PRIVACY POLICY – FRIOPACKING

FRIOPACKING SAC , identified with RUC No. 20494691524, with address at Carretera Panamericana Sur, Km 298, district of Subtanjalla, province and department of Ica, is responsible for the processing of personal data collected through its website http://www.friopacking.pe and other digital or physical channels.

This Privacy Policy details how the personal data of users, customers, suppliers, and applicants is collected, used, stored, and protected, in compliance with Law No. 29733 – the Personal Data Protection Law of Peru and considering international best practices (GDPR).

Use of the website implies acceptance of this Privacy Policy.

IDENTITY AND RESPONSIBILITY FOR PROCESSING:

HOLDER	**FRIOPACKING SAC**
TAX IDENTIFICATION	20494691524
TAX ADDRESS	Panamericana Sur Km 298, distrito de Subtanjalla, provincia y departamento de Ica.
BUSINESS ADDRESS	Av. 28 de Julio No. 753, Oficina 802, distrito de Miraflores, provincia y departamento de Lima.
PROXY	Alvaro Alejandro Chavez Girao
RESPONSIBLE AREA	Communication and Institutional Image
CONTACT	Pablo Flores Chavez
EMAIL	pflores@friopacking.pe
WEBSITE	http://www.friopacking.pe

ON THE PRINCIPLES APPLIED TO DATA PROCESSING:

- Legality, Loyalty and Transparency : For FRIOPACKING, it is essential to require its clients, suppliers, business partners, employees, and third parties directly or indirectly linked, among others, their consent for the processing of personal data for specific purposes.
- Data Minimization : We only require data when strictly necessary.
- Retention Period Limitation : We retain data only for as long as necessary.
- Integrity and Confidentiality : We adopt technical and organizational measures to guarantee the security of personal data.

ON THE COLLECTION OF PERSONAL DATA:

We collect personal data in the following cases:

- Contact forms or commercial inquiries.

- Hiring or application processes.
- Interaction with our website through cookies.

ON THE PURPOSE OF THE PROCESSING OF PERSONAL DATA:

- Commercial Management : Sending quotes, sales tracking, customer service, among other information and/or documentation for the fulfillment of the corresponding purposes.
- Contractual Relationship : Execution of contracts, invoicing, management of payment collections, among others related to this activity.
- Recruitment : Candidate evaluation, payroll management, among others.
- Statistical Analysis : Report preparation, market research, sector analysis, among others.

ON THE LEGITIMATION FOR DATA PROCESSING

- Consent : It is the manifestation of free, specific, informed and unequivocal will by which the data owner accepts that FRIOPACKING, process their personal data for one or several specific purposes.

  Example: i) A potential customer completes a contact form on the website to request information about the design and construction of refrigeration plants and ticks the box agreeing to receive commercial communications from FRIOPACKING. ii) A user subscribes to the FRIOPACKING newsletter and consents to receive company updates, industry news, and special offers. iii) An applicant for a job at FRIOPACKING consents to the processing of their personal data (including sensitive data, such as health data, if applicable) for the selection and evaluation process.
- Contract Execution : Refers to the processing of data necessary for the execution of a contract to which the data subject is directly or indirectly involved, for the implementation, at the latter's request, of pre-contractual measures.

  Example: i) A customer provides their personal data (name, address, contact details, financial information) to formalize a contract for the construction of an industrial refrigeration plant with FRIOPACKING. ii) FRIOPACKING processes a supplier's data (contact name, company details, bank details) to manage the contractual relationship, including making payments and monitoring services provided. iii) FRIOPACKING processes an employee's data (identification data, contact details, bank details, employment details) to manage their employment contract, including paying salaries, managing benefits, and fulfilling employment obligations.
- Compliance with Legal Obligations : This is the processing of data necessary for compliance with a legal obligation applicable to FRIOPACKING.
  Example: i) FRIOPACKING communicates its employees' data to the tax authorities for the purpose of fulfilling tax obligations (e.g., tax withholdings). ii) FRIOPACKING

provides information to judicial or administrative authorities within the framework of legal proceedings. iii) FRIOPACKING retains its customers' billing data for the period required by commercial and tax legislation.

- Legitimate Interest : Data processing is necessary for the satisfaction of legitimate interests pursued by FRIOPACKING or by a third party, provided that such interests are not overridden by the interests or fundamental rights and freedoms of the data subject.

  Example: 1) FRIOPACKING processes customer data to send them information about products or services similar to those they have already contracted, based on its legitimate interest in maintaining the business relationship (provided the customer has not objected to receiving such communications). ii) FRIOPACKING uses video surveillance systems in its facilities to guarantee the safety of its employees, assets and facilities, based on its legitimate interest in protecting its assets. iii) FRIOPACKING carries out statistical analyses of the browsing data of users of its website to improve its operation and optimize the user experience, based on its legitimate interest in improving its online business.

REGARDING DATA RETENTION:

The data will be retained as long as necessary for the purposes described or in accordance with legal deadlines:

1. STORAGE PERIOD:
   - Customer Data :
     - Information required for billing: Retain for the period required by tax legislation (generally, several years).
     - Contact and business data: Retained as long as the business relationship is active. If there is no activity (e.g., 4 years), it is anonymized or deleted, unless there is a legal obligation to retain it for a longer period.
     - Communications and inquiries: Retain for a reasonable period to address potential future claims or inquiries (e.g., 2-3 years)
   - Supplier Data:
     - Data required for contract and payment management: Retained for the duration of the contract and the time necessary to comply with legal obligations (e.g., statutes of limitations).
     - Contact information: Keep updated while the business relationship is maintained .
   - Employee Data:
     - Employment contracts and documentation: Retain as required by labor and social security laws (time limits vary depending on the type of document).
     - Payroll data: Retain for the period required by tax and labor legislation.

- Resumes of unsuccessful candidates: Retain for a limited period (e.g., 6 months or 1 year) with the candidate's consent for possible future opportunities.

- Website user data:
  - Browsing data (cookies): The retention period will depend on the type of cookie (session, persistent, etc.), as specified in the Cookie Policy.
  - Contact form data: Retained for the time necessary to respond to the inquiry and, if consent is obtained for commercial communications, until the user withdraws their consent.

2. CRITERIA FOR DETERMINING CONSERVATION:
   - Legal Obligations :
     - Compliance with tax, labor, commercial, and other laws that establish specific retention periods.
     - Limitation periods for legal actions (e.g., for contractual claims).
     - Requirements for the preservation of accounting and financial documents.
   - Operational Needs of FRIOPACKING :
     - Time needed to manage relationships with customers and suppliers.
     - Need to keep records for defense in case of claims.
     - Use of data for statistical analysis and service improvement (provided they are anonymized where possible).
   - Rights of Data Subjects:
     - Balancing data retention periods with the right to data deletion (right to be forgotten).
     - Inform data subjects about the criteria used to determine retention periods.
   - Safety Considerations:
     - Minimize data retention time to reduce the risk of security incidents.
     - Implement appropriate security measures throughout the retention period.
3. ELIMINATION AND/OR ANONYMIZATION PROCESS:
   - Elimination:
     - Technical procedure for the secure elimination of data (e.g., secure deletion, physical destruction of media).
     - Ensuring that the removal is complete and irreversible.
     - Document the disposal process to demonstrate compliance.
     - Establish a schedule or system for the periodic deletion of data that has reached its retention period
   - Anonymization :
     - Definition of anonymization techniques that will be used in the process for dissociation, generalization and/or suppression).
     - Ensure that anonymization is effective and that the anonymized data no longer allows the data subject to be identified.

- Specify which data can be anonymized and in which cases anonymization is preferred to deletion (e.g., for statistical analysis)

REGARDING THE RIGHTS OF PERSONAL DATA OWNERS:

This section describes in detail the rights that individuals (data subjects) have over their personal information that FRIOPACKING collects and processes. These rights allow individuals to have control over their data, including the ability to access it, correct it if it is inaccurate, delete it in certain circumstances, object to its use for certain purposes, restrict its processing, and, in some cases, request the transfer of their data to another service provider.

The purpose of this section is to inform data subjects about how they can exercise these rights and how FRIOPACKING is committed to responding to their requests in accordance with current legislation. Furthermore, if a data subject believes that the processing of their personal data violates current regulations, they have the right to file a complaint with the National Data Protection Authority (ANPDP), the competent body in Peru for the protection of personal data and the supervision of compliance with Law No. 29733.

1. RIGHT OF ACCESS:
   - Definition : The right of access allows the data subject to obtain confirmation as to whether FRIOPACKING is processing personal data concerning him or her and, where that is the case, to obtain a copy of such data and certain information regarding its processing.
   - Considerations for FRIOPACKING :
     - Inform about the categories of data processed (e.g. identification data, contact data, financial data).
     - Detail the purposes of the treatment.
     - Indicate the recipients or categories of recipients to whom the data is or will be communicated.
     - Specify the expected data retention period or, if not possible, the criteria used to determine this period.
     - Inform about the existence of the right to request rectification, deletion or limitation of processing, and to object to processing.
     - Detail the right to file a complaint with the supervisory authority (the National Data Protection Authority in Peru).
     - Indicate, where applicable, the existence of automated decisions, including profiling, and the logic involved, as well as the significance and expected consequences of such processing.
     - Provide a copy of the personal data being processed.
   - Procedure :

- Establish a clear and simple procedure for data subjects to exercise their right of access (e.g., through a request form, by email, etc.).
- Set a reasonable response time (the legal deadline in Peru is 20 business days).
- Provide the information in a format clear and easily understandable.

2. RIGHT OF RECTIFICATION:
   - Definition : The right to rectification allows the data subject to obtain the rectification of inaccurate personal data concerning him or her or to have incomplete personal data completed.
   - Considerations for FRIOPACKING:
     - Inform about the right to rectify inaccurate data.
     - Establish a procedure for data subjects to communicate the data they wish to rectify and provide the necessary supporting documentation.
     - Make the rectification without undue delay.
     - Communicate the rectification **to** each of the recipients to whom the personal data has been communicated, unless it is impossible or requires a disproportionate effort.
   - Procedure:
     - Define a communication channel for rectification requests.
     - Establish a response period for rectification.
     - Implement internal mechanisms to verify the accuracy of the corrected data.

3. RIGHT TO DELETION (Right to be forgotten):
   - Definition : The right to erasure (or right to be forgotten) allows the data subject to obtain the deletion of personal data concerning him or her in certain circumstances.
   - Considerations for FRIOPACKING:
     - Inform about the cases in which deletion is appropriate:
       - The personal data are no longer necessary in relation to the purposes for which they were collected or processed.
       - The data subject withdraws the consent on which the processing is based and this is not based on another legal basis.
       - The data subject objects to the processing and no other legitimate grounds for processing prevail.
       - Personal data has been unlawfully processed.
       - Personal data must be deleted to comply with a legal obligation.
     - Inform about exceptions to the right to erasure (e.g., when processing is necessary for compliance with a legal obligation, for the exercise of the right to freedom of expression and information, etc.).
     - Take reasonable steps to inform the controllers processing the personal data of the deletion request.
   - Procedure:
     - Establish a procedure for data subjects to request the deletion of their data.

- Evaluate whether deletion is appropriate based on the applicable assumptions and exceptions.
- Perform deletion safely and completely.
- Inform the owner of the decision taken.

4. RIGHT OF OPPOSITION:
   - Definition : The right to object allows the data subject to object to the processing of personal data concerning him or her in certain circumstances .
   - Considerations for FRIOPACKING:
     - Inform about the right to object to processing based on the legitimate interest of FRIOPACKING or a third party.
     - Inform you about your right to object to processing for direct marketing purposes, including profiling related to such marketing.
     - Respond to the data subject's objection, unless FRIOPACKING demonstrates compelling legitimate grounds for processing that prevail over the data subject's interests, rights, and freedoms, or for the formulation, exercise, or defense of legal claims.
   - Procedure:
     - Establish a procedure for owners to exercise their right to object.
     - Evaluate the reasons given by the data subject to oppose the processing.
     - Inform the data subject about the decision taken and, where appropriate, about the compelling legitimate reasons that justify the processing .

5. RIGHT TO LIMIT PROCESSING:
   - Definition : The right to restriction of processing allows the data subject to obtain restriction on the processing of personal data concerning him or her in certain cases, in which case FRIOPACKING may only process the data for certain purposes.
   - Considerations for FRIOPACKING:
     - Inform about the cases in which the limitation of treatment is appropriate:
       - The owner challenges the accuracy of the personal data, for a period that allows FRIOPACKING to verify the accuracy of the same.
       - The processing is unlawful and the data subject opposes the erasure of the personal data and requests that their use be restricted instead.
       - FRIOPACKING no longer needs the personal data for the purposes of processing, but the data subject requires them for the formulation, exercise, or defense of legal claims.
       - The data subject has objected to the processing, while it is being verified whether FRIOPACKING's legitimate grounds prevail over those of the data subject.
     - Inform FRIOPACKING of its obligation to communicate the processing restriction to each of the recipients to whom the personal data has been communicated, unless this is impossible or requires a disproportionate effort.

- Procedure :
  - Establish a procedure for data subjects to request restriction of processing.
  - Check whether any of the assumptions that justify the limitation are met.
  - Limit data processing to permitted purposes.
  - Inform the owner of the decision taken.

6. RIGHT TO DATA PORTABILITY:
   - Definition : The right to data portability allows the data subject to receive the personal data concerning him or her, which he or she has provided to FRIOPACKING, in a structured, commonly used and machine-readable format, and to transmit them to another data controller without hindrance from FRIOPACKING, when the processing is based on consent or a contract and is carried out by automated means.
   - Considerations for FRIOPACKING:
     - Inform about the right to data portability and the conditions for exercising it.
     - Provide personal data in a structured, commonly used, machine-readable format (e.g., CSV, JSON).
     - Facilitate the direct transmission of data to another data controller, when technically possible.
     - Inform about the right to have personal data transmitted directly from FRIOPACKING to another data controller, provided that this is technically feasible.
   - Procedure:
     - Establish a procedure for data subjects to request portability of their data.
     - Verify whether the processing is based on consent or a contract and whether it is carried out by automated means.
     - Provide data in the appropriate format and facilitate transmission, where appropriate.
     - Inform the owner about the decision taken

REGARDING THE RECIPIENTS OF PERSONAL DATA:

This section of the Privacy Policy informs data subjects about who may receive or access their personal data. This includes both internal entities within FRIOPACKING and external organizations or individuals. It details the identity of these recipients and the reasons for sharing the data, the specific types of data, the security measures implemented to protect the data during transfer (especially in the case of international transfers), and the responsibilities of these recipients regarding the protection of personal data. This includes a) Technology services such as web hosting providers, email service providers, cloud storage providers, customer relationship management (CRM) software providers, human resource management (HRM) software providers, web analytics service providers, digital

marketing service providers, among others; and b) Competent authorities with whom personal data information is shared (e.g., judicial, administrative, regulatory authorities) when there is a legal obligation to do so or within the framework of a legal procedure.

All of the above is developed under the obligations of confidentiality and security, with FRIOPACKING ensuring that the recipients of the personal data will undertake to: i) process the personal data in accordance with the established purposes, ii) maintain the confidentiality of the personal data and iii) implement appropriate security measures to protect the personal data.

REGARDING THE SECURITY OF PERSONAL DATA:

This section describes the measures FRIOPACKING has in place to protect personal data against unauthorized access, loss, alteration, destruction, or any other form of unlawful processing. It also details both technical measures (such as encryption and firewalls) and organizational measures (such as security policies and staff training), covering physical, logical, and administrative security aspects. It also explains the procedures established for managing and responding to security incidents, ensuring the confidentiality, integrity, and availability of information.

1. PHYSICAL SECURITY MEASURES:

- Physical access control to our facilities :
  - Access to our offices is controlled by access cards and biometric identification systems.
  - The data centers are equipped with 24-hour surveillance systems and security personnel.
  - FRIOPACKING offers: Access controls (cards, codes, biometrics, keys), Entry and exit records, Surveillance (cameras, security personnel), Protection against natural disasters (fires, floods, earthquakes).

  It should be noted that FRIOPACKING, as part of its physical security, has implemented video surveillance systems in its facilities to guarantee the safety of its employees, visitors, assets, and infrastructure, based on its legitimate interest. This data processing is carried out in compliance with the Personal Data Protection Directive for Video Surveillance Systems (Resolution 019-2020-JUS/DGPDP), which establishes the principles of purpose, proportionality, quality, and security in the use of captured images. Recordings are kept for a maximum period of 30 calendar days (unless they must be kept longer due to an internal or legal procedure) and are protected by appropriate technical and organizational measures. Data subjects may exercise their rights regarding the captured images, in accordance with the provisions of this policy.
- Security of information media :
  - Company laptops and mobile devices are protected with passwords and disk encryption.

- Physical files are stored in locked cabinets and in rooms with restricted access.
- Encryption of devices and storage media.
- Procedures for the secure destruction of documents and devices.
- Control of the output of company devices.

2. LOGICAL SECURITY MEASURES:

- Computer system access control :
  - Access to our databases is restricted to authorized personnel and is achieved through unique credentials and secure passwords.
  - We implemented an Identity and Access Management (IAM) system to control user permissions .
  - User authentication (passwords, two-factor authentication).
  - User authorization (permission and privilege control).
  - Logging of user activity (access logs).
  - Strong password policies.
- Malware protection :
  - All company equipment has updated antivirus software.
  - We implement firewalls to protect our network from unauthorized access.
  - Antivirus and antimalware software.
  - Firewalls.
  - Intrusion detection and prevention systems (IDS/IPS).
  - Regular security updates
- Data encryption :
  - Data transmission over the Internet is carried out using secure protocols (HTTPS).
  - Sensitive data is encrypted both in transit and at rest.
  - Data encryption in transit (SSL/TLS).
  - Data encryption at rest (database encryption, file encryption).
- Backup and Recovery:
  - We perform daily backups of our databases and store them in secure locations.
  - We have a disaster recovery plan to ensure business continuity.
  - Frequency and type of backups.
  - Backup location (local, remote, cloud).
  - Data restoration procedures.
  - Periodic testing of recovery procedures

3. ADMINISTRATIVE SECURITY MEASURES

- Security Policies and Procedures :
  - We have an Information Security Policy that establishes the rules and responsibilities regarding data protection.

- We implement procedures for managing security incidents, accessing information, and destroying data.
- Privacy Policy.
- Procedures for accessing, using, storing and deleting data.
- Security incident management procedures.
- Password policy.

- Staff training and awareness:
  - All employees receive regular training on data protection.
  - We conduct awareness campaigns on security risks and best practices.
  - Security incident drills.
  - Awareness materials (leaflets, posters, etc.).
  - Evaluating the effectiveness of training.
- Responsibility and Roles :
  - Appointment of a Data Protection Officer (DPO) to oversee compliance with the regulations.
  - Each department is responsible for the security of the data it processes.
  - Definition of roles and responsibilities in the Security Policy.
  - Monitoring and control mechanisms
- Security audits :
  - We conduct periodic internal and external security audits to evaluate the effectiveness of our security measures.
  - Scope of audits.
  - Corrective actions arising from audits.

4. PROCEDURES FOR THE MANAGEMENT OF SECURITY INCIDENTS:

- Detection and notification :
  - We have a procedure for detecting and reporting security incidents that establishes the steps to follow in the event of a security breach.
  - Employees are required to immediately report any security incidents they detect.
  - Detection mechanisms (IDS, SIEM).
  - Notification channels (email, phone).
  - Notification deadlines.
  - Notification responsibilities.
- Evaluation and response :
  - An incident impact assessment is conducted and containment and recovery measures are implemented.
  - The competent authorities and affected parties are informed, where appropriate.
- Track record :
  - A record is maintained of all security incidents, including date, description, impact, and actions taken.

- Corrective actions implemented are monitored to prevent the recurrence of incidents.
- Root cause analysis.

In summary, this section aims to inform data subjects about FRIOPACKING's commitment to the security of their information and the specific actions taken to protect it.

REGARDING THE USE OF COOKIES:

Our website uses cookies. See the Cookie Policy at https://friopacking.pe/politica-de-cookies.

REGARDING CHANGES IN THE PRIVACY POLICY:

We reserve the right to modify this policy to adapt it to legislative or practical changes.