

PRIVACY AND PERSONAL DATA PROTECTION POLICY

ÍNDICE

I.	General Information	3
II.	Objective	3
III.	Scope	3
IV.	Definitions	3
V.	Policy	4
5.1	Consent and legitimization of the processing	4
5.2	Personal data: purpose of processing and scope	4
5.3	Guiding principles	5
5.4	Purposes of personal data	5
5.5	Data subjects' rights	6
5.6	Conditions for processing data	6
a.	Consent of the data subject.....	6
b.	Cases in which consent is not required.....	7
c.	Provision of information.....	7
d.	Duty to inform the data subject.....	7
e.	Revocation of authorization and/or suppression of data:.....	7
f.	Persons to whom the information may be provided:.....	7
g.	Cross-border data flows:.....	7
5.7	Security of personal data	8
5.8	Procedures	8
5.9	CREDIT REPORT's duties in the processing of data	9
5.10	Duties of the Data Processor	10
5.11	Security measures	10
5.12	Data retention	11
5.13	Policy modifications	11

PRIVACY AND PERSONAL DATA PROTECTION POLICY

I. General Information

Credit Report Latin American, hereinafter referred to as CREDIT REPORT, in the exercise of some of its internal and external operations collects, uses, manages, transfers, store and processes information, which may be associated with information belonging to physical persons in the development of its activities. This policy seeks to ensure adequate communication of its compliance, pursuant to Law No. 29733 on the Protection of Personal Data, as well as its regulations.

II. Objective

The purpose of this policy is to make known the way in which CREDIT REPORT protects the personal data of customers, suppliers, and employees, from its collection through the different channels of the organization, whether physical or digital.

If users decide to modify their personal data, this can be done through the forms provided, which can be found in the Annex to this policy.

Although this is a voluntary action, if you do not provide your personal data, CREDIT REPORT will not be able to process them for the purposes stated. Therefore, the provision of your personal data for these purposes is a requirement necessary for CREDIT REPORT to be able to meet requests for the services provided, communicate with citizens and/or carry out any other purposes specified in this document.

III. Scope

This policy applies to all personal data banks and/or files containing personal data that are processed by CREDIT REPORT.

IV. Definitions

- **Data Controller:** is the physical or legal person who, alone or together with others, determines the purposes and means of the processing of personal data, i.e., CREDIT REPORT will be responsible for the personal data obtained through its various collection channels and provided by CREDIT REPORT users, as well as the companies that are part of it (through services provided to the institution).
- **Personal Data Subject:** the person to whom the personal data shared and processed belong.
- **Personal data:** any information about an identified or identifiable physical person (the user), such as name, ID card number, passport, location data or one or more elements of a person's physical, physiological, genetic, psychological, economic, cultural, or social identity.
- **Processing:** any operation or set of operations performed upon personal data or sets of personal data (whether automated or not), such as collection, registration, organization, rectification, consultation, usage, distribution, or any other form of enabling access, collation or interconnection, restriction, suppression, or destruction of personal data.

- Right of access: this is the user's right to know what data CREDIT REPORT is processing and to obtain a copy of this data.
- Right to rectification: this is the user's right to update, rectify and/or correct his/her personal data.
- Right to object: this is the user's right to object at any time to the processing of his/her personal data by CREDIT REPORT.
- Right to erasure ("right to be forgotten"): this is the user's right to request the suppression of his/her data in any document, file, or place where they are accessible.
- Right to restrict processing: this is the user's right to demand that the processing of his/her data be limited when any of the circumstances established by law occur, such as the unlawful processing of the data or that CREDIT REPORT no longer needs it.

V. Policy

5.1 Consent and legitimization of the processing

CREDIT REPORT processes the user's data:

- (i) When they expressly consent to the processing of their personal data for the purposes detailed in this document and/or;
- (ii) When the processing is necessary to execute a contract for the provision of services and products to which the user is a part of.

5.2 Personal data: purpose of processing and scope

This policy applies to the personal data belonging to **customers and employees**, provided by them, using their freedom, voluntarily and consciously. The information collected and stored includes basic data entered through registration forms, contact forms or other similar forms, such as, for example, name, ID card number, passport, gender, age, telephone number, email address, country of residence, among other data collected through the various channels that the institution manages. Before sending their personal data, citizens will be able to see which data are essential for the correct provision of services and which will be of an ancillary nature.

Users are solely responsible for the truthfulness and accuracy of the data provided. Users may only be over 18 years old and/or those with sufficient legal capacity. Likewise, they shall be solely responsible for the data provided by third parties, as well as for guaranteeing that they have been informed of this Privacy Policy and have obtained their express consent.

5.3 Guiding principles

CREDIT REPORT will consider the following principles in the processing of personal data.

- a. **Lawfulness principle:** The processing of personal data in terms of Law 29733 is a regulated activity that must be subject to the provisions of the aforementioned law, and other provisions that regulate it. The collection of personal data by fraudulent, unfaithful, or unlawful means is prohibited.
- b. **Principle of consent:** In accordance with the principle of consent, the processing of personal data is lawful when the personal data subject has given his or her free, prior, express, informed, and unequivocal consent. Forms of consent in which consent is not directly expressed, such as those in which it is necessary to presume or assume the existence of a will that has not been expressed, are not admissible. Even consent given with other declarations must be stated expressly and clearly.
- c. **Principle of purpose:** In accordance with the principle of purpose, a purpose is considered to be determined when it has been clearly expressed, with no room for confusion, and when the purpose for which the personal data will be processed is objectively specified. In the case of personal data banks containing sensitive data, their creation can only be justified if their purpose, in addition to being legitimate, is specific and in accordance with the activities or explicit purposes of the holder of the personal data bank. Professionals who carry out the processing of personal data, in addition to being limited by the purpose of their services, are obliged to maintain professional secrecy.
- d. **Quality principle:** Personal data to be processed must be true, accurate and, as far as possible, up to date, necessary, relevant, and adequate in relation to the purpose for which they were collected. They should be kept in a form that ensures their security and only for as long as necessary to fulfil the purpose of the processing.
- e. **Proportionality principle:** Any processing of personal data must be adequate, relevant, and not excessive to the purpose of which the data were collected.
- f. **Security principle:** The personal data controller and the data processor must take the necessary technical, organizational, and legal measures to ensure the security of personal data. The security measures must be appropriate and in accordance with the processing to be carried out and the category of personal data concerned.
- g. **Principle of resource availability:** All personal data subjects must have the necessary administrative or jurisdictional means to claim and enforce their rights when these are violated by the processing of their personal data.
- h. **Principle of adequate level of protection:** For the cross-border flow of personal data, an adequate level of protection must be guaranteed for the personal data to be processed, or at least comparable to that provided for by law or international standards on the matter.

5.4 Purposes of personal data

CREDIT REPORT will use the personal data provided by the users for the following purposes:

Employees and collaborators:

- CREDIT REPORT will request personal information from its employees to comply with current labor regulation requirements and/or the development of projects related to human resources such as payroll registration, personnel attendance, personnel selection, benefits registration, among others.

Lessor services (physical persons such as suppliers):

- To manage the payment of services and products requested.
- To contact about the provision of the contracted services and products.

5.5 Data subjects' rights

The personal data subject will have the following rights:

- a. The personal data subject may only exercise the rights of information, access, rectification, cancellation, opposition, and objective processing of personal data, without prejudice to the rules governing representation.
- b. The exercise of one or some of the rights does not exclude the possibility of exercising one or some of the others, or may it be understood as a prerequisite for the exercise of any of them.
- c. To know, update and rectify its personal data before **CREDIT REPORT** or the designated data processor. This right may be exercised, among others, against partial, inaccurate, incomplete, divided, misleading data or data whose processing is expressly prohibited or has not been authorized.
- d. To be informed by **CREDIT REPORT** or designated data processor, upon request, of the use it has made of his or her personal data.
- e. To revoke authorization and/or request the deletion of the data when processing does not respect the constitutional and legal principle, rights and guarantees. The revocation and/or deletion will proceed when the National Authority of Personal Data Protection has determined that in the processing **CREDIT REPORT** or the designated data processor, have incurred in conduct contrary to Law 29733 and the Constitution.
- f. To have Access, free of charge, under the conditions set in this document, to their personal data that have been processed.

5.6 Conditions for processing data

- a. Consent of the data subject:

For **CREDIT REPORT** to carry out any personal data processing action, the prior and informed authorization of the data subject is required, which must be obtained by any means available for subsequent consultation. These mechanisms may be predetermined through technical means that facilitate the data subject its automated manifestation or may be in writing or orally with the recording and storage of the corresponding evidence.

CREDIT REPORT will adopt the necessary procedures to request, at the latest during data collection, the data subject's consent to the processing of the data and will inform the data subject of the personal data to be collected, as well as the specific purposes of the processing for which consent is obtained.

Personal data held in publicly accessible sources may be processed by **CREDIT REPORT** if they are by nature public data.

In case of substantial changes in the content of **CREDIT REPORT's** data processing policies, regarding the identification of the data controller and the purpose of the processing of personal data, which affect the content of the authorization, **CREDIT REPORT** shall communicate these changes to the data subjects, before or at the latest at the time of implementing the new policies, and shall obtain a new consent from the data subject when the change refers to the purpose of the processing. For the communication of changes and authorization, technical means may be used to facilitate this activity.

b. Cases in which consent is not required

- Information required by a public or administrative body in the exercise of its legal functions or by court order.
- Data of public nature.
- Cases of medical or health emergency.
- Processing of information authorized by Law for historical, statistical, or scientific purposes.
- Data related to the Civil Registry of Persons.

c. Provision of information

The information requested by the data subject will be provided by **CREDIT REPORT** in the same manner as the request was made.

d. Duty to inform the data subject

CREDIT REPORT, at the time of requesting the data subject's consent, shall clearly and expressly inform him/her of the following:

- The processing to which their personal data will undergo and the purpose of this.
- The optional nature of the response to the questions that are asked when they deal with sensitive data or data of children and adolescents.
- The rights that he or she has as the data subject.
- The identification, physical or electronic address and telephone number of the data controller.

e. Revocation of authorization and/or suppression of data:

Data subjects may at any time request **CREDIT REPORT**, the suppression of their personal data and/or revoke the authorization granted for the processing of these, by submitting a request, in accordance with the provisions of Law 29733 of 2011 and the regulations of DS No. 003-2013-JUS of 2013.

The request for suppression of information and the revocation of authorization shall not proceed when the data subject has a contractual duty to remain in **CREDIT REPORT's** database.

f. Persons to whom the information may be provided:

Information about personal data that has been processed by **CREDIT REPORT** may be provided to the following persons:

- To the data subjects, their successors in title or their legal representatives.
- To public or administrative entities in the exercise of their legal functions or by court order.
- To third parties authorized by subject data or by law.

g. Cross-border data flows:

Information provided to **CREDIT REPORT** that could be stored or processed outside the national territory, in these cases the information security criteria defined and implemented by the institution ensure that such information is only shared through intermediaries with the same established level of security.

5.7 Security of personal data

CREDIT REPORT complies with the legally required personal data protection measures and has adopted the measures reasonably required according to current technical knowledge and good practices for the custody and management of information in order to prevent the loss, misuse, alteration, unlawful intrusion and theft of personal data provided by users.

5.8 Procedures

The data subject or his/her successors in title have the right to submit queries and/or complaints to CREDIT REPORT, prior verification of their identity, by writing to the following address at any time, to withdraw their consent to the processing of their personal data and/or to exercise their rights of Access, information, rectification, opposition, deletion, limitation, oblivion, portability and not to be object of individualized decisions, by writing to CREDIT REPORT with the subject "PERSONAL DATA" to the following addresses:

- Physical/legal address: Calle Enrique Palacios 360, piso 4 Miraflores, Lima
- E-mail: datospersonales@crlacorp.com

CREDIT REPORT will respond to the query and/or complaint by the same means by which it was made:

a) **Queries (Access / Information)**

The data subjects or their successors in title may consult the personal information of the data subject contained in the database of **CREDIT REPORT**, who will provide the applicant with all the information contained in its databases, linked to the identification of the data subject.

The data subject may consult his or her personal data free of charge every time there are substantial modifications in **CREDIT REPORT's** data processing.

Any consultation will be answered by the same means by which they were made within 05 working days of their submission. To exercise the right, the data subject or his/her successors in title must submit the Access form, which can be found in the Annex to this policy.

b) **Complaints (Applications / Requests)**

The data subject or their successors in title who consider that the information contained in a database should be subject to rectification, cancellation, or opposition, or when they notice the alleged breach of any of the duties contained in Law 29733 of 2011, may submit a request to the Holder of the personal data bank or to the Data controller of **CREDIT REPORT**.

If the information provided in the request is insufficient or erroneous in a way that does not allow its attention, **CREDIT REPORT** may require, within seven (7) days of receiving the request, additional documentation to the personal data subject to address it (Article 56 of the regulations).

Within ten (10) days of having received the request, counted from the day following its receipt, the personal data subject shall attach any additional documentation that he/she deems relevant to support his/her request. Otherwise, the request shall be deemed not to have been received.

The maximum response times for complaints in accordance with the regulations of the law are as follows:

- The right to information shall be five (05) days from the day following the submission of the corresponding request.
- The right of access shall be twenty (20) days from the day following the submission of the request by the personal data subject.
- Rights of rectification, cancellation or opposition, the maximum period for response by the personal data subject bank or data controller shall be ten (10) days from the day following the submission of the corresponding request.

Except for the time limit established for the exercise of the right to information, the time limits corresponding to the response or attention of the other rights may be extended only once, and for an equal period, at the most, if the circumstances justify it. The justification for the extension of the deadline must be communicated to the personal data subject within the period to be extended.

c) **Requirement of applicability**

The data subject or successors in title may only submit a complaint to the National Authority for the Protection of Personal Data once they have exhausted the consultation or complaint procedure before **CREDIT REPORT**.

5.9 CREDIT REPORT's duties in the processing of data

- Guarantee the data subject, at all times, the full and effective exercise of the right of habeas data.
- Request and keep, under the conditions provided by law, a copy of the respective authorization granted by the data subject.
- Duly inform the data subject about the purpose of the collection and the rights he/she is entitled to by virtue of the authorization granted.
- Take measures aimed at preserving the information under the security conditions to prevent its falsification, loss, consultation, use or unauthorized or fraudulent access.
- Take measures to ensure that the information provided to the Data Controller is truthful, complete, accurate, up-to-date, verifiable, and comprehensible.
- Update the information, communicating in a timely manner to the Data Processor, all developments with respect to the data previously provided and take other necessary measures to ensure that the information provided to the Data Processor is kept up to date.
- Rectify the information when it is incorrect and communicate what is relevant to the Data Processor.
- Provide the Data Processor, where appropriate, only with data whose Processing has been previously authorized in accordance with the provisions of the Law.
- Demand that the Data Processor at all times respect the conditions of security and privacy of the Data Subject's information.
- Process queries and complaints filed under the terms set forth in the law.

- Adopt an internal manual of policies and procedures to ensure proper compliance with this law and, especially, to process queries and complaints.
- Inform the Data Processor when certain information is under discussion by the Data Subject once the claim has been filed and the respective process has not been completed.
- Inform the Data Controller, upon request of the Data Subject, about the use given to his or her data.
- Inform the National Authority for the Protection of Personal Data when there are violations to the security policies and there are risks in the administration of the Data Subjects' information.
- Comply with the instructions, requirements and recommendations issued by the National Authority for the Protection of Personal Data.

5.10 Duties of the Data Processor

Data processors shall comply with the following duties without prejudice to the other provisions of the Law and other provisions governing their activity:

- Guarantee the Data Subject, at all times, the full and effective exercise of the right to habeas data.
- Take measures to keep the information under the necessary security conditions to prevent its falsification, loss, consultation, unauthorized or fraudulent use or access.
- Timely update, rectify or delete data under the terms of this law.
- Update the information reported by the data controllers within five (5) working days of its receipt.
- Process queries and complaints made by Data Controllers under the terms set forth in the Law.
- Adopt an internal manual of policies and procedures to ensure proper compliance with the Law and, especially, to handle queries and complaints from Data Subjects.
- Refrain from circulating information that is being disputed by the Data Subject and whose blocking has been ordered by the National Authority for the Protection of Personal Data.
- Allow access to the information only to those persons who may have access to it.
- Inform the National Authority for the Protection of Personal Data when there are violations to the security policies and there are risks in the administration of the information of the Data Subjects.
- Comply with the instructions and requirements issued by the National Authority for the Protection of Personal Data.
- Safeguard the security of the databases containing Personal Data.
- To maintain confidentiality concerning the Processing of Personal Data.

5.11 Security measures

CREDIT REPORT takes all reasonable precautions and measures of a technical nature aligned with the good practices provided by the ISO 27001:2013 standard by implementing in the institution an Information Security Management System - ISMS, in order to ensure the security of the personal data of the Data Subjects, mainly those aimed at preventing their modification, loss and unauthorized processing or access.

The application of security measures is intended to ensure the conservation, confidentiality, integrity, and availability of the data.

CREDIT REPORT's security guidelines are supported by information security policies built under the best practices and existing security standards and in compliance with current regulations.


These policies are strictly complied with by direct and indirect employees, service providers and suppliers, who work within **CREDIT REPORT**.

5.12 Data retention

CREDIT REPORT will keep the personal data of the users for different periods depending on the purpose of the processing. Therefore, the data will be kept for as long as a contractual relationship for the provision of products and services between **CREDIT REPORT** and the users is in force and/or as long as the users do not request the deletion of the personal data. Likewise, users understand and accept that certain personal data must be kept by **CREDIT REPORT** in accordance with legal regulations and in accordance with the terms established by law.

5.13 Policy modifications

CREDIT REPORT may make changes and update this policy according to latest changes or legislative or jurisprudential requirements and/or the needs of the institution, among others; therefore, users are advised to review this policy regularly and/or each time they access the website.



Juan Isaac Rodríguez Gutiérrez
CREDIT REPORT
LATINAMERICAN S.A.C.
Gerente General