acts as respondent for any questions relating to the protection of personal information.

Management of confidential information

Management is the person responsible for ensuring the protection of personal information. Management may delegate this responsibility by stating it in writing. On the Perez website must be indicated, under the title of the management or person responsible, “person responsible for the protection of personal information” as well as the means of contacting them. The management or person responsible ensures that a Confidentiality Incident Register is kept.

Guidelines

- Obligation of confidentiality
  Perez employees are required to sign this confidentiality agreement (Appendix A) before carrying out their duties. The obligation of confidentiality applies for the duration of the employee's relationship with Perez and survives the end of this relationship.

- Collection and use of confidential information
  Perez may, if necessary, create one or more files containing confidential information concerning employees. The purpose of creating such files is to:
  - o Keep contact details up to date;
  - o Document work related situations;
  - o Allow the carrying out of administrative tasks required or permitted by law (income tax, group insurance, etc.).

- Perez may, if necessary, create one or more files containing confidential information concerning customers, suppliers and partners. The purpose of creating such files is to:
  - Keep contact details up to date;
  - Document relationships and events.
  - Confidential information can only be collected from the person concerned, unless the person concerned consents to the collection being made from others or the law authorizes it.

- Retention of personal data

  Perez employees must ensure that all electronic documents containing confidential information, including those copied to a portable storage device, are encrypted and protected by passwords. These passwords must be changed once a year, as well as each time the people with access to the files concerned are replaced.

  Perez employees must keep confidential information in paper format in lockable filing cabinets and ensure that the filing cabinets are locked at the end of each work day. Keys to filing cabinets must be kept in secure locations.

- Disclosure of confidential information to a third party

  Other than in situations where the law requires it, or if the life, health or safety of the person concerned is seriously threatened, confidential information may only be disclosed to a third party after obtaining written, explicit consent, free and informed by the person concerned. Such consent can only be given for a specific purpose and for the duration necessary to achieve the latter.

- Data retention

  Data is retained in accordance with the schedule provided below or for as long as necessary to fulfill the purposes for which it was collected and to comply with the organization's legal obligations. The retention period is calculated from the date of the last update.

Retention schedule	
Data type	**Retention period**
Accounting documents	7 years
Contracts and leases	7 years
Data on customers and suppliers	Permanent
Employee data	Permanent

- Destruction of confidential information

  At the latest upon expiry of the retention period, the confidential information is destroyed so that the data contained therein can no longer be reconstructed.

- Communication of confidential information

  Any person has the right to know the confidential information that Perez has received, collected and keeps about them, to have access to such information and to request that rectifications be made to it.

- Privacy incident

  o When a Perez employee notices a confidentiality incident, he or she communicates with management or the person responsible for ensuring the protection of personal information.

  o Management or responsible person identifies reasonable measures to reduce the risk of harm and to prevent further incidents.

- Management or the responsible person assesses whether the incident presents a risk of serious harm.

  - In the event that the incident presents a risk of serious harm, Management or the person responsible immediately notifies the Commission for Access to Information (CAI) via the form provided for this purpose and any person whose information personnel are affected.
  - Management or the responsible person keeps a record of all incidents.

- The management or responsible person responds to the CAI's request for a copy of the register, if applicable.

- Breach of the obligation of confidentiality

  An employee breaches his or her duty of confidentiality when he or she:
  - Communicates confidential information to individuals who are not authorized to have access to it;
  - Discusses confidential information when individuals who are not authorized to have access to it are likely to hear it;
  - Leaves confidential information on paper or computer media in plain sight in a place where individuals not authorized to have access to it are likely to see it;
  - Fails to follow the provisions of this policy.

  In the event of a breach of the obligation of confidentiality, appropriate disciplinary measures, which may go as far as termination of the employment contract, will be taken with regard to the offending. party and corrective measures will be adopted if necessary, in order to prevent a such a scenario does not happen again.

- Possibility of filing a complaint regarding non-compliance with the principles

  A person may file a complaint in the event of non-compliance with the principles relating to the protection of personal information by contacting the person responsible for the protection of personal information indicated on the Perez website under the Contact Us section or by contacting management if the complaint concerns the person responsible for the protection of personal information.

  The person responsible of the protection of privacy is :

  Nadia Talbot
  Controller
  ntalbot@bouty.com

  As provided by law, the person having been refused access or rectification of confidential information concerning him or her may file a complaint with the Commission for Access to Information for the examination of the disagreement within thirty (30) days of Perez's refusal to grant his request or of the expiry of the time limit for responding to it.