


CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA OF FERREYCORP S.A.A. AND ITS SUBSIDIARY COMPANIES			 FCO-GCAC-LEG-COD-001	
TÍTULO			CÓDIGO	
LEGAL			31/03/2025	31/03/2030
CATEGORY – PURPOSE OF THE DOCUMENT			INITIAL EFFECTIVE DATE	FINAL EFFECTIVE DATE
CORPORATE	CODE	Corporate Management of Corporate Affairs	1.0	23
CATEGORY	TYPE	ISSUER	VERSION	PAGES
LEVEL OF CONFIDENTIALITY: GREEN				

CODE OF CONDUCT FOR THE PROCESSING OF PERSONAL DATA OF FERREYCORP S.A.A. AND ITS SUBSIDIARY COMPANIES

ISSUED BY:

CORPORATE MANAGEMENT OF CORPORATE AFFAIRS - FERREYCORP S.A.A.

THIS DOCUMENT HAS BEEN AUTHORIZED IN THE REGULATORY SYSTEM BY:

Prepared by:	Reviewed by:	Approved by:
Rodolfo Gutierrez Diez Senior Legal Advisor, Ferreycorp S.A.A.	Eduardo Ramírez del Villar Corporate Manager of Corporate Affairs, Ferreycorp S.A.A.	Mariela Garcia De Fabbri General Manager, Ferreycorp S.A.A.

I.- OBJECTIVE

Ferreycorp S.A.A., its subsidiary companies, and its non-profit entity (Asociación Ferreycorp), hereinafter referred to as "the Corporation," recognize the importance of protecting the personal data of its employees, clients, suppliers, and other stakeholders with whom it interacts, and is committed to complying with the provisions of Law No. 29733 – Personal Data Protection Law and its Regulations, approved by Supreme Decree 016-2024-JUS, as well as other applicable regulations.

This Code of Conduct, hereinafter referred to as "the Code," aims to establish the principles and guidelines governing the processing of personal data within the Corporation, which are mandatory for Peruvian companies, in order to ensure the confidentiality, protection, integrity, and availability of the data, as well as the exercise of the rights of the data subjects.

The provisions of this Code shall apply to Ferreycorp subsidiaries operating in countries other than Peru, to the extent that they do not conflict with local laws and regulations, in which case they shall adopt this Code alongside local laws.

II.- SCOPE

The provisions contained in this Code must be complied with by all employees of the Corporation who create, collect, store, and/or process personal data of the various stakeholders as part of the activities, processes, and services provided, regardless of the medium in which the data is stored—be it physical, magnetic, digital, optical, or others.

The Code is primarily addressed to the General Managements, Human Resources departments and divisions, and employees of all the Corporation's subsidiaries in Peru in different management areas and divisions, who, by the nature of their duties, are responsible for managing personal data of any stakeholder or business partner, as well as to the Corporate Management of IT, Processes, and Information; the Corporate Management of Corporate Affairs; and the Corporate Management of Auditing.

The Personal Data Officer, the Corporate Management of Corporate Affairs, the Corporate Management of Auditing, and the Corporate Management of TPI, through its Information Security Deputy Management, are responsible for ensuring and/or reviewing compliance with these regulations.

III.- LEGAL AND REGULATORY REFERENCE

3.1.- Law No. 29733 – Personal Data Protection Law.

3.2.- Supreme Decree No. 016-2024-JUS – Regulations of Law No. 29733, Personal Data Protection Law.

3.3.- Security Standard for the Processing and Protection of Personal Data (FCO-GTPI-SGI-NOR-001).

3.4.- Procedure for Notification of Personal Data Security Incidents (FCO-GTPI-SGI-PRD-001).

IV.- DEFINITIONS

4.1.- Personal Data: Information associated with a natural person that identifies or makes them identifiable. Categories of Personal Data include: first and last names, national ID number, home address, telephone number, mobile phone number, email address, image, voice, signature, banking information, etc. The main data managed by the Corporation are:

Employee and applicant data - Human Resources

Client and prospective client data

Investor data

Supplier data

Security control data

4.2.- Data Subject: The natural person to whom the Personal Data belongs.

4.3.- Internal Personal Data Protection Officer: Employee appointed by the subsidiary's General Management as the person responsible for matters related to Personal Data.

4.4.- Personal Data Bank: An organized set of personal data, whether automated or not, regardless of the form or method of its creation, collection, storage, organization, or access.

4.5.- Personal Data Bank Controller: Employee appointed as the custodian of the data bank, who determines the purpose and content of the personal data bank, its processing, and the security measures to be applied.

4.6.- Cross-Border Data Flow: The transfer of Personal Data to a recipient located in a country different from that of the sender, regardless of the medium in which the data is stored, the means used for its transfer, or the processing it undergoes.

4.7.- ARCO Request Manager: Employee responsible for managing and responding to requests from Data Subjects to exercise their rights of Access, Rectification, Cancellation, and Opposition (ARCO).

V.- GENERAL PRINCIPLES

The processing of Personal Data within the Corporation is based on the following principles:

- **Legality:** Personal Data is collected and processed in accordance with applicable laws and regulations.
- **Consent:** The consent of the Data Subject is obtained freely, prior to processing, expressly, and in an informed manner, except for the exceptions established by law.
- **Purpose:** Personal Data is collected and processed for specific, lawful, and defined

purposes, which are communicated to the Data Subject.

- **Proportionality:** The Personal Data collected and processed must be adequate, relevant, and not excessive in relation to the purpose for which it is collected.
- **Quality:** Personal Data must be accurate, complete, and up to date. Reasonable measures are taken to ensure the accuracy and currency of the data.
- **Security:** Appropriate technical, organizational, and legal security measures are implemented to protect Personal Data against unauthorized access, misuse, alteration, loss, or destruction.
- **Transparency:** Data Subjects are informed about the processing of their Personal Data, including the purpose, recipients, and the rights available to them.
- **Confidentiality:** The confidentiality of Personal Data is guaranteed, and employees and third parties involved in data processing are required to maintain appropriate confidentiality.
- **Accountability:** Legal, technical, and organizational measures are applied to ensure effective compliance with personal data regulations, and the personal data bank controller or other responsible party must be able to demonstrate such compliance.

VI.- RIGHTS OF PERSONAL DATA SUBJECTS

The Corporation recognizes and guarantees the following rights of personal data subjects ("ARCO" Rights):

- **Access:** The right to obtain information about the Personal Data concerning them and the processing to which it is subjected.
- **Rectification:** The right to correct inaccurate or incomplete Personal Data.
- **Erasure (Cancellation):** The right to request the deletion of Personal Data when it is no longer necessary for the purpose for which it was collected, or when the Data Subject withdraws their consent.
- **Objection:** The right of the Data Subject to object to the processing of their Personal Data on legitimate and well-founded grounds.
- In addition to these rights, the Data Subject has the right to request the transfer of their Personal Data to another controller or holder of a Personal Data Bank, provided that its exercise does not impose an excessive or unreasonable financial or technical burden on the controller or processor (Portability).

Procedures for Exercising ARCO Rights

Data subjects may exercise their ARCO rights by submitting a written request through the channel established by each subsidiary of the Corporation for such purposes.

Requests must be submitted in writing to the address of the subsidiary company or to the following email address: privacidad@<subsidiary>.com.pe, either by the Data Subjects themselves (attaching their identification document) or by the representative of the Data Subject, who, in addition to their own identification document, must attach the power of attorney proving such representation.

The request will be handled by the ARCO Request Manager, in accordance with the guidelines and deadlines established in the protocol for handling ARCO rights requests, as implemented in each subsidiary.

VII.- RESPONSIBILITIES

7.1 OF THE CORPORATION

The Corporation has a Corporate Personal Data Protection Committee, a Personal Data Officer, a Deputy Management of Information Security, a Corporate Management of Corporate Affairs, Internal Personal Data Protection Officers in each subsidiary, Personal Data Bank Controllers, ARCO Request Managers, and Human Resources Managers or Heads, as well as Employees, all of whom have specific responsibilities regarding the processing of Personal Data, as detailed in this Code.

7.1.1 OF THE CORPORATE PERSONAL DATA PROTECTION COMMITTEE

The Corporate Personal Data Protection Committee is composed of the Personal Data Officer, the Corporate Manager of TPI, the Corporate Manager of Corporate Affairs, the Corporate Manager of Auditing, the Deputy Manager of Information Security, and the Senior Legal Advisor. The Committee will be chaired by the Deputy Manager of Information Security. It will meet regularly on a semi-annual basis and exceptionally when the situation so requires.

The main purpose of the Corporate Personal Data Protection Committee is to supervise, advise, and evaluate the development and compliance of the Corporation's personal data protection regulations.

The Corporate Personal Data Protection Committee will be supported by the Internal Personal Data Protection Officer of each company, who will be responsible for ensuring the correct implementation and compliance with the Committee's directives and decisions within the companies under their scope of control.

7.1.2 OF THE PERSONAL DATA OFFICER

- Inform and advise the Internal Personal Data Protection Officer of each company, the data controllers, and the employees involved in the processing of Personal Data regarding their obligations under current personal data protection regulations.
- Verify and report to the relevant parties on compliance with the provisions of the Law, its Regulations, all rules contained in this Code of Conduct, and any other applicable regulations.
- Cooperate, as appropriate, with the National Authority for the Protection of Personal Data in fulfilling its duties and responsibilities.
- Act as the contact point for the National Authority for the Protection of Personal Data on matters relating to the processing of Personal Data.

7.1.3 OF THE DEPUTY MANAGEMENT OF INFORMATION SECURITY

- Manage and keep the information security management system up to date, integrating within its scope the Personal Data Banks.
- Supervise the technical security controls related to the loss, access, alteration, or unauthorized processing of Personal Data, and manage their implementation through the different responsible areas.
- Manage and keep up to date the incident management procedure for the protection of Personal Data.
- Report to the Corporate Committee and the Personal Data Officer on assigned functions and tasks, particularly on the occurrence of any incident.

7.1.4 OF THE CORPORATE MANAGEMENT OF CORPORATE AFFAIRS

- Carry out the registration process of the Personal Data Banks and the declaration of cross-border data flow for the Corporation's companies before the General Directorate of Personal Data Protection.
- Provide consent forms, personal data protection agreement templates, and other necessary mechanisms for the implementation of legal measures.
- Provide legal advice to the Corporation in the implementation of legal measures.
- Develop an awareness and training program on personal data protection.
- Stay up to date on the latest versions of the law and its regulations, and communicate them promptly to the Deputy Manager of Information Security, the Personal Data Officer, the general managers of each Corporation company, and the President of the Asociación Ferreycorp.
- Verify, together with the Corporate Management of Auditing, compliance with this regulation.

7.1.5 OF THE CORPORATE MANAGEMENT OF AUDITING

- Conduct annual audit reviews, or when necessary, of compliance with applicable regulations in each company.
- Identify gaps in compliance with this regulation.
- Issue recommendations and obtain action plans from those responsible to address the gaps.
- Follow up and validate the implementation of the recommendations and action plans.
- Issue audit reports and progress updates on the implementation of recommendations and action plans to those responsible.
- Report any situation contrary to the provisions of this regulation to the Corporate Personal Data Protection Committee, the General Management of Ferreycorp, and, if the case warrants, to the Board of Directors' Audit and Risk Committee.

7.2. OF FERREYCORP COMPANIES AND NON-PROFIT ENTITY

7.2.1. OF THE GENERAL MANagements AND THE PRESIDENT OF THE ASOCIACIÓN FERREYCORP

- Appoint the Internal Personal Data Protection Officer, who will be responsible for managing the implementation and ongoing monitoring of compliance with each of the requirements of the law and its regulations, and ensure that they fully comply with their functions and responsibilities.
- Appoint the Personal Data Bank Controller, as applicable (for employees, suppliers, clients, investors, participants, human resources, or other categories as designated), who will keep the information up to date before the National Personal Data Protection Registry of the Ministry of Justice.
- Appoint the ARCO Request Manager.
- Supervise and control proper compliance with this regulation.

7.2.2. OF THE INTERNAL PERSONAL DATA PROTECTION OFFICER

- Identify and keep updated the inventory of the Personal Data Bank.
- Identify and keep updated the record of procedures for obtaining Personal Data and the systems used for its processing.
- Conduct a compliance assessment with the legal requirements and a risk evaluation for the company or non-profit entity in the event of non-compliance.
- Define action plans based on the compliance assessment and risk evaluation.
- Review and address observations and audit results from annual audits, incorporating them into action plans.
- Periodically monitor the progress of action plans.
- Ensure and control the recording of evidence of compliance with legal requirements.
- Report to the General Management or to the President of the Asociación Ferreycorp on compliance status and obligations, as well as the development and fulfillment of the obligations of the Personal Data Bank owners.

7.2.3. OF THE PERSONAL DATA BANK CONTROLLERS

- Identify the Personal Data Banks, assess their complexity and the existence of cross-border data flows, and complete/update the forms for their registration and updating.
- Identify the procedures for obtaining Personal Data and implement measures to obtain the consent of Data Subjects.
- Identify the systems used for processing Personal Data and inform the Deputy Management of Information Security to coordinate the implementation of the corresponding IT security controls.
- Ensure the implementation of technical security controls for Personal Data Banks under their responsibility and in physical format.
- Periodically review the access privileges that personnel have to the Personal Data Banks under their responsibility.
- Periodically report to the Personal Data Protection Committee on compliance status with their assigned responsibilities.
- Maintain evidence of compliance with each of the requirements established by law.
- Continuously inform the Internal Personal Data Protection Officer on the compliance status of their obligations.

7.2.4 OF THE ARCO REQUEST MANAGERS

The person responsible for handling requests must fulfill the following responsibilities:

- Implement and keep up to date the protocol for handling ARCO rights requests from Data Subjects.
- Receive, analyze, coordinate, and ensure the proper handling of ARCO rights requests.
- Periodically report to the Internal Personal Data Protection Officer on the status of ARCO rights requests received.
- Ensure the preservation of each ARCO rights request as evidence of compliance with the law.
- Coordinate with the Corporate Management of Corporate Affairs to ensure timely responses to ARCO rights requests.

7.2.5. OF THE HUMAN RESOURCES MANAGERMENTS OR HEADS OF EACH FERREYCORP COMPANY AND THE ASOCIACIÓN FERREYCORP

Human Resources managements/heads must:

- Promote employee participation in the personal data protection awareness and training program.
- Ensure that all employees sign the confidentiality agreement and the personal data processing agreement.
- Periodically report to the Personal Data Protection Committee on compliance status with their assigned responsibilities.
- Maintain evidence of compliance with each legal requirement.

7.2.6. OF ALL EMPLOYEES

Employees must:

- Participate in personal data protection awareness, training, and education programs, regardless of their format.
- Sign the confidentiality agreement and the personal data processing agreement, and comply with their content.
- Notify any event that compromises the security of personal data and may affect the personal, family, or reputational integrity of the Data Subjects or any of the Corporation's companies and the Asociación Ferreycorp.

VIII.- ON THE COLLECTION OF PERSONAL DATA

Subsidiaries of the Corporation and the Asociación Ferreycorp must identify the contact points through which Personal Data is collected.

Any management or department that, as part of its processes, services, or activities, needs to collect Personal Data must do so after obtaining the informed, express, and unequivocal consent of the Data Subjects, and exclusively for the purpose for which consent was obtained.

Notwithstanding the above, there may be specific situations where it is not necessary to obtain direct consent from Data Subjects due to a legal mandate, because the personal data is necessary for the execution of a contractual relationship in which the Data Subject is a party, among other cases. Such situations must be analyzed by the Internal Personal Data Protection Officer and/or the Personal Data Bank Controller, together with the Corporate Management of Corporate Affairs and the Personal Data Officer.

If, during the collection of Personal Data, it is found that there are Data Subjects not included in the identified and registered data banks in the inventory, this must be reported to the Internal Personal Data Protection Officer, who will appoint the controller of the new Personal Data Bank, and this person must implement all necessary organizational, legal, and technical security measures.

For reception areas or locations where Personal Data from visitors is collected, as well as premises, branches, or offices with video surveillance cameras recording visitors, it is not necessary to obtain written consent; it is sufficient to install a visible notice specifying the purpose of data collection and the channel for exercising ARCO rights, for each reception area or location with a camera.

Whenever a management or department uses a website to collect Personal Data, the website's main page must include the privacy policy, and each page with a data collection form must include a reference to this policy, where the Data Subject provides consent to process their Personal Data.

The main cases where Corporation subsidiaries may collect personal data via websites include:

- Responding to inquiries or complaints and following up on them.
- Sending information or advertising about products and services.
- Inviting participation in seminars, training sessions, workshops, contests, surveys, and other activities or events.
- Registering the Data Subject in the Operators' Club or another similar educational program developed by the Corporation's subsidiaries.
- Internal client management and administration, market studies, or commercial/statistical research.

- Carrying out billing processes; e-commerce.
- Managing applications for current or future vacancies in any of the Corporation's subsidiaries.
- Conducting evaluations for granting credit, updating or verifying information, or using it as a reference source.

IX.- ON PERSONAL DATA PROTECTION AGREEMENTS

For all cases in which the Corporation's subsidiaries contract third parties—such as clinics, call centers, couriers, among others—for services involving the collection, processing, or access to any Personal Data managed by the company, a personal data protection agreement must be signed, provided by the Corporate Management of Corporate Affairs.

For employees involved in the processing of Personal Data, the Corporation's subsidiaries must sign the confidentiality agreement provided by the Corporate Management of Corporate Affairs.

X.- ON THE DURATION OF PERSONAL DATA PROCESSING

The Personal Data processed by the Corporation will be stored for as long as necessary to fulfill the purposes of this regulation.

XI.- ON PERSONAL DATA INCIDENTS

Any event or breach of personal data security must be reported and addressed immediately, following the guidelines established in the Procedure for Notification of Personal Data Security Incidents (FCO-GTPI-SGI-PRD-001), as incidents must be reported to the Ministry of Justice within forty-eight (48) hours of their occurrence.

When an incident significantly affects the rights of the Data Subjects, they must be notified as soon as the event is confirmed.

Failure to comply with the obligation to notify a personal data security incident according to the aforementioned procedure will constitute a serious violation of this Code of Conduct.

Depending on the severity of the non-compliance, disciplinary sanctions may be applied, including but not limited to: verbal or written warnings, temporary suspensions, and even termination of employment, without prejudice to liability for damages caused by the incident, both to the Corporation and to the affected Data Subjects.

XII.- SECURITY AND CONFIDENTIALITY MEASURES

The Corporation has implemented and maintains appropriate technical, organizational, and legal security measures to protect Personal Data against unauthorized access, misuse, alteration, loss, or destruction, as detailed in the Security Standard for the Processing and Protection of Personal Data (FCO-GTPI-SGI-NOR-001). These measures are reviewed and updated periodically to ensure their effectiveness.

XIII.- ON THE DETERMINATION OF NATIONAL AND INTERNATIONAL PERSONAL DATA TRANSFERS AND THEIR GUARANTEES

This section of the Code of Conduct aims to establish the guidelines for carrying out Personal Data transfers, both within the national territory and to other countries, ensuring at all times compliance with Peruvian personal data protection regulations.

1. National Transfers::

- **Identification of Transfers:**

- An inventory must be prepared of all Personal Data transfers carried out within the Corporation, identifying the recipients of the data, the purpose of the transfer, and the legal basis supporting it. This includes companies and entities of the Corporation located inside and outside the country, as well as other third parties with whom there is a commercial or contractual relationship.

- **Guarantees:**

- Contractual clauses will be established to ensure that recipients of Personal Data comply with the data protection obligations set forth in Law No. 29733 and its Regulations.
- Periodic audits will be carried out to verify compliance with these obligations.
- Adequate technical and organizational security measures will be implemented to protect Personal Data during the transfer and while in the possession of the recipient.

2. International Transfers:

- **Assessment of the Receiving Country:**

- Before carrying out an international transfer of personal data, it must be evaluated whether the receiving country has an adequate level of data protection, in accordance with the standards established by Peruvian regulations.
- Consideration will be given to the existence of data protection laws, the independence of the supervisory authority, and the existence of effective mechanisms to protect the rights of data subjects.
-

- **Transfer Mechanisms:**

- If the receiving country does not have an adequate level of protection, transfer mechanisms must be implemented to ensure the protection of personal data, such as:
 - Standard contractual clauses: Use of standard contractual clauses approved by the Corporate Management of Corporate Affairs.
 - Security Standard: Application of the provisions of the Security Standard for the Processing and Protection of Personal Data.
 - Informed consent: Obtaining the Data Subject's informed consent for the international transfer.

- **Additional Guarantees:**

- Additional security measures will be implemented to protect Personal Data during international transfers, such as data encryption and anonymization.
- Ongoing monitoring of international transfers will be carried out to verify compliance with the established guarantees.

XIV.- TRAINING AND AWARENESS

The Corporation is committed to maintaining a culture of Personal Data protection through a comprehensive training and awareness program. This program includes:

- Ongoing training on the importance of data protection, the principles of the Code of Conduct, and individual responsibilities in data processing.
- An annual mandatory course for all employees, providing in-depth instruction on Personal Data processing practices.
- Periodic meetings with Internal Personal Data Protection Officers and Personal Data Bank Controllers to address specific issues and ensure alignment.

XV.- SUPERVISION AND COMPLIANCE

The Corporation's supervision and compliance structure is based on the collaboration of three key management areas:

- **Corporate Management of Corporate Affairs:**
 - Lead efforts to promote a culture of compliance in matters of Personal Data protection.
 - Ensure that this Code is aligned with applicable laws and regulations in the field.
 - This includes monitoring changes in legislation and updating this Code accordingly, if necessary.
 - Disseminate the contents of this Code and promote employee training.
- **Corporate Management of Auditing:**
 - Carry out an independent control mechanism.
 - Evaluate the effectiveness of internal controls and verify compliance with this Code through periodic audits.
 - Review processes, records, and systems to identify potential risks and deficiencies.
 - Generate reports to be presented to the Corporation's companies and entities, for decision-making and follow-up on action plans until their implementation.
- **Corporate Management of TPI (Technology, Processes, and Information):**
 - Through its Deputy Management of Information Security, ensure compliance with regulations related to information security.
 - Protect the confidentiality, integrity, and availability of information.
 - Implement security measures, monitor systems, and respond to security incidents.
 - Implement technology-related regulations, ensuring that all processes involving information comply with the highest security standards.

XVI.- AMENDMENTS

This Code will be modified or updated periodically to reflect changes in legislation, regulations, and best practices in the field of Personal Data protection.

XVII.- FINAL PROVISIONS

This Code is mandatory for all employees and third parties involved in the processing of Personal Data within the Corporation.

Any breach of this Code may result in disciplinary measures, including termination of employment.

XVIII.- CONTACT

If you have any questions or concerns regarding this Code of Conduct, you may contact us at the following email address: privacidad@ferreycorp.com.pe

XIX.- EFFECTIVE DATE: From March 31, 2025

XX.- FORMS. Forms for collecting Personal Data must be adapted to each specific situation. There is no single model, as the content and structure depend on:

Purpose: The reason for collection must be clear, and the form must be limited to the strictly necessary data.

Processing: The actions to be taken with the data (storage, processing, transfer, etc.) will determine the requirements of the form.

Nature of the data: Sensitive data or data referring to minors require enhanced security measures and reinforced consent.

Among the main forms implemented are the following:

- 20.1: Authorization for the Processing of Personal Data of Suppliers.
- 20.2: Authorization for the Processing of Personal Data of Clients.
- 20.3: Authorization for the Processing of Personal Data of Students enrolled in training courses.
- 20.4: Authorization for the Processing of Personal Data of Employees.
- 20.5: Authorization for the Processing of Personal Data of Job Applicants.
- 20.6: ARCO Rights Request Form for Personal Data Protection.
- 20.7: Visitor Registration Notice Signage.
- 20.8: Video Surveillance Camera Notice Signage.

Annex 20.1
AUTHORIZATION FOR THE PROCESSING OF PERSONAL
DATA PROTECTION FOR SUPPLIERS

[Name], identified with National Identity Document (D.N.I.) No. [____], with Taxpayer Identification Number (R.U.C.) No. [____], residing at [____], district of [____], province of [], department of [], HEREBY **AUTHORIZES** the company **<Full name of subsidiary>** (hereinafter **<short name of subsidiary>**) to include and process the personal data provided or generated as a result of the service provision relationship in favor of **<short name of subsidiary>**, acknowledging that the personal data provided will be stored in the database called “**Suppliers**,” owned by **<short name of subsidiary>**, which is duly registered with the National Authority for the Protection of Personal Data.

The processing may be carried out directly by **<short name of subsidiary>** or may be shared with companies affiliated with the business group, associated companies, or by a designated third-party agent, which may be located within or outside the national territory, in accordance with the terms and purposes of this consent.

The **purpose** of the processing is to ensure the proper execution of the contractual relationship, even after the contractual relationship has ended. For this reason, the authorization is granted for an indefinite period or until it is revoked. Furthermore, other purposes of processing your information include: (i) managing the supplier list; (ii) sending commercial proposals for both products and services; (iii) coordinating billing and payments; (iv) conducting inquiries and quotations; (v) executing the service provided; and (vi) administrative and commercial purposes.

Some of the data covered by this authorization include: full name, DNI and RUC number, address, telephone number, image, email address, nationality, banking details, tax information, and other data that may be considered personal data. The information provided may also be used for statistical purposes.

It is established that, at any time, you may exercise your ARCO rights: access, rectification, objection, and cancellation of personal data, by sending a communication addressed to the offices of **<short name of subsidiary>** or via email.

Finally, you declare that you comply with the provisions of the Personal Data Protection Law and its Regulations, as applicable in the context of the service provision relationship you maintain with **<short name of subsidiary>**. In the event of non-compliance, **<short name of subsidiary>** may take the necessary legal actions to recover any damages it may suffer as a result of such non-compliance.

This Authorization is signed as a sign of agreement in the city of Lima, on the [____] day of the month of [____] of the year two thousand [____].

SIGNATURE
DATE: ____/____/____

Annex 20.2

**AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA OF CLIENTS IN ACCORDANCE
WITH LAW No. 29733**

[Name], identified with National Identity Document (D.N.I.) No. [____], with Taxpayer Identification Number (R.U.C.) No. [____], residing at [____], district of [____], province of [____], department of [____], **HEREBY AUTHORIZES** the company **<full name of subsidiary>** (hereinafter **<short name of subsidiary>**) to include and process the personal data provided or generated as a result of the service provision relationship in favor of **<short name of subsidiary>**, acknowledging that the personal data provided will be stored in the database called "**CLIENTS**," owned by **<short name of subsidiary>**, which is duly registered with the National Authority for the Protection of Personal Data.

The processing may be carried out directly by **<short name of subsidiary>** or may be shared with companies affiliated with the business group, associated companies, or by a designated third-party agent, which may be located within or outside the national territory, in accordance with the terms and purposes of this consent.

The purpose of the processing is to ensure the proper execution of the contractual relationship, even after it has ended. For this reason, the authorization is granted for an indefinite period or until it is revoked. Furthermore, other purposes of processing your information, by phone or email, include: (i) adequately responding to information requests; (ii) sending information about the products sold and services provided by the company; (iii) determining whether you are interested in acquiring any of the products and/or services offered; (iv) sending quotations and product and/or service specifications; (v) sending promotions, newsletters, and event invitations; (vi) processing billing and payment for services rendered and products sold; and (vii) administrative and commercial purposes.

Some of the data covered by this authorization include: full name, DNI and RUC number, address, telephone number, image, email address, nationality, banking details, tax information, and other data that may be considered personal data. The information provided may also be used for statistical purposes.

It is established that, at any time, you may exercise your ARCO rights: access, rectification, objection, and cancellation of personal data, by sending a communication addressed to the offices of **<short name of subsidiary>** or via email.

Finally, you declare that you comply with the provisions of the Personal Data Protection Law and its Regulations, as applicable in the context of the service provision relationship you maintain with **<short name of subsidiary>**. In the event of non-compliance, **<short name of subsidiary>** may take the necessary legal actions to recover any damages it may suffer as a result of such non-compliance.

This Authorization is signed as a sign of agreement in the city of Lima, on the [____] day of the month of [____] of the year two thousand [____].

SIGNATURE
DATE: ____/____/____

Annex 20.3
AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA OF STUDENTS IN
ACCORDANCE WITH LAW No. 29733

[Name], identified with National Identity Document (D.N.I.) No. [____], with Taxpayer Identification Number (R.U.C.) No. [____], residing at [____], district of [____], province of [____], department of [____], HEREBY AUTHORIZES the company **<full name of subsidiary>** (hereinafter **<short name of subsidiary>**) to include and process the personal data provided or generated as a result of the service provision relationship in favor of **<short name of subsidiary>**, acknowledging that the personal data provided will be stored in the database called "STUDENTS," owned by **<short name of subsidiary>**, which is duly registered with the National Authority for the Protection of Personal Data.

The processing may be carried out directly by **<short name of subsidiary>** or may be shared with companies affiliated with the business group, associated companies, or by a designated third-party agent, which may be located within or outside the national territory, in accordance with the terms and purposes of this consent.

The purpose of the processing is to provide information about the courses offered by the Ferreycorp Corporation company and to manage the training activities.

Some of the data covered by this authorization include: full name, DNI and RUC number, address, telephone number, image, email address, nationality, banking details, tax information, and other data that may be considered personal data. The information provided may also be used for statistical purposes.

It is established that, at any time, you may exercise your ARCO rights: access, rectification, objection, and cancellation of personal data, by sending a communication addressed to the offices of **<short name of subsidiary>** or via email.

Finally, you declare that you comply with the provisions of the Personal Data Protection Law and its Regulations, as applicable in the context of the service provision relationship you maintain with **<short name of subsidiary>**. In the event of non-compliance, **<short name of subsidiary>** may take the necessary legal actions to recover any damages it may suffer as a result of such non-compliance.

This Authorization is signed as a sign of agreement in the city of Lima, on the [____] day of the month of [____] of the year two thousand [____].

SIGNATURE

DATE: ____/____/____

Annex 20.4
AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA OF EMPLOYEES IN
ACCORDANCE WITH LAW No. 29733

[Name], identified with the National Identity Document (D.N.I.) No. [_____], with Taxpayer Identification Number (R.U.C.) No. [_____], residing at

[_____], district of [_____], province of [_____], department of [_____], HEREBY AUTHORIZES the company <full name of subsidiary> (hereinafter <short name of subsidiary>) to include and process the personal data provided or generated as a result of the employment relationship in favor of <short name of subsidiary>, acknowledging that the personal data provided will be stored in the database called "EMPLOYEES," owned by <short name of subsidiary>, which is duly registered with the National Authority for the Protection of Personal Data.

The processing may be carried out directly by <short name of subsidiary> or may be shared with companies affiliated with the business group, associated companies, or by a designated third-party agent, which may be located within or outside the national territory, in accordance with the terms and purposes of this consent.

The purpose of the processing is related to the employment relationship for the position applied for, and it is necessary to have your data for: (i) curriculum vitae; (ii) completion of forms or documents required to maintain in relation to the employment relationship; and (iii) providing employment-related information.

Some of the data covered by this authorization include: full name, DNI and RUC number, address, telephone number, image, email address, nationality, banking details, tax information, and other data that may be considered personal data. The information provided may also be used for statistical purposes.

It is established that, at any time, you may exercise your ARCO rights: access, rectification, objection, and cancellation of personal data, by sending a communication addressed to the offices of <short name of subsidiary> or via email.

Finally, you declare that you comply with the provisions of the Personal Data Protection Law and its Regulations, as applicable in the context of the employment relationship you maintain with <short name of subsidiary>. In the event of non-compliance, <short name of subsidiary> may take the necessary legal actions to recover any damages it may suffer as a result of such non-compliance.

This Authorization is signed as a sign of agreement in the city of Lima, on the [_____] day of the month of [_____] of the year two thousand [_____].

SIGNATURE

DATE: ____ / ____ / ____

Annex 20.5
AUTHORIZATION FOR THE PROCESSING OF PERSONAL DATA OF JOB APPLICANTS IN
ACCORDANCE WITH LAW No. 29733

[Name], identified with National Identity Document (D.N.I.) No. [_____] , with Taxpayer Identification Number (R.U.C.) No. [_____] , residing at [_____] , district of [_____] , province of [_____] , department of [_____] , HEREBY AUTHORIZES the company <full name of subsidiary> (hereinafter <short name of subsidiary>) to include and process the personal data provided or generated as a result of the service provision relationship in favor of <short name of subsidiary>, acknowledging that the personal data provided will be stored in the database called "APPLICANTS," owned by <short name of subsidiary>, which is duly registered with the National Authority for the Protection of Personal Data.

The processing may be carried out directly by <short name of subsidiary> or may be shared with companies affiliated with the business group, associated companies, or by a designated third-party agent, which may be located within or outside the national territory, in accordance with the terms and purposes of this consent.

The purpose of the processing is related to the job application process within the company, requiring the completion of forms or other types of documents, as well as data needed for medical, psychological, and aptitude evaluations.

Some of the data covered by this authorization include: full name, DNI and RUC number, address, telephone number, image, email address, nationality, banking details, tax information, and other data that may be considered personal data. The information provided may also be used for statistical purposes.

It is established that, at any time, you may exercise your ARCO rights: access, rectification, objection, and cancellation of personal data, by sending a communication addressed to the offices of <short name of subsidiary> or via email.

Finally, you declare that you comply with the provisions of the Personal Data Protection Law and its Regulations, as applicable in the context of the service provision relationship you maintain with <short name of subsidiary>. In the event of non-compliance, <short name of subsidiary> may take the necessary legal actions to recover any damages it may suffer as a result of such non-compliance.

This Authorization is signed as a sign of agreement in the city of Lima, on the [_____] day of the month of [_____] of the year two thousand [_____].

SIGNATURE

DATE: ____/____/____

Annex 20.6
REQUEST FORM FOR ARCO RIGHTS REGARDING PERSONAL DATA
PROTECTION

DATA SUBJECT:

Last Name(s) First Name(s)

LEGAL REPRESENTATIVE OF THE DATA SUBJECT:

Last Name(s) First Name(s)

Street: _____ N°: _____
Office/Apartment.: _____ District: _____ Province: _____
Region: _____ Phone.: _____

Relationship with the Company:

Email _____

DOES THE APPLICANT AUTHORIZE RECEIVING NOTIFICATIONS ON THE APPROVAL OR DENIAL OF THIS REQUEST THROUGH ELECTRONIC MEANS?

YES _____

NO _____

Email address (if authorized): _____

- ☐ ACCESS to your personal data.
- ☐ RECTIFICATION of your personal data.
- ☐ CANCELLATION of your personal data from the databases.
- ☐ OBJECTION to the processing of your personal data.

In the case of requests for rectification of personal data, the Data Subject must indicate the modifications to be made and provide the documentation supporting their request.

DESCRIPTION OF THE REQUEST:

Attached: A copy of the Data Subject's Identity Document and, in the case of a legal representative, the certificate of authority issued by the Public Registry Office confirming the registration of the representative's power of attorney, along with any documents supporting the request.

NOTIFICATION OF RESPONSE TO YOUR REQUEST:

Email:

Address:

Name and Signature of the Data Subject or Legal Representative
DATE:

Annex 20.7
VISITOR REGISTRATION NOTICE SIGNAGE

Por razones de seguridad, sírvase indicar sus datos personales antes de ingresar.

Para consultas o ejercer sus derechos de titular de datos personales, comuníquese a
privacidad@<nombre de subsidiaria.com.pe>

Annex 20.8
VIDEO SURVEILLANCE CAMERA NOTICE SIGNAGE

ZONA VIDEOVIGILADA



(Por razones de seguridad esta local cuenta con cámaras de video vigilancia. Para consultas o ejercer sus derechos de titular de datos personales, comuníquese a privacy@acti.com.ec o acti@acti.com.ec)

(Por razones de seguridad, usted está siendo grabado. Para ejercer sus derechos de la Ley 20039, Ley de protección de datos personales, comuníquese a acti@acti.com.ec.)

THIS DOCUMENT HAS BEEN AUTHORIZED IN THE REGULATORY SYSTEM BY:

ROLE	NAME	POSITION	DATE / STATUS
Preparer	Rodolfo Gutierrez Diez	Senior Legal Advisor	Approved – 04/07/2025 11:49
Reviewer	Eduardo Ramirez Del Villar	Corporate Manager of Corporate Affairs	Approved – 04/07/2025 12:43
Approver	Mariela Garcia De Fabbri	General Manager	Approved – 04/08/2025 22:23