Credicorp Compliance and Ethics
Personal Data Protection Program (PDP)
Personal Data Protection Corporate Policy
Effective date: 07/12/2018
Date of Publication: 06/12/2018

1. General objectives

Credicorp Group companies are committed to the protection and privacy of Users' Personal Data in compliance with the Peruvian Law on Protection of Personal Data - Law No. 29733, its regulations approved by Supreme Decree No. 003-2013-JUS and their respective amendments ("Personal Data Protection Rules"). Consistent with this, this Corporate Policy aims to:

a) Establish the general guidelines for the Processing and Transfer of Personal Data of individuals, such as employees, Users (as defined below), clients, and suppliers, with respect to all the companies of the Credicorp Group.

b) Ensure that the companies of the Credicorp Group comply with the Personal Data Protection Rules.

c) Make all the employees of the Credicorp Group companies aware of the impact of non-compliance with the Personal Data Protection Rules.

2. 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.

a) **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.

b) **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 and access.

c) **Consent:** authorization of the Owner of the Personal Data for the Data Controller to Process and / or Transfer the data.

d) **DPDP:** Directorate of Personal Data Protection

e) **Personal Data:** that numerical, alphabetical, graphic, photographic, acoustic information, about personal habits, or of any other type concerning to an individual, that identifies the individual or makes him or her identifiable directly or indirectly through means that can be reasonably used. 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.

f) **Sensitive Data:** Personal Data referring to physical, moral or emotional characteristics, facts or circumstances of an individual's affective or family life, personal habits of the most intimate circle, information related to physical or mental health, biometric data that by themselves comprise Personal

Data, data referring to racial and ethnic origin, income, political, religious, philosophical or moral opinions or convictions, union affiliation, information related to health or sexual life.

g) **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.

h) **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.

i) **Credicorp Group companies**: local Credicorp Group companies such as Banco de Crédito del Perú, Mibanco, Prima AFP, Pacífico Seguros, Pacífico Asiste and Credicorp Capital Perú and its subsidiaries (Credicorp Capital SAB, Credicorp Capital Sociedad Titulizadora and Credicorp Capital Servicios Financieros).

j) **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.

k) **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 at the direction of the Data Controller. Such person includes whoever performs the processing without the existence of a Personal Data Base.

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

m) **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.

n) **Personal Data Owner:** individual to whom the Personal Data pertains.

o) **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.

p) **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.

q) **Users**: individuals who can make use of certain services offered by the companies of the Credicorp Group without having to be clients or who have any signed contract with the company. E.g.: individuals who pay for electricity or water services at the BCP, who enter a company's sales office to request information about the products it offers, etc.

3. 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.

These are outside the scope of the Personal Data Protection Rules:

- The Processing carried out on information supplied by a legal person.
- A Personal Data Base created by individuals for exclusively domestic purposes or related to their private or family life.
- Public administration data bases, when processing of Personal Data is necessary for the fulfilment of the powers assigned by law for national defence, public security and for the development of activities in criminal matters for the investigation and suppression of crime.

4. Responsibilities

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.
- Ensure the BCP Credicorp Regulatory Compliance Officer performs the function of the representative of the Data Controller before the DPDP. In the case of the other companies of Credicorp group, the General Management will appoint a representative.

d) According to the Corporate Information Security Policy, the Parent Company`s Information Security Officer (BCP) or the Information Security Officer in each Credicorp Company,should:

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 on 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.

e) All employees of each of the Credicorp Group companies shall comply with the Personal Data Protection Rules and this Corporate Policy, for which they shall take into account the policies established by the Corporate Compliance Division of each Credicorp Company.

5. 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 will prevail.

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

6. Guidelines / Policies

6.1. 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.

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. A Consent is considered valid only if it is provided directly by the Owner of the Personal Data himself/herself.

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

The Personal Data contained in a Personal Data Base shall be precisely adjusted to reality. The data directly provided by the Owner thereof is presumed to be 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.

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.

6.2. 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, the Consent shall 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 Personal Data Owner also should be informed whether he she must provide responses to any questionnaire asking for Personal Data, and what the consequences of providing or refusing to provide his or her Personal Data will be. In addition, the Personal Data Owner should be informed about the anticipated duration of the retention of his or her Personal Data, the possibility of Transfer of the Personal Data, and the rights that the Protection Law of Personal Data grants Personal Data Owner and the means through which the Personal Data Owner may exercise those rights.

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

According to article 14 of the Law on Protection of Personal Data, 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 collected or transferred for the exercise of the functions of public entities within the scope of their powers.

b) 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 Centres, etc.)

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

d) 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.

e) 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.

f) 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.

g) 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.

h) When an anonymisation or dissociation procedure has been applied.

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

j) 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.

k) 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.

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

m) 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.).

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

6.4. Supplier contracting

Credicorp Group companies shall incorporate a Personal Data protection clause in the contracts they sign with their suppliers when the latter have access to data from Users, clients or employees of the company, which may vary according to the following details:

a) General clause of suppliers.

b) Clause for Collection providers.

c) Clause for contracts for the acquisition of databases.

d) Clause for Credicorp company database enrichment contracts.

In the case of a commercial alliance with the exchange of Personal Data of Users, clients or employees, the Credicorp Group company will include another type of clause for the protection of Personal Data in the Contract, by which both parties are obliged to comply with the Protection Rules of Personal information. In the same way, the contracts that the companies of the Credicorp Group have between them shall also include a clause for the protection of Personal Data when any of them has access to data of Users, clients or employees of the counterpart.

6.5. Processing of Personal Data of Minors

The companies of the Credicorp Group will only process the Personal Data of minors 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 guardiant´s permission. Parents and guardians will be held responsible for all the acts carried out by the minors in their charge.

6.6. 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 shall 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).

6.7. 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.

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 / Suppression

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.

a. Revocation

The Personal Data Owner has the right to revoke his/her consent for the Processing of his/her Personal Data at any time, without previous justification and provided that said processing is carried out for purposes additional to those for which Processing is authorized as a matter of law. In this sense, the revocation request will not be granted if the Personal Data is necessary for the execution of the contractual relationship that the Owner of the Personal Data maintains with the Credicorp Group company, nor if such company shall keep the Personal Data for historical, statistical or scientific in accordance with applicable legislation. In these cases, without prejudice to the exercise of the right of revocation, the Data Controller will keep the corresponding information for the period provided in the current legal provisions.

6.8. Registry of Personal Data Bases and Communication of Cross-Border Transfers

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.

7. 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 either prepare reports in good faith and / or participate in reporting any illegal act or breach of this Policy. It should be noted that any employee who retaliates will be subject to disciplinary sanctions.

8. 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 12/20/2017	
Bárbara Falero	Corporate Chief Compliance Officer
José Marangunich	Management of the Corporate Security Area
David Saenz	Management of the Information Technology Division
Guillermo Morales	Management of Legal Division and General Secretariat
Leandro Rocha	Management of Data & Analytics Division