Credicorp Compliance and Ethics
Personal Data Protection Program (PDP)
Personal Data Protection Corporate Policy
Effective date: 26/05/2025
Date of Publication: 22/05/2025

1. General objectives

Credicorp Group Companies are committed to the protection and privacy of the Personal Data of the Data Subjects, as well as to compliance with the Personal Data Protection regulations in force in each country where they operate.

This Corporate Policy aims to:

a) Establish the general guidelines for the Processing and Transfer of Personal Data of stakeholders such as employees, users, clients, and suppliers in all Credicorp Group Companies.
b) Ensure that the Credicorp Group Companies comply with the Personal Data Protection regulations.
c) Raise awareness among all employees of the Credicorp Group Companies about the impact of non-compliance with the Personal Data Protection regulations.

2. Regulatory framework

This policy is grounded in Personal Data Protection Law No. 29733 **(Data Protection Law)** and its Regulations, approved by Supreme Decree No. 016-2024-JUS, in force in Peru, as well as other complementary, amending, and clarifying regulations.

Credicorp Group Companies that are not domiciled in Peru must comply with this Corporate Policy, provided that doing so does not contravene the applicable regulations in their respective jurisdictions. Any reference to the Data Protection Law, “national territory,” or Peru shall be understood as referring to the applicable regulation in force for the Credicorp Group Company and the country in which it is domiciled.

3. Definition

a) **Information Asset:** all physical documents (PD), digital documents (DD) and computer applications (APP) that have a value for the company and / or support or are part of the activity, process or line of business of the organization.
b) **Computer application outside the custody of the Systems Unit (APPnoIT):** all information assets oriented to data processing and administration that are managed by a Unit, and are also housed in the same Unit or in the Systems Unit. This definition includes digital files with programming logic in their content, such as: macros in Excel, databases in Access, workflows in SharePoint, among others.
c) **Personal Data Base:** organized set of Personal Data, automated or not, and regardless of whether it is in physical, magnetic, digital, or other form, and regardless of the form or modality of its creation, training, storage, organization or access, provided that it allows access to the Personal Data without disproportionate effort.
d) **Consent:** authorization of the Owner of the Personal Data for the Data Controller to Process and / or Transfer the data.
e) **DPDP:** Directorate of Personal Data Protection
f) **Personal Data:** Any information about a natural person that identifies them or makes them identifiable through means that can be reasonably used, or when the person’s identity can be verified directly or indirectly through the combination of data. This includes, but is not limited to, numerical, alphabetical, graphic, photographic, or acoustic information, as well as data related to personal habits, location, online identifiers, or any other type of information concerning physical, economic, cultural, or social aspects. E.g.: names and surnames, NID

(National identification number) / RUC (unique taxpayer registry), passport, sex, profession, age, nationality, date of birth, address, telephone, email, photograph, signature, voice, etc.

g) **Sensitive Data:** These are Personal Data related to economic income, Biometric Data, racial or ethnic origin, neural, moral, or emotional characteristics, data related to affective or family life, personal habits pertaining to the most intimate sphere of the individual, union membership, political, religious, or philosophical opinions or beliefs, data related to sexual life, physical or mental health, or other similar aspects that affect personal privacy. Health-related data are considered to include information about past, present, or forecasted physical or mental health. This also includes information derived from medical acts, degree of disability, and genetic information.

h) **Biometric data:** personal data obtained from a specific technical processing, relating to the physical, physiological or behavioral characteristics of a natural person that allow or confirm the unique identification of such person, such as facial images or dactyloscopy data. Biometric data constitutes sensitive data.

i) **Digital document (DD):** any information asset that contains data in electronic format, and that requires a computing device for access and consultation. Any digital file containing programming logic in its content, such as macros in Excel, is excluded from this definition.

j) **Physical document (PD):** all information assets containing data recorded in a tangible format such as cash receipts, operational control documents, active documents, passive documents and documents for physical filing, among others.

k) **Profiling:** a form of automated processing of personal data that makes it possible to evaluate aspects of a natural person, in a specific and continuous manner, in order to analyze or predict aspects relating to his or her professional performance, economic situation, health, personal preferences, interests, reliability, behaviors or habits, location or movements.

l) **Credicorp Group Companies:** empresas peruanas y extranjeras del Grupo Credicorp, tales como el Banco de Crédito del Perú, Mibanco Perú, Prima AFP, Pacífico S.A. Entidad Prestadora de Salud y sus empresas: Clínica San Felipe S.A., Sistemas de Administración Hospitalaria S.A.C, La Esperanza del Perú S.A., Clínica Sánchez Ferrer S.A., Doctor + S.A.C., Oncocare S.A.C., Laboratorios Roe S.A., Centro Médico Odontológico Americano S.A.C., Análisis Clínicos ML S.A.C., Prosemedic S.A.C. , Pacífico Seguros, Pacífico Asiste, Grupo Crédito, Culqi, Krealo, Patronato BCP, Instituto Bicentenario, Joinnus, Yape Market S.A.C y Credicorp Capital Perú y sus subsidiarias (Credicorp Capital SAB, Credicorp Capital SAF, Credicorp Capital Sociedad Titulizadora y Credicorp Capital Servicios Financieros), Mibanco Colombia, Credicorp Colombia, Credicorp Chile, ASB Panamá, BCP Panamá, Tyba and Monokera.

m) **Data Processor:** any natural or legal person under private law or public entity that, alone or acting jointly with another, performs the Personal Data Processing on behalf of the Data Controller by virtue of a legal relationship under which such person acts in the direction of the Data Controller. Such a person includes whoever performs the processing without the existence of a Personal Data Base.

n) **Processing order:** Transfer of Personal Data by or on behalf of the Data Controller to a Data Processor pursuant to a legal arrangement that delimits the scope of action of the Data Processor.

o) **Transit purposes:** implies that the means are not used for the specific purpose of performing the processing of personal data, such as processing, storage, downloading, viewing and/or similar, but exclusively to move personal data from one place to another.

p) **Cross-border Transfer of Personal Data:** International transfer of Personal Data to a recipient located in a country other than the country of origin of the Personal Data, regardless the format these are in, the means by which the transfer was made, or the processing they receive.

q) **Personal Data Officer:** person appointed by the controller or processor of personal data for the verification, advice and implementation of compliance with the legal regime on personal data protection.

r) **Personal Data Portability:** Action through which the holder of the personal data obtains the information he/she has provided to a data controller, in order to transmit it to another data controller.
s) **First contact:** Prior contact that may be made by a holder of a personal data bank with the purpose of obtaining the consent of the holder of the personal data to subsequently contact him/her for commercial and advertising purposes.
t) **Data Enrichment Provider:** A company that has a commercial relationship with a Credicorp Group Company, whether or not it is part of the group, and that, in its capacity as **Data Controller** (or **Data Bank Holder**, depending on the applicable jurisdiction), has obtained the **Data Subject's Consent** to transfer their information, always in compliance with applicable personal data protection regulations.
u) **Data Controller:** natural person, legal person under private law or public entity that decides on the purpose and means of the processing of personal data. This definition is not restricted to the owner of the data bank but includes any person who decides on the processing of personal data, even if he/she is not in a personal data bank.
v) **Business partners:** Companies that have a business relationship with the Credicorp Group Company, which may or may not belong to the Credicorp Group.
w) **Third-Party Companies:** Companies to which Personal Data may be transferred and whose list is available to the Data Subject. This includes companies within the Credicorp Group.
x) **Personal Data Owner:** individual to whom the Personal Data pertains.
y) **Data Controller:** individual, legal entity of private law or public entity that determines the purpose and content of the Personal Data Base, the processing of the Personal Data in the Personal Data Base, and the security measures to apply to the Personal Data Base.
z) **Transfer:** any transmission, supply or manifestation of Personal Data, national or international, to a legal person under private law, to a public entity or to an individual other than the Owner of Personal Data.
aa) **Processing:** any operation or technical procedure, automated or not, that allows the collection, registration, organization, storage, conservation, elaboration, modification, extraction, consultation, use, blocking, deletion, communication by transfer or by diffusion or any other form of processing that facilitates access, correlation or interconnection of Personal Data.

4. Scope of Personal Data Protection Rules

The Personal Data Protection Rules establish a protection framework for Personal Data that is to be contained and / or is intended to be contained in Personal Data Bases of public and / or private administration, whose processing is carried out by individuals, public entities or institutions of the private sector in the national territory or in the following cases:

- It is carried out by a Data Controller or Data Processor, regardless of its location, in behalf of the Data Controller established in Peruvian territory.
- When the Data Controller or the Data Proceessor is not established in Peruvian territory, but Peruvian legislation is applicable by contractual provision or international law.
- When the Data Controller or the Data Processor is not established in Peruvian territory, but uses means located in Peru, unless such means are used solely for transit purposes that do not involve the processing of personal data. This includes the following assumptions:

  a. The Personal Data Bank Holder or the Data Controller carries out activities related to the offer of goods or services directed to data subjects located in Peru.
  b. When the Personal Data Bank Holder or the data controller carries out activities aimed at analyzing the behavior of data subjects located in Peruvian territory, as well as the

elaboration of profiles that seek to predetermine behaviors, preferences, habits or the like.

These are outside the scope of the Personal Data Protection Rules the Processing carried out on information supplied by a legal person.

5. Responsabilities

In order to comply with the Personal Data Protection Standards, directors, managers, the Credicorp Regulatory Compliance Officer, Information Security Officers, those in charge of both in the companies of the Credicorp Group, and employees in general will have the following responsibilities:

a) The Board of Directors of each of the companies of the Credicorp Group shall carry out the necessary actions in order that each company adopt the necessary measures to ensure compliance with the Personal Data Protection Standards and ensure periodic control of compliance with the policies and procedures that are implemented for this purpose.

b) Managers in the Credicorp Group companies shall align their procedures to this Corporate Policy and adopt the necessary measures to ensure that the personnel in charge know and apply it.

c) The Credicorp Regulatory Compliance Officer and / or the respective managers in the Credicorp Group companies shall:

- Incorporate into Credicorp's compliance culture the obligations related to the protection of Personal Data.
- Ensure monitoring and investigation for compliance with this Corporate Policy.
- Coordinate sanctions for non-compliance with this Corporate Policy.
- Ensure the development and implementation of procedures to ensure compliance with the Personal Data Protection Standards.
- Be an interlocutor between the DPDP and the companies of the Credicorp Group.
- Manage the registration and updating of the Personal Data Bases and Cross-Border Transfers of responsibility of the companies of the Credicorp Group before the DPDP.
- Assist with DPDP inspections and requirements.
- Inform the Board of Directors on any topic of interest related to compliance with this Corporate Policy.
- At BCP, the Credicorp Regulatory Compliance Officer performs the function of representative of the Personal Data Bank Holder before the DPDP. In the case of the other Credicorp Group Companies, the General Management will be the one to designate the representative.

d) The Credicorp Group´s Personal Data Officer shall:

- Perform their duties with due regard to the risks associated with personal data processing operations, taking into account the nature, scope, context and purposes of such processing.
- Inform and advise the holder of the personal data bank or the data controller and the employees dealing with the processing of personal data regarding their obligations under the Law, the Regulations and other provisions.
- Act as a point of contact for the National Authority for the Protection of Personal Data.

- Verify and report on compliance with the provisions of the regulations on the protection of personal data, as well as compliance with the policies of the data bank owner or data processor on the protection of personal data, including the assignment of responsibilities, awareness and training of personnel involved in processing operations, and audits to be carried out.
- To cooperate, as appropriate, with the National Authority for the Protection of Personal Data for the performance of its purposes and attributions.

e) The Information Security Officer of the parent company (BCP), or the person designated to perform these duties within the entity, or the Information Security Officer in each Credicorp Group Company, in accordance with the Information Security Governance defined in standard 4205.010.67 – Corporate Information Security General Policy, shall

a. IT Security:

- Identify the rules on the matters that refer to the Personal Data Protection Rules.
- Define the security baselines for the infrastructure where the applications reside.
- Define security guidelines for applications that carry out Personal Data Processing outside the facilities of each Credicorp Company.
- Execute virtual training so that employees know the internal technical security regulations.
- Define security guidelines for sending Personal Data by computer support means.
- Define guidelines for maintaining audit records.
- Define guidelines for email transfers.
- Define guidelines for Non-IT Apps and Digital Documents to comply with the Personal Data Protection Standards.

b. Information Security for Physical Documents:

- Identify the standards required to implement compliance with the Personal Data Protection Rules.
- Define security guidelines for the Processing of Personal Data in physical documents inside and outside the facilities.
- Define security guidelines for the transfer and sending of Personal Data by physical means in order to adopt measures that prevent the access or manipulation of the information object of the transfer.
- Define guidelines so that the Processing of physical documents that contain Personal Data comply with the Personal Data Protection Regulations.
- Train employees in security controls, as required by in the internal security guidelines, for the processing of Personal Data in physical documents.
- Monitor compliance with security guidelines for the Processing of personal data in physical documents.

f) All employees of each of the Credicorp Group Companies shall comply with:

- Make appropriate treatment of the Personal Data to which it has access.
- Make sure to follow the processes already implemented by the corresponding areas.
- Use the Personal Data for the purpose for which they were collected and on which the Personal Data Holder has given us his Consent.
- The Personal Data Protection Rules.
- This Corporate Policy, for which the policies established by the Corporate Compliance Division of each Credicorp Company shall be taken into account.

g) Purposes for the collection of Personal Data:

- Execution of the contractual relationship (in the case of employees, this includes the employment relationship).
- The Credicorp Group Company that obtained the Consent may, either directly or through its Data Processors:
  - Offer its own products or services, or those of Third-Party Companies.
  - Send invitations to its own events or those of Third-Party Companies.
  - Send information about loyalty programs and benefits offered by itself or by Third-Party Companies.
  - Conduct market research and studies, as well as profiling activities.
  - Enrich its own Database or that of Third-Party Companies.
  - Transfer Personal Data to Third-Party Companies so that they may carry out the same purposes described above.

6. General considerations

As there are functions and roles that handle Personal Data, the managements may have greater restrictions in their unit than the provisions of this Corporate Policy, in which case the most demanding provision will prevail.

If exceptions to this Corporate Policy are required, the conformity of the Credicorp Regulatory Compliance Officer should be had.

7. Guidelines / Policies

7.1. Guiding Principles

The Credicorp Group companies, in their capacity as Data Controllers, shall comply with the guiding principles of personal data protection, in accordance with the provisions of the Personal Data Protection Standards and the guidelines established by the Legal Division of each of the Credicorp Companies and Corporate Compliance Division. These principles are listed below:

a) Principle of Legality

The processing of personal data is done in accordance with the provisions of the Law. The collection of personal data by fraudulent, unfair or unlawful means is prohibited.

b) Principle of Consent

The Processing of Personal Data is lawful when the Owner of the Personal Data gives his/her free, prior, express, informed and unequivocal Consent. Consent formulas in which the consent is not expressed in a direct way are not admitted.

c) Principle of Purpose

It is considered that a purpose is determined, when it has been expressed clearly, without confusion and when the goal of the Processing of Personal Data is objectively specified.

In the case of Personal Data Bases that contain Sensitive Data, their creation can only be justified if their purpose, in addition to being legitimate, is concrete and in accordance with the activities or explicit purposes of the Data Controller.

Data processors, in addition to being limited by the purpose of their services, are obliged to keep professional secrecy.

d) Principle of Proportionality

All Personal Data Processing shall be adequate, relevant and not excessive to the purpose for which the Personal Data were collected.

e) Quality Principle
Personal Data to be processed must be truthful, accurate, and, to the extent possible, up to date, necessary, relevant, and appropriate in relation to the purpose for which they were collected. It is presumed that the data directly provided by the Data Subject are accurate.

f) Principle of Security

In the Processing of Personal Data, the necessary security measures shall be adopted in order to avoid any processing contrary to the Personal Data Protection Rules, including adulteration, loss, deviations of information, intentional or not, whether the risks come from human interventions or the technological means used.

g) Principle of Appeal Disposition

All Personal Data Owners shall have available administrative or jurisdictional channels through which to claim and assert their data protection rights, when they believe those rights have been violated by Data Processing.

h) Principle of Adequate Protection Level

For the Cross-Border Flow of Personal Data, a sufficient level of protection must be guaranteed for the Personal Data to be processed; such level of protection must be at least comparable to that provided by the Personal Data Protection regulations or by applicable international standards on the matter.

i) Principle of Transparency

The processing of personal data must be informed in a clear, accessible and understandable manner for the holder of the personal data. This principle ensures that the holder is fully aware of the conditions of the processing, of the rights he/she may exercise and of the provisions set forth in Article 18 of the Data Law.

j) Principle of Proactive Responsibility

In the processing of personal data, legal, technical and organizational measures must be implemented to ensure effective compliance with the applicable regulations. In addition, the owner of the personal data bank or the person responsible for the processing must be able to demonstrate such compliance.

7.2. Consent of the Personal Data Owner

The Companies of the Credicorp Group, in their capacity as Data Controllers, have the obligation to obtain the Consent of the Owner of the Personal Data to the Processing and

Transfer of his or her Personal Data, taking into account the provisions of the Rules of Personal Data Protection and the guidelines established by the Legal Division of each of the Credicorp Companies and the Corporate Compliance Division. The Consent shall be:

- **Free**: without error, bad faith, violence or fraud, such that may affect the manifestation of will of the Personal Data Owner, which shall be voluntary.

- **Previous:** shall be requested before the collection and processing of Personal Data.

- **Express and unmistakable:** shall be stated in the conditions that do not admit doubts as to its granting. The manifestation of the will of the Owner of Personal Data can be verbal when it is externalized orally in person or through the use of any technology that allows oral dialogue; or, written by means of a document with a signature, a fingerprint or another such as authorized by the legal system that remains or may be printed on a paper surface or the like (e.g. "clicking" is a valid written statement through digital media). In the case of Sensitive Data, Consent must necessarily be expressed in writing.

- **Informed:** the Owner of Personal Data shall be informed by the Data Controller clearly, expressly, simply and prior to its collection, as to the purpose for which his/her Personal Data will be processed, who are or may be its recipients, the existence of the Personal Data Base in which they will be stored, as well as the identity and address of the Data Controller and, if applicable, the Data Processor, the mandatory or optional nature of your answers to the questionnaire proposed to you, the consequences of providing your Personal Data and of your refusal to do so, the time during which the Personal Data will be kept, the Transfer of your Personal Data, the existence of automated decisions, including profiling, and information regarding the consequences for the Personal Data Holder, and the possibility of exercising the rights granted to you by the Personal Data Protection Law and the means provided for such purpose.

  Additionally, the consent of the personal data subjects may be obtained through the First Contact. Once a data subject's data is obtained in a lawful manner, it may be used only once to request consent for the processing of his or her data for advertising and/or commercial prospecting purposes.

  In the event that the personal data used to carry out this figure have not been collected directly by the owner of the information, this must be brought to the attention of the owner of the information in the first contact communication, indicating the source of collection of these.

  If the owner of the personal data grants consent for advertising and/or commercial prospecting purposes during the First Contact, advertising may be offered during the second part of the call. If the owner of the data does not give his consent for commercial purposes, he may not be contacted again under the same figure in order to obtain his consent.

  Credicorp Group companies are responsible for the treatment of personal data in the process of prospecting their products and/or services, regardless of the means used. The third-party companies hired to contact the holder of the personal data fulfill the role of providers in charge.

7.3. Revocation of Consent

The right of the Data Subject to revoke his or her Consent for the Processing of his or her Personal Data at any time, without prior justification and provided that such processing is carried out for purposes additional to those that give rise to the authorized Processing. The revocation request must be carried out through easily accessible and unconditional, simple, fast and free mechanisms and within a maximum period of 10 working days, during which time it is necessary to adapt the new processing and those in the process of being carried out. However, such revocation request shall not proceed if the Personal Data are necessary for the execution of the contractual relationship that the Personal Data Holder maintains with the Credicorp Group Company, nor if the Personal Data must be kept for historical, statistical or scientific reasons in accordance with the applicable legislation. Notwithstanding the exercise of the right of revocation, the Holder of the Personal Data Bank shall keep the corresponding information for the term foreseen in the legal provisions in force.

7.4. Exceptions to the Need for Consent of the Personal Data Owner

The Data Controller or the Data Processor does not need to obtain the authorization of the Owner of the Personal Data when carrying out Processing in the following cases:

a) When Personal Data is contained or intended to be contained in sources accessible to the public (RENIEC, SUNAT, SBS, JNE, SUNARP, ESSALUD, White Pages, Professional Schools, INFOCORP, Risk Centers, etc.)

b) When these are Personal Data on capital and credit solvency, in accordance with the provisions of the law.

c) When there is a rule for the promotion of competition in regulated markets, issued in the exercise of the regulations function by the regulatory bodies referred to in Law 27332 - Framework Law of Regulatory Bodies for Private Investment in Public Services, or then to take its place, provided that the information provided is not used to the detriment of the user's privacy.

d) When Personal Data is necessary for the preparation, celebration and execution of a contractual relationship in which the Personal Data Owner is part of it or when it is Personal Data that derives from a scientific or professional relationship of the owner and is necessary for its development or compliance.

e) When Personal Data Processing related to health is carried out and is necessary, in risky circumstances, for the prevention, diagnosis and medical or surgical processing of the owner, provided that such Processing is carried out in health establishments or by professionals in the science of health, observing professional secrecy; or when there are reasons of public interest provided by law or when they shall be treated for reasons of public health, both reasons shall be classified as such by the Ministry of Health; or to carry out epidemiological or similar studies, as long as appropriate dissociation procedures are applied.

f) When the Processing is carried out by non-profit organizations whose purpose is political, religious or related to a union and refers to the Personal Data collected from their respective members, which shall be related to the purpose for which their activities are limited and cannot be transferred without the consent of those.

g) When an anonymization or dissociation procedure has been applied.

h) When the Processing is necessary to safeguard the legitimate interests of the Personal Data Owner by the Data Controller or Data Processor.

i) When the Processing is for purposes linked to the system of prevention of money laundering and terrorist financing or others that respond to a legal mandate.

j) In the case of economic groups made up of companies that are considered obliged to report, in accordance with the regulations that regulate the Financial Intelligence Unit, that can be shared with each other of their respective clients for the purposes of money laundering and financing prevention. terrorism, as well as other regulatory compliance, establishing adequate safeguards on the confidentiality and use of the information exchanged.

k) When the Processing is carried out in a constitutionally valid exercise of the fundamental rights to freedom of information.

l) When the Processing or Transfer is in compliance with a national or international standard (e.g. delivery of information to the FIU by the rules on prevention of money laundering and terrorist financing, to MINTRA by the rules of safety and health at work, SUNAT or the IRS (USA) for FATCA regulations, etc.).

m) Others established by law, or by the regulations granted pursuant to the Personal Data Protection Law.

7.5. Supplier and business partners contracting

The Credicorp Group Companies must include a clause on Personal Data protection in the contracts they sign with their suppliers when the latter have access to Personal Data of Users, clients or collaborators of the company. Such suppliers may provide specific services on behalf of and on behalf of the Company (data processor) or information sales services (enrichment supplier).
Likewise, in the face of any subcontracting that the suppliers -as data processors- may perform, the Credicorp Group Companies shall keep the responsibility for the processing of Personal Data.

In this sense, the Personal Data protection clauses may be the following, according to the type of contracting:

a) For the case of a relationship with a data processor, in which one of the Credicorp Group Companies transfers personal data to the provider (processor), the Personal Data protection clause shall contain the following information:

- Commitment to comply with the rules regarding personal data by the supplier.
- Possibility of carrying out audits to the supplier in order to verify compliance with the obligations assumed in terms of protection and processing of personal data.
- Commitment to maintain the confidentiality of the information submitted.
- Commitment to eliminate the information transferred once the contractual relationship has ended.

- Indication to transfer any ARCO rights request submitted to the person in charge to the Credicorp Group Company with whom the contract was entered into immediately and within a term no longer than 3 business days.
- Prohibition to subcontract to another company without express written authorization from the Credicorp Group Company.
- Indication to immediately report any security incident related to the personal data that was shared with you.

b) For the case of a relationship with a data enrichment provider, in which one of the Credicorp Group Companies acquires personal data, the Personal Data protection clause shall contain the following information:

- Acknowledgement that it is the supplier who obtains the data provided to the company being solely responsible for its legality.
- Statement that the provider has obtained the required Consents, authorizations, and permissions under Personal Data regulations prior to the Transfer, or, alternatively, falls under one of the exceptions provided for in the Data Protection Law.
- Commitment by the provider to make all necessary efforts to ensure that the information to be transferred corresponds to the Data Subject whose data enrichment has been requested.
- Right to verify whether providers have obtained the Data Subject's Consent to share the information (e.g., through sampling).
- Right to request documentary evidence regarding the origin of the acquired information (verification of lawful sources).

c) In the case of commercial partnership agreements, where Business Partners transfer Personal Data between each other:

- Commitment by the Business Partners to comply with Personal Data Protection regulations.
- Commitment to delete the transferred information once the contractual relationship has ended.
- Prohibition on subcontracting another company without the express and written authorization of the Business Partner.
- Declaration that the Personal Data or information used to execute the commercial partnership has been lawfully obtained in accordance with Personal Data Protection regulations.
- Statement that both parties are authorized to use and process the Personal Data for the purpose of executing the commercial partnership, as well as to transfer it to the Business Partner.

When the commercial partnership involves the exchange of Personal Data of users, clients, or employees, the Credicorp Group Company shall include an additional Personal Data Protection clause in the agreement, under which both parties commit to comply with Personal Data Protection regulations. Likewise, contracts entered into between Credicorp Group Companies must also include a Personal Data Protection clause whenever any of them has access to the users', clients', or employees' data of the other party.

Furthermore, when Business Partners agree to exchange Personal Data, it must first be verified that the Data Subject's Consent has been obtained for such Transfer, unless the

exchange is necessary for the execution of a contractual relationship entered into with the Data Subject.

Similarly, secure channels and mechanisms for the transfer of information must be agreed upon with Business Partners in order to ensure the security, integrity, and confidentiality of the transferred Personal Data.

7.6. Processing of Personal Data of Minors

The Companies of the Credicorp Group will only process the Personal Data of minors under fourteen years age with the prior Consent of their parents or guardians. In this sense, minors are not authorized to provide their personal data throught the website without their parent´s or guardian's permission. Parents and guardians will be held responsible for all the acts carried out by the minors in their charge.

In the case of persons over fourteen and under eighteen years of age, according to their capacity, they may grant consent for the processing of their personal data provided that the information provided has been expressed in a language understandable to them, in accordance with the relevant regulations.

The Credicorp Group Companies that carry out information processing in platforms or services in the digital environment make reasonable efforts to verify the identity of those who grant consent and the age of the same taking into account the available technology.

7.7. Processing of Personal Data by means of video-surveillance system

The Credicorp Group Companies shall carry out the Processing of Personal Data collected by means of video surveillance systems only for purposes related to security and/or labor control, in accordance with the applicable rules.

In order to comply with the proportionality principle, the Processing of Personal Data must be adequate, pertinent and not excessive in relation to the purposes that justified its collection. Under no circumstances shall recording or sound recording systems be placed in places intended for employees' rest or recreation, such as locker rooms, toilets or similar.

In all cases, Users and employees must be informed of the capture and/or recording of images and/or sounds. This measure is complied with by displaying informative signs in all video-monitored areas, as well as by making available to the Personal Data Subjects an additional information sheet with the information required by article 18 of the Law.

The scope of the location and contents of the informative posters should consider the guidelines established in Directive No. 01-2020-JUS/DGTAIPD, Directive for the processing of personal data through video surveillance systems.

The Holder of the Personal Data Bank shall register the video-surveillance Data Bank before the National Authority for the Protection of Personal Data and shall store the personal data for a term of thirty (30) days and up to a maximum term of sixty (60) days, unless otherwise provided for in sectorial rules.

The Credicorp Group Companies may employ persons in charge who shall carry out Personal Data Processing on behalf of the companies, in which case a contract/agreement/ document shall be formalized where the object and purposes of the Processing are established as well as the confidentiality obligation, the obligations related to security measures, the prohibition to process Personal Data for purposes other than those set forth in the contract and other

obligations set forth in the LPDP. The Personal Data that we capture through video surveillance systems will not be transferred to third parties, unless we have the prior and express consent of the owners, it is required by a competent authority and / or there is a legal obligation that authorizes it.

The Credicorp Group Companies must ensure the confidentiality of the Personal Data captured by means of video surveillance systems for which they must prohibit access to non-authorized personnel and establish confidentiality agreements with the personnel who control or will have access to the video surveillance systems.

In compliance with the principle of security, the Holder of the Personal Data Bank must adopt the necessary technical and organizational measures to guarantee the security of the data and avoid its alteration, loss, unauthorized Processing or access.

7.8. Security measures

The Data Controller shall implement the corresponding security measures according to the type of Information Asset that supports the Personal Data. Credicorp group Companies shall ensure compliance with the General Corporate Information Security Policy and other internal policies regarding the processing of Information Assets and related risks.

These policies contain guidelines to ensure compliance with the Personal Data Protection Standards, ensuring adequate:

a) Access Control (who can access it? When? From where? What can you do?)

b) Secure storage of Personal Data (backups, areas with protected access).

c) Secure transfer of Personal Data outside the Credicorp Group Companies (authorized means of transport, security measures such as encryption to prevent unauthorized access, loss or corruption of information during transit).

d) Secure transfer of Personal Data to prevent access or manipulation.

e) Protection of Personal Data in physical documents (copy or reproduction of documents, custody, transfer, destruction).

In addition, the Personal Data Bank Holder must have a security document which must be formally approved and dated and must contain at least the procedures for access management, privilege management and periodic verification of the privileges assigned to the information systems, including technological platforms, mobile applications, database engines, among others, used to process personal data. The security document is mandatory for all employees who have access to information systems.

Likewise, in order to comply with the said guidelines, the Personal Data Bank Holder must implement technical measures aimed at applying technological processes that restrict access to personal data only to collaborators and users when its processing is necessary and guarantees the integrity and security of the same.

In the event of a personal data security incident that (i) generates exposure to large volumes of personal data, (ii) may affect a large number of people, (iii) when it involves sensitive data or (iv) when there is an evident damage to other rights or freedoms, the Data Authority must be notified within 48 hours after becoming aware of it.

If the notification is made after 48 hours, it must include detailed justification and/or supporting evidence explaining the delay, even if the incident has been remedied or resolved internally.

The notification of the security incident must state and describe at a minimum (i) the nature of the security incident, (ii) the name and contact details of the Personal Data Oficial or other point of contact, (iii) the potential consequences of the incident, and (iv) the steps taken or proposed to be taken to remedy the security breach.

In addition, if a personal data security incident is noticed that affects the data subject in other of his or her rights, it must be communicated within 48 hours in plain and clear language, as well as of the measures taken to mitigate its effects. If the communication is made after 48 hours, the delay must be justified.

In the event that the security incident takes place in the digital environment, the notification must also be made to the National Digital Security Center in accordance with the provisions of Emergency Decree 7-2020.

7.9. Attention to Protected Rights

The companies of the Credicorp Group shall guarantee and heed the attention to the protected rights that the Owner of the Personal Data may exercise. To do this, they shall keep channels, procedures and information available to deal with requests within the terms established by the Personal Data Protection Regulations.

In the event that the request for the exercise of protected rights is submitted to the person in charge of the personal data, such person is obliged to immediately or within a maximum of three (3) days forward such request to the Credicorp Group Company with which he/she has contracted.

The rights that the Personal Data Owner can exercise are:

a) Access / Information

The right of access is the right to be informed about the Personal Data included in the Data Bases of the Credicorp Group Company, as well as the conditions and generalities of the Processing and Transfer thereof.

The right to information is the right of the Personal Data Owner to be informed about the purpose(s) for which his or her Personal Data will be processed, with whom the Personal Data may be shared, the existence of the Personal Data Base in which Data Controllers store the personal data and the identity and address of the Data Controller. The Personal Data Owner also has the right to know, if applicable, who is the Data Processor, whether there will be Transfers of the Owner's Personal Data and if so, to whom, and the consequences of providing the Personal Data to Credicorp and the consequences of refusing to provide it. In addition, the Personal Data Owner has the right to know how long the Personal Data will be maintained and how the Personal Data Owner may exercise all of his or her privacy rights under law.

b) Rectification / Update

The Personal Data Owner has the right to update, add to, or otherwise modify his or her Personal Data. This right applies with respect to data that is partially or totally inaccurate, incomplete, erroneous, false or out of date. The Owner of Personal Data shall specify the data that is wanted to be rectified, updated and/or included, as well as the correction and / or incorporation that needs to be carried out by the Credicorp Group company and shall

attach supporting documents, as needed, to demonstrate that the requested rectification and / or addition is appropriate.

c) Cancellation / Supression

The Personal Data Owner has the right to request that a Data Controller holding the Personal Data of the Owner delete or otherwise remove, in whole or in part, his / her Personal Data maintained by the Data Controller. Such a request must be granted if the Personal Data of the Owner has ceased to be necessary or relevant for the purpose that it was collected by the Data Controller, provided that: (i) the term for Credicorp's Processing of the Personal Data has expired, (ii) the Personal Data Owner has decided to revoke his or her Consent for the Processing, or (iii) the Processing does not comply with the Personal Data Protection Rules.

The Data Controller shall inform the Owner of Personal Data that his/her deletion/removal request will not be granted when his/her Personal Data is necessary to execute the contractual relationship that is maintained with the Credicorp Group company or when the Personal Data shall be kept during the periods provided in the current legal provisions, or when the Personal Data are kept by virtue of historical, statistical or scientific reasons in accordance with applicable legislation.

d) Opposition

The Personal Data Owner has the right to oppose the placement of his or her Personal Data in a Personal Data Base of responsibility of the Credicorp Group Company or to the Processing of the Owner's Personal Data when the Personal Data Owner either (i) has not consented to the collection of the Personal Data because the Personal Data have been collected from sources of public access or (ii) having given his or her consent, the Personal Data Owner proves there are legitimate and founded reasons related to a specific personal situation that justifies the exercise of this right.

e) Portability of Personal Data

The Personal Data Subject may request to receive the data about himself/herself that he/she has provided to a data controller, in a structured, commonly used and machine-readable format, and to transmit it to another data controller or personal data bank owner when: (i) the processing is based on consent or on a contractual relationship to which the data subject is a party; or, (ii) the processing is carried out by automated means.

Derived, inferred or constructed data -i.e., those data that have undergone at least one personalization, categorization or profiling process- may be subject to portability whenever the Credicorp Group Company so determines.

When exercising data portability, the data subject is entitled to have his/her data transmitted directly from one data controller or data bank owner to another when this is technically possible. This does not imply that an excessive or unreasonable financial or technical burden is imposed on Credicorp Group Companies.

The transfer of this information must be carried out through an automated means that guarantees the security and integrity of the information.

f) Objective processing of Personal Data

The Personal Data Subject has the right not to be subject to decisions, automated or not, that produce legal effects, discrimination or significantly affect him/her, including those based solely on automated processing aimed at evaluating, analyzing or predicting, without human intervention, certain personal aspects of him/her. For example, his or her professional performance, economic situation, health status, sexual orientation or identity, among others. Exceptions are those cases in which this occurs within the framework of the negotiation, conclusion or execution of a contract or in cases of evaluation for the purpose of incorporation to a public entity.

When personal data are processed as part of a decision-making process without the participation of the Personal Data Holder, the Credicorp Group Company must inform this processing to the holder as soon as possible. The Personal Data Subject must be in all cases in the possibility of defending his/her point of view on the decisions made on the basis of his/her personal data in order to safeguard his/her legitimate interest, without prejudice of exercising the other rights set forth in this section.

7.10. Registry of Personal Data Bases and Communication of Cross-Border Transfer

The Companies of the Credicorp Group are obliged to register the Personal Data Bases under their responsibility in the National Registry of Personal Data, administered by the General Directorate of Protection of Personal Data (DPPD) of the Ministry of Justice (MINJUS), and to declare whether the Personal Data Bases consist of physical (files, warehouses) or digital (applications, Excel, Access, etc.) support, and to communicate the Cross-Border Transfers that each Credicorp Group company carries out.

In this sense, the Credicorp Regulatory Compliance Officer or the respective managers in the Credicorp Group Companies shall be informed about the existing Personal Data Bases that are identified and that have not been registered with the MINJUS, or that any area will create through an initiative, project, new product, new channel or new service, among others, who will analyse if that Personal Data Base is part of some other base already registered or if it requires registering as a Parent Personal Data Base. In the same way, the Credicorp Regulatory Compliance Officer or the respective managers in the Companies of the Credicorp Group shall be informed of the international transfers of Personal Data that will be carried out so that communication can be made to the DPPD about Cross-Border Transfers of Personal Data.

In accordance with the principle of adequate level of protection, in order to transfer personal data abroad, Credicorp Group Companies must guarantee a sufficient level of protection for the processing to be applied, which is at least equivalent to that provided for in Peruvian regulations or international standards on the matter.

7.11. Processing of biometric data

The Data Controller of the Personal Data Bank must only process biometric data when it is proportional, strictly necessary and not excessive with the purpose of the processing.

The processing of biometric data is subject to the rules of consent and the exceptions set forth in the Personal Data Protection Law and its Regulations (sections 6.2 and 6.3 of this document). However, since it is a sensitive data, if the processing requires the consent of the biometric data holder, this consent must be obtained by Credicorp Group Company through a

written means such as, for example, a click of acceptance in a website or an electronic signature.

This treatment deserves, due to its sensitivity, a higher level of protection. Therefore, it is the obligation of the Credicorp Group Companies to establish, implement and maintain technical, organizational and legal measures necessary and sufficient to guarantee the security of the biometric data in its maximum expression, avoiding its alteration, loss, treatment or unauthorized access.

In this sense, according to the biometric data processing to be carried out, the Credicorp Group Companies shall define the security measures aimed at guaranteeing, during the whole cycle of the biometric data processing, the availability, integrity and confidentiality of the personal data they manage, in order to avoid their adulteration, loss or unauthorized processing.

7.12. Personal data protection impact assessment

The Impact Assessment related to the protection of personal data is a proactive accountability mechanism that allows the owner of the personal data bank or the data controller to analyze in advance the risks associated with the handling of such information. This analysis, which is optional, aims to mitigate possible negative impacts and can function as an administrative liability mitigator.

This assessment is performed prior to the processing of personal data, especially in cases of sensitive information, processing for profiling purposes, data of persons in vulnerable situations (such as minors, members of indigenous peoples in isolation or initial contact, or persons with disabilities), processing of large volumes of data, or any other case indicated by the National Authority for the Protection of Personal Data.

7.13. Additional Considerations on Cognitive and Generative Artificial Intelligence

In the case of initiatives promoted within Credicorp Group Companies aimed at implementing a specific action—such as modifying a process, launching a project, changing a product, or introducing a new product—using Artificial Intelligence components, the principles and guidelines on privacy and security established in the Corporate Responsible Artificial Intelligence Policy must also be taken into account. These principles ensure the privacy, proportionality, and objective processing of Personal Data.

Terms written in uppercase and not defined in this policy are defined in the Corporate Responsible Artificial Intelligence Policy.

8. Presentation of reports of potential violations of the Personal Data Protection Regulations and warning signs

The employee of a Credicorp Group Company shall inform the Credicorp Regulatory Compliance Officer, the respective managers in Credicorp Group Companies, their immediate superior manager, or anonymously through the Credicorp Genetic Alert system of any illegal act or breach of this Corporate Policy designed to guarantee compliance with the Personal Data Protection

Regulations. The headquarters that receive any complaints from their employees should redirect them to the Compliance unit of the Credicorp company. Each company will adopt the necessary measures to protect the confidentiality of any report, subject to the law, regulations or legal procedures.

Companies are strictly prohibited from retaliating against employees who, in good faith, report or participate in reporting any unlawful act or breach of this Corporate Policy. It should be noted that any employee who engages in retaliation will be subject to disciplinary sanctions.

9. Disciplinary measures

Violations of this Corporate Policy or lack of cooperation with an internal investigation may lead to the application of disciplinary sanctions depending on the severity of the case, which may lead to the separation of a Credicorp Group Company employee from his/her duties, in accordance with labour legislation; without prejudice to civil and criminal actions that may correspond.

Document approved by:
Credicorp Directory held in session of 29/09/2021 and 16/04/2025
Management of the Corporate Security Area
Management of Legal Division and General Secretariat
Management of Data & Analytics Division
Chief Data Officer Credicorp
Non-Financial Risk Division Management
Corporate Chief Compliance Officer