

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

1. OBJECTIVE

The objective of this policy is to serve as a tool for upholding everyone's constitutional right to know, update, and rectify information collected about them in databases or files, and the other constitutional rights, freedoms, and guarantees referred to in Article 15 of the Political Constitution, as well as the right to information enshrined in Article 20 thereof.

Executive summary

BLC Colombia S.A.S. is committed to protecting the privacy of the personal data it processes (employees, clients, business partners, and other identifiable individuals). BLC Colombia S.A.S.'s policies, guidelines, and actions support this commitment to Personal Data protection.

Each employee is personally responsible for complying with this Policy as part of fulfilling their responsibilities at BLC Colombia S.A.S. In summary, the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership is prohibited, as is the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, health-related data, or data concerning a natural person's sex life or sexual orientation, except in specific cases established by law.

Therefore, in compliance with the constitutional guarantees enshrined in Article 15 of the Political Constitution regarding everyone's right to personal and family privacy, and the ability to know, update, and rectify information collected about them in databases and files of public and private entities, BLC Colombia S.A.S. presents the following Personal Data Protection Policy to all stakeholders, in accordance with the guidelines set out in Law 1581 of 2012 and its implementing decrees.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

2. SCOPE

The principles and provisions contained in this policy apply to personal data recorded in any database that makes such data subject to processing by private entities.

The personal data protection framework does not apply to:

- a) Databases or files maintained exclusively for personal or household purposes. When these databases or files are to be provided to third parties, the Data Subject must be informed and their authorization requested beforehand. In this case, the controllers and processors of the databases and files will be subject to the provisions of Law 1581 of 2012.
- b) Databases and files intended for national security and defense, as well as the prevention, detection, monitoring, and control of money laundering and terrorist financing.
- c) Databases intended for and containing intelligence and counterintelligence information.
- d) Databases and files containing journalistic information and other editorial content.
- e) Databases and files regulated by Law 1266 of 2008. ¹
- f) Databases and files regulated by Law 79 of 1993. ²

1. Establishing general provisions on habeas data and regulating the handling of information contained in personal databases, particularly financial, credit, commercial, service-related information and information originating in third countries, and issuing other provisions.

2. LAW 79 OF 1993 (October 20) (Repealed by Art. 58 of Law 2335 of 2023, except for Art. 5) Regulating Population and Housing Censuses throughout the national territory.

3. DEFINITIONS

The following definitions are enshrined in Law 1581 of 2012 and provide an understanding of each of the topics addressed in this document:

Processing:

Any operation or set of operations performed on personal data, such as collection, storage, updating, use, circulation, or deletion.

Personal data:

Any information linked to or that may be associated with one or more identified or identifiable natural persons.

Public data:

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

Data that is not semi-private, private, or sensitive. Public data includes, among other things, data relating to a person's marital status, profession or occupation, and status as a merchant or public servant. By their nature, public data may be contained in public records, public documents, official gazettes and bulletins, and final court judgments that are not subject to confidentiality, among other sources.

Sensitive data:

Sensitive data means data that affects the Data Subject's privacy or whose misuse may lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in trade unions, social or human rights organizations, or organizations that promote the interests of any political party or safeguard the rights and guarantees of opposition political parties, as well as data concerning health, sex life, and biometric data.³

Database:

An organized set of personal data subject to processing.

Data Subject:

A natural person whose personal data is subject to processing.

Authorization:

The Data Subject's prior, express, and informed consent to the processing of personal data.

Data Controller:

A natural or legal person, public or private, who, alone or jointly with others, decides on the database and/or the processing of the data.

Data Processor:

A natural or legal person, public or private, who, alone or jointly with others, processes personal data on behalf of the Data Controller.

3. Biometric data comprises the physical, biological, or behavioral characteristics of an individual that uniquely distinguish them from the rest of the population. Computer systems that measure biometric data as part of identifying and/or authenticating a person are known as biometric security systems or simply biometric systems. Examples of biometric data include fingerprints, hand geometry, iris analysis, retinal analysis, veins on the back of the hand, facial features, voice patterns, handwritten signatures, keystroke dynamics, walking cadence, gesture analysis, and DNA analysis (Revista Seguridad Defensa Digital).

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

4. RESPONSIBILITIES

BLC Colombia S.A.S., as a legal entity, is the Data Controller for the personal data held in the databases of each of its areas. However, the following administrative units have been designated as Data Processors based on the types of data they handle:

DATA TYPES	RESPONSIBLE AREA
Payroll	Human Capital
Suppliers	Administration and Finance Department
Clients	Administration and Finance Department

5. PROCESS MAP

Not Applicable.

6. DEVELOPMENT

6.1. PRINCIPLES:

BLC Colombia S.A.S. structures its Personal Data Protection Policy around the following principles:

- Purpose limitation principle:** Information processing at BLC Colombia S.A.S. serves a legitimate purpose in accordance with the Constitution and the Law, for the performance of activities related to its corporate purpose.
- Freedom principle:** Processing may only take place with the Data Subject's prior, express, and informed consent. Personal data may not be obtained or disclosed without prior authorization.
- Truthfulness or quality principle:** Information subject to processing must be truthful, complete, accurate, up to date, verifiable, and understandable.
- Transparency principle:** Processing must guarantee the Data Subject's right to obtain from the Data Controller or Data Processor information about data concerning them held in their databases.
- Security principle:** Information subject to processing must be handled

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

using the technical, human, and administrative measures necessary to secure records, preventing their alteration, loss, unauthorized or fraudulent consultation, use, or access.

f) **Confidentiality principle:** All persons involved in data processing are required to ensure the confidentiality of the information, even after their involvement in any of the tasks comprising the processing has ended.

g) **Privacy by design and by default principle:** BLC Colombia S.A.S. will adopt the principle of "privacy by design and by default," ensuring that technical and organizational measures are incorporated from the initial development stages of all initiatives involving the processing of personal data.

h) **Demonstrated responsibility principle, "Accountability":** BLC Colombia S.A.S. commits to implementing appropriate organizational, technical, and legal measures to ensure and demonstrate effective compliance with this Personal Data Protection Policy.

i) **Data minimization principle:** BLC Colombia S.A.S. guarantees that it will only collect and process personal data that is adequate, relevant, and limited to what is strictly necessary to fulfill the purposes communicated.

j) **Proportionality principle:** Data processing by BLC Colombia S.A.S. will follow the criterion of proportionality, ensuring that the measures adopted are appropriate, necessary, and not excessive in relation to the purposes pursued.

k) **Impact Assessment principle:** When new processes involving large-scale or sensitive personal data processing are implemented, BLC Colombia S.A.S. may conduct a privacy impact assessment to identify and mitigate potential risks.

6.2. DATA SUBJECTS' RIGHTS:

Data Subjects whose personal data is held in BLC Colombia S.A.S.'s databases have the following rights:

a) **Right to know, update, and rectify their personal data:** Data Subjects may exercise this right in relation to partial, inaccurate, incomplete, fragmented, or misleading data, or data whose processing is expressly prohibited or has not been authorized.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

b) **Right to request proof of authorization:** Data Subjects may request proof of the authorization granted for the processing of their data, in accordance with Article 9 of Law 1581 of 2012. The data specified in Article 10 of that Law is exempt from this obligation.

c) **Right to be informed about the use made of their personal data:** Data Subjects have the right to know at any time how their personal data has been used, upon a request addressed to the Data Controller.

d) **Right to revoke authorization and/or request deletion of the data:** Data Subjects may revoke the authorization granted to BLC Colombia S.A.S. for processing their personal data if they find that constitutional and legal principles, rights, and guarantees have not been respected.

e) **Right to access their personal data:** Data Subjects may access, free of charge, their personal data that has been processed.

6.3. AUTHORIZATION:

6.3.1 Authorization by Data Subjects:

Data Subjects may authorize BLC Colombia S.A.S. to process their data through any means that can be consulted subsequently.

When requesting authorization, the following must be clearly and expressly communicated:

- a) The processing to which their personal data will be subject, which, in the case of BLC Colombia S.A.S., falls within the fulfillment of its corporate purpose.
- b) The optional nature of answers to questions concerning sensitive data or data relating to children and adolescents.
- c) Their rights as a Data Subject.
- d) The physical and electronic addresses through which they may exercise their rights as a Data Subject before BLC Colombia S.A.S., as the Data Controller.

Proof of compliance with the provisions of this article must be retained, and a copy must be provided to the Data Subject upon request.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

6.3.2 International Transfer and Acceptance by the Data Subject:

Data Subjects whose personal data is processed by BLC, including but not limited to employees, clients, suppliers, contractors, strategic partners, and any other third party related to the organization, expressly, freely, and knowingly accept the international transfer of their personal data to its associates and partners, as well as to other entities comprising BLC Colombia S.A.S.'s corporate structure, when such transfer is necessary to fulfill the company's corporate purpose or its contractual relationships.

This acceptance is given with full knowledge that the data may be processed in countries that may not provide a level of data protection equivalent to that of the country of origin.

BLC guarantees that these transfers comply with the principles of lawfulness, purpose limitation, freedom, security, transparency, and restricted access and circulation, and that it adopts the contractual, organizational, and technical measures necessary to protect personal data in accordance with international standards and applicable national legislation.

Given its multinational corporate structure, BLC Colombia S.A.S. may carry out international transfers of personal data to its partners in Argentina and other underlying corporate structures, subsidiaries, or strategic partners comprising BLC Colombia S.A.S., provided that such transfers are necessary to fulfill its administrative, contractual, commercial, operational, or legal compliance purposes. This policy aligns with the privacy guidelines of BLC Colombia S.A.S., headquartered in Argentina, respecting local regulations and international best practices in data protection

These transfers will be carried out under the principles of **lawfulness, purpose limitation, freedom, truthfulness, transparency, restricted access and circulation, security, and confidentiality**, ensuring that the processing of personal data maintains the same level of protection required by Colombian legislation.

BLC Colombia S.A.S. will adopt the contractual, technical, and organizational measures necessary to ensure the protection of the transferred data, including entering into agreements or contractual clauses that guarantee appropriate conditions of confidentiality, security, and respect for Data Subjects' rights.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

In all cases, international transfers will be carried out in accordance with Law 1581 of 2012 and its implementing decrees.

6.3.3 Cases in which the Data Subject's authorization is not required:

In accordance with Article 10 of Law 1581 of 2012, the Data Subject's authorization is not required for:

- a) Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- b) Data of a public nature
- c) Medical or health emergencies
- d) Information processing authorized by law for historical, statistical, or scientific purposes.
- e) Data related to individuals' Civil Registry records.
- f) Other cases established by Law.

6.4. DUTIES OF THE DATA CONTROLLER:

BLC Colombia S.A.S., as the Data Controller for personal data, has the following duties:

- a) Guarantee the Data Subject's full and effective right to Habeas Data at all times.
- b) Request and retain a copy of the authorization granted by the Data Subject.
- c) Properly inform the Data Subject of the purpose of collection and the rights arising from the authorization granted.
- d) Keep information under the security conditions necessary to prevent alteration, loss, unauthorized or fraudulent consultation, use, or access.
- e) Rectify incorrect information and communicate the relevant changes to each Data Processor.
- f) Process inquiries and complaints within the terms established in Law 1581 of 2012.
- g) Update changes to information reported by Data Subjects within five (5) business days of receipt.
- h) Promptly update, rectify, or delete data within the terms established in Law 1581 of 2012.

6.5. DUTIES OF DATA PROCESSORS:

The duties of natural or legal persons who, on behalf of BLC Colombia

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

S.A.S., process personal databases as Data Processors are as follows:

- a) Guarantee the Data Subject's full and effective right to Habeas Data at all times.
- b) Keep information under the security conditions necessary to prevent alteration, loss, unauthorized or fraudulent consultation, use, or access.
- c) Promptly update, rectify, or delete data within the terms established in Law 1581 of 2012.
- d) Update changes to information reported by the Data Controller within (5) business days of receipt.
- e) Refrain from circulating information disputed by the Data Subject and whose blocking has been ordered by the Superintendence of Industry and Commerce.

6.6. PURPOSES OF INFORMATION PROCESSING BY BLC COLOMBIA S.A.S.:

BLC Colombia S.A.S. will process personal data authorized by Data Subjects within the scope of its economic activity and corporate purpose, including, by way of example, the following purposes:

Type of Data Subject	Purpose of Processing	Legal Basis / Authorization	Responsible Area / Processor	Safekeeping Medium or Channel	Retention Period
Clients and prospective clients	Manage business relationships, contracts, proposals, and billing.	Data Subject's authorization / Service agreement / Law 1581 of 2012.	Commercial Department / Administration and Finance Department.	Corporate CRM system / Secure digital files.	During the contract term and for at least 5 years thereafter.
	Provide technical support, maintenance, and follow-up for IT solutions.	Service agreement / Legitimate interest.	Technology Department.	Service platform / Internal management system.	For the duration of the business relationship and in accordance with legal obligations.
	Conduct marketing, loyalty, satisfaction, and corporate event activities.	Data Subject's authorization / Legitimate interest.	Commercial Department / Communications.	Communications platform / Corporate repository.	Until authorization is revoked or the Data Subject requests deletion.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

Suppliers, contractors, and strategic partners	Manage selection, engagement, evaluation, payments, and contractual compliance.	Contract / Labor and commercial law.	Purchasing / Accounting / Human Resources.	ERP system / Digital or physical file.	During the contractual relationship and for 10 years after the accounting close.
	Verify background, references, and regulatory compliance.	Legal compliance / Legitimate interest.	Compliance / Audit / Legal.	Internal database / Supporting documentation.	Until contractual or regulatory obligations have been fulfilled.
Employees, former employees, and candidates	Manage recruitment, onboarding, payroll, well-being, and social security processes.	Employment contract / Law 1581 / Substantive Labor Code.	Human Resources / Occupational Health and Safety.	Payroll system / Digital or physical employee file.	During the employment relationship and for 20 years after termination.
	Control access to the company's physical and technological resources.	Legitimate interest / Security compliance.	Human Resources / Technology.	Access control system / Internal records.	During the employment or contractual relationship.
Partners, shareholders, and beneficial owners	Fulfill transparency, regulatory reporting, and due diligence obligations (UIAF, SIC, DIAN).	Corporate regulations / AML/ CFT prevention / Data Subject's authorization.	Legal Department / General Management.	Corporate register / Legal file.	During the corporate relationship and for at least 10 years thereafter.
	Manage communication and the exercise of corporate rights.	Legitimate interest / Legal obligation.	Legal Department.	Corporate minutes and records.	For the duration of the company and under applicable commercial regulations.
Visitors and third parties	Entry control, physical security, and video surveillance.	Legitimate interest / Regulatory compliance.	Security / Administration.	Video surveillance system / Visitor log.	A maximum of 30 calendar days unless legally or judicially required.
Transfers to underlying corporate structures	Share data with partners and other allies for support, administration, and corporate compliance.	Data Subject's authorization / International Data Transfer Policy / Law 1581 / Recipient country's Data Protection Law	General Management / Data Protection Officer.	Global repositories / Secure encrypted channels.	During the relationship and in accordance with the International Data Transfer Policy.
General (applicable to all Data Subjects)	Fulfill legal, contractual, accounting, and audit obligations.	Law 1581 / Sector regulations.	Administration and Finance Department.	Digital and physical files / Internal repositories.	As legally required (at least 10 years).
	Manage inquiries, grievances, complaints, and habeas data rights.	Exercise of ARCO rights.	Data Protection Officer / Customer Service.	Official personal data service email.	Until the procedure or complaint is finally resolved.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

	Implement compliance, ethics, and information security policies.	Corporate compliance / Accountability.	Compliance / Legal / Data Protection Officer.	Internal documentation / Management system.	Ongoing for as long as the policy remains active.
--	--	--	---	---	---

6.7. PROCESSING OF SENSITIVE DATA:

Sensitive data is data that affects the Data Subject's privacy and may lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in trade unions, social or human rights organizations, as well as data concerning health, sex life, and biometric data.

The Data Subject is not required to provide or authorize the processing of their sensitive data, except when such authorization is not required by law, or when Processing is necessary to safeguard the Data Subject's vital interests and they are physically or legally incapacitated, or in medical or health emergencies.

Sensitive data collected by BLC Colombia S.A.S. is processed for the following purposes, depending on the type of database concerned:

- a) Carry out the actions relevant to fulfilling BLC Colombia S.A.S.'s corporate purpose, as well as other related actions concerning the Data Subject.
- b) Historical and statistical purposes
- c) Manage all types of procedures, particularly requests, grievances, and complaints.
- d) Fulfill obligations undertaken by BLC Colombia S.A.S. toward the Data Subject regarding payment of salaries, statutory employee benefits, and other compensation established in the employment contract or required by law (in the case of company employees).
- e) Offer corporate well-being programs and plan BLC Colombia S.A.S. business activities for the Data Subject and their beneficiaries, such as children, spouses, permanent partners, etc. (in the case of company employees).
- f) Provide information to third parties with whom BLC Colombia S.A.S. has a contractual relationship when disclosure is necessary to fulfill the contracted purpose.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

6.8. PROCESSING OF MINORS' DATA:

BLC Colombia S.A.S. has security measures in place to provide enhanced protection for data collected about minors, ensuring respect for the overriding rights of children and adolescents.

In all cases, prior, express, and informed authorization will be requested from the Data Subject, guardian, or representative of the minor before personal data collection begins. The Data Subject is not required to provide or authorize such processing, except when such authorization is not required by law, or when Processing is necessary to safeguard the Data Subject's vital interests and they are physically or legally incapacitated, or in medical or health emergencies.

BLC Colombia S.A.S. processes the personal data of children and minors to guarantee their rights; offer administrative or cultural services provided by the company; conduct activities involving photographs or videos for dissemination; enroll them in the social security system or similar public entities; and, in general, conduct employee well-being activities involving the minor and adolescent children of employees or any other person associated with the company. Such processing takes place provided that: a) its purpose serves the best interests of children and adolescents; b) the processing performed by BLC Colombia S.A.S. ensures respect for their fundamental rights; c) the minor's right to be heard is respected, and their opinion is assessed based on their maturity, autonomy, and ability to understand the processing of the data; d) the requirements established in Law 1581 of 2012 for personal data processing are met.

6.9. SERVICE CHANNELS:

BLC Colombia S.A.S. will be responsible for handling Data Subjects' requests, inquiries, and complaints through any of the following channels, in accordance with the requirements for processing inquiries and complaints established in section 14 of this policy:

Office address: Co-Work Latam Astorga- Calle 8 # 43C - 68 - El Poblado

Offices 201 and 202 (Floor 2) - Medellín - Antioquia - Colombia

Email: contabilidadygestion@blcglobal.net

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

6.10. PROCEDURES FOR EXERCISING DATA SUBJECTS' RIGHTS:

6.10.1 Right of access or inquiry:

Data Subjects may exercise their right to access or inquire about their data by writing to BLC Colombia S.A.S. at **contabilidadygestion@blcglobal.net** or by regular mail to **Co-Work Latam Astorga- Calle 8 # 43C - 68 - El Poblado - Offices 201 and 202 (Floor 2) - Medellín - Antioquia - Colombia.** The request must contain the following information:

- Include "Exercise of the right of access or inquiry" in the subject line.
- The Data Subject's first and last names.
- A photocopy of the Data Subject's citizenship ID card or any other document establishing that the Data Subject is the person making the request, or a photocopy of the citizenship ID card or identification document of their representative and proof of representation, as applicable.
- The specific request for access or inquiry.
- Address for notices, date, and the applicant's signature.
- Documents supporting the request, where applicable.

Upon receipt, BLC Colombia S.A.S. will respond to the inquiry within a maximum of ten (10) business days from the date of receipt. If the inquiry cannot be addressed within that period, the interested party will be informed of the reasons for the delay and the date on which the inquiry will be addressed, which may in no case exceed five (5) business days following the expiration of the initial period.

6.10.2 Complaints:

Data Subjects may file a complaint concerning their data by writing to BLC Colombia S.A.S. at **contabilidadygestion@blcglobal.net** or by regular mail to **Co-Work Latam Astorga- Calle 8 # 43C - 68 - El Poblado - Offices 201 and 202 (Floor 2) - Medellín - Antioquia - Colombia.** The request must contain the following information:

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

- a) Include "Complaint or Grievance for correction/deletion/revocation or for a violation" in the subject line
- b) The Data Subject's first and last names.
- c) A photocopy of the Data Subject's citizenship ID card or any other document establishing that the Data Subject is the person making the request, or a photocopy of the citizenship ID card or identification document of their representative and proof of representation, as applicable.
- d) A description of the facts and the specific request for correction, deletion, revocation, or a violation.
- e) Address for notices, date, and the applicant's signature.
- f) Supporting documents that the applicant wishes to rely on, where applicable.

If the complaint is incomplete, the interested party will be asked to correct the deficiencies within five (5) days of receipt of the complaint. If two (2) months elapse from the date of that request without the applicant providing the required information, the complaint will be deemed withdrawn.

Once a complete complaint is received, a notation reading "complaint in progress" and the reason for it will be entered in the database within no more than two (2) business days. The notation must remain until the complaint is decided.

BLC Colombia S.A.S. will resolve the complaint within a maximum of fifteen (15) business days from the day following its receipt. If the complaint cannot be addressed within that period, the interested party will be informed of the reasons for the delay and the date on which the complaint will be addressed, which may in no case exceed eight (8) business days following the expiration of the initial period.

6.11. MANAGEMENT OF INCIDENTS AND SECURITY BREACHES:

BLC Colombia S.A.S. recognizes that, despite the preventive measures adopted, security incidents may occur that affect the integrity, availability, or confidentiality of the personal data processed by the organization. For this reason, the following procedure is established to manage, control, analyze, and mitigate such events, in line with a preventive and continuous improvement approach.

6.11.1 DEFINITION OF A DATA SECURITY INCIDENT:

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

A security incident means any confirmed or reasonably suspected event that:

Involves unauthorized disclosure, loss, alteration, or improper access to personal data;

- Affects the systems or assets where such information is stored or processed;
- Causes interruptions in the processes supporting personal data processing;
- Compromises fulfillment of the purposes communicated to the Data Subject.

6.11.2 INCIDENT RESPONSE PROCEDURE:

When an incident is detected or reported, the following phases will be activated:

a. Detection and notification:

Any employee, third party, or processor must immediately notify the Ethics and Compliance Officer or the channel established by the company for these cases.

b. Incident recording:

The incident will be documented in the management system, identifying: date, origin, event description, systems involved, type of data affected, and potentially affected Data Subjects.

c. Impact assessment:

A technical and legal analysis of the event will assess its criticality based on:

- Type of data affected (sensitive, financial, biometric, etc.);
- Volume of information compromised;
- Number of Data Subjects affected;
- Potential legal, reputational, or contractual consequences. This assessment will draw on the criteria in the personal data protection risk matrix to determine the severity of the event and prioritize the response.

d. Containment and mitigation:

Immediate actions will be implemented to stop exposure, limit its spread, and prevent further harm. This includes disconnecting systems, revoking access, or suspending services.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

e. Notification to Data Subjects or authorities (if applicable):

Where required by law or recommended by the impact assessment, affected Data Subjects and/or the Superintendence of Industry and Commerce will be notified, specifying:

- Nature of the incident;
- Data compromised;
- Measures adopted;
- Recommendations for Data Subjects.

f. Investigation and root cause analysis:

An analysis will be conducted to identify the source of the incident, assess control failures, and document lessons learned.

g. Corrective actions and continuous improvement:

Actions will be defined and implemented to prevent the incident from recurring, strengthening technical controls, operating procedures, or organizational measures.

h. Closure and documentation:

The incident will be formally closed once containment and improvement measures have been completed, with a record documenting the event's traceability.

6.11.3 Classification of Common Associated Risks:

BLC Colombia S.A.S. uses an institutional risk matrix as a core tool to identify, assess, and classify risks associated with personal data processing. This matrix assesses the likelihood, potential impact, and criticality of each risk, facilitating the prioritization of preventive and corrective actions.

Under this Incident Response Plan, the matrix will be applied in the following phases:

- During the assessment of reported incidents, to establish their severity and legal, technical, or operational consequences, and define the appropriate course of action;
- During periodic updates to the data protection management system, as part of the continuous improvement cycle;

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

- During internal audits or compliance reviews, to verify the effectiveness of current controls and identify new exposures.

In addition, a periodic inspection and review process will be implemented to:

- Identify and document new risks arising from changes in processes, technologies, regulations, or third-party relationships;
- Incorporate new risks into the institutional matrix;
- Adjust action plans, controls, and processing protocols as appropriate.

This approach maintains a dynamic, adaptable risk management model aligned with regulatory requirements, in which each incident is also an opportunity to strengthen organizational security and accountability for personal data.

6.11.4 Responsible Party for the Response:

The Data Officer and/or the processor designated by BLC Colombia S.A.S., together with the technology area and the units responsible for processing, will lead the response process, ensuring its proper execution and compliance with established guidelines.

6.12. THIRD-PARTY AUDIT AND MANAGEMENT:

BLC Colombia S.A.S. recognizes that a significant portion of personal data processing may be carried out through third-party contractors, suppliers, or strategic partners, who, as Data Processors, must act under the instructions and guidelines established by the company, ensuring appropriate levels of security, confidentiality, and legal compliance at all times.

6.12.1 Selection and contracting criteria:

Under its procurement and compliance policies, BLC Colombia S.A.S. will apply the following criteria when engaging third parties involved in personal data processing activities:

- Verification of regulatory compliance in data protection;
- Assessment of the technical and organizational measures implemented by the supplier;

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

- Execution of specific contractual clauses on confidentiality and personal data processing;
- Review of background, references, or information security certifications (where applicable).

6.12.2 Confidentiality and processing agreements:

Any third party accessing personal data managed by BLC Colombia S.A.S. must sign a Personal Data Confidentiality and Processing Agreement, which will include at least:

- Authorized purpose of processing;
- Limits on the use of information;
- Confidentiality obligations, including after the contractual relationship ends;
- Required security measures;
- Prohibition on subcontracting without express authorization;
- Liability framework and penalty clause for noncompliance.

6.12.3 Confidentiality and Personal Data Protection Clauses:

Confidentiality, personal data processing authorization, and image use clause for employees.

The employee freely, expressly, and knowingly authorizes BLC Colombia S.A.S., as Data Controller, to collect, store, circulate, use, transfer, and delete their personal and sensitive data in order to fulfill legal, contractual, and operational obligations arising from the employment relationship. This authorization includes information contained in résumés, personal and professional references, occupational history, financial and health information, and other data necessary for comprehensive human resources management.

Likewise, the employee authorizes the use of their image, name, voice, and other identifying elements in institutional, communication, corporate, and employee well-being activities, always within a framework of respect, good faith, and the company's own purposes.

The employee undertakes to maintain absolute confidentiality regarding all internal, technical, personal, or commercial information to which they have access during their

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

employment, with this obligation surviving for five (5) years after the employment relationship ends.

Personal data will be processed in accordance with BLC Colombia S.A.S.'s Personal Data Protection Policy, available at the Data Subject's request, and with Law 1581 of 2012 and its supplementary regulations.

Confidentiality and personal data processing clause for third parties.

The contractor declares that they understand and accept that, during their relationship with BLC Colombia S.A.S., they may have access to confidential information, as well as personal data of clients, employees, suppliers, or other third parties. Accordingly, the contractor undertakes to:

1. Maintain the confidentiality of all information to which they have access, and refrain from disclosing, reproducing, or using it for purposes other than those authorized under the contract.
2. Process personal data solely under the instructions of BLC Colombia S.A.S., as Data Controller, and for expressly authorized purposes.
3. Implement technical, human, and organizational protection measures in accordance with Law 1581 of 2012 and other applicable regulations.
4. Refrain from subcontracting data processing without prior, express, written authorization.
5. Allow audits or verifications by BLC Colombia S.A.S., when required, to validate compliance with data protection obligations.

In the event of noncompliance, the contractor undertakes to pay, as a contractual penalty, an amount equal to 20% of the total contract value, without prejudice to other legal actions. Confidentiality obligations will survive for five (5) years after the contract ends.

6.12.4 Inspection and supervision:

In conducting its commercial, technological, and administrative activities, BLC Colombia S.A.S. may engage suppliers, contractors, strategic partners, or

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

third parties who, by the nature of the services provided, access, manage, process, or hold personal data on behalf of the company.

To ensure compliance with applicable personal data protection regulations, BLC Colombia implements a third-party management and audit system based on the following principles and guidelines:

a) Third-party selection and evaluation

Before engaging any third party with access to personal data, an evaluation and due diligence process will verify:

- Their compliance with Law 1581 of 2012, Decree 1377 of 2013, Law 25.326 (Argentina) or the local law applicable to the recipient of the information, and other applicable regulations.
- The existence of internal information security and personal data protection policies, procedures, and controls.
- Their technical, organizational, and legal capacity to guarantee the confidentiality, integrity, and availability of information.

b) Formalization of commitments

Any third party processing personal data on behalf of BLC Colombia S.A.S. must first sign a **Personal Data Confidentiality and Processing Agreement**, establishing:

- Specific obligations for safekeeping, security, and confidentiality.
- The prohibition on using data for purposes other than those authorized.
- Conditions for returning or securely deleting data once the contractual relationship ends.
- The obligation to report any security incident affecting personal data within 48 hours of detection.

c) Monitoring and audit

BLC Colombia may conduct periodic or extraordinary inspections of suppliers and partners with access to personal data to verify compliance with contractual and regulatory obligations.

These audits may include document reviews, security assessments, interviews, or on-site or remote inspections, according to the criticality of the service provided.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

Audit results will be documented and, where appropriate, improvement plans or corrective measures will be implemented and must be addressed by the third party within the deadlines defined by BLC.

d) Shared responsibility and accountability

Third parties involved in processing personal data on behalf of BLC Colombia S.A.S. will act under the principle of demonstrated responsibility (accountability), maintaining evidence of compliance with their obligations and ensuring lawful, secure, and transparent processing.

BLC Colombia will retain the right to suspend or terminate the contractual relationship with any third party that fails to comply with this document or applicable personal data protection regulations.

e) Subprocessors or international technology partners

When personal data processing involves international transfers (for example, cloud services, management platforms, or support for BLC Colombia S.A.S.), the same standards established in the International Personal Data Transfer Policy will apply, ensuring equivalent or higher protection and security measures.

6.12.5 Updates and ongoing monitoring:

Third-party relationships will be monitored continuously through:

- Periodic compliance assessments;
- Updates to contractual commitments if the nature of processing changes or legal provisions are amended;
- Recording and analysis of third-party-related incidents;
- Inclusion of third parties in the processing risk matrix when their activity presents a significant level of exposure.

BLC Colombia S.A.S. may restrict, suspend, or terminate contractual relationships with third parties that do not guarantee appropriate conditions for personal data protection or that fail to comply with this document or applicable regulations.

6.13. LEGAL RETENTION AND RETENTION OF PERSONAL DATA:

Legal retention refers to the obligation of organizations to

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

retain and protect certain information, including personal data, for a minimum period defined by law, even after the contractual relationship or the purpose that prompted its collection has ended. This obligation is intended to ensure compliance with legal, tax, employment, accounting, or regulatory duties, as well as for evidentiary and oversight purposes.

In Colombia, legal retention is primarily established in Article 28 of Law 1581 of 2012, which provides that Data Controllers may retain personal data when a legal or contractual obligation requires them to do so. In addition, other sector-specific or cross-sector regulations establish minimum retention periods for different types of information.

In compliance with this obligation, BLC retains certain personal data according to the following parameters:

1. **Accounting and financial information:** must be retained for a minimum of 10 years, as established by the Commercial Code (Article 28) and the Tax Statute (Article 632).
2. **Employment information of current and former employees:** must be retained for a minimum of 20 years, in accordance with Article 134 of the Substantive Labor Code and related Ministry of Labor regulations.
3. **Civil, commercial, and service agreements:** must be retained for at least 5 years after termination, in accordance with the criteria of the Commercial Code and current contractual regulations.
4. **Information related to social security and parafiscal contributions:** must be retained for a minimum of 10 years, in accordance with Decree 1072 of 2015 (Single Regulatory Decree for the Labor Sector).
5. **Personal data records and consents:** must be retained for the duration of the relationship with the Data Subject and for at least 5 additional years, in accordance with the accountability principles established in Law 1581 of 2012 and the Guidelines for Data Controllers issued by the Superintendence of Industry and Commerce (SIC).

This legal retention provision expressly applies to all documents signed with counterparties - including employment contracts, commercial agreements, informed consents, authorizations, minutes, reports, and other supporting

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti

	Personal Data Protection BLC Colombia S.A.S.	Document	GLOB_SGI_DC_13
		Confidentiality	Public
		Revision: 00	Date: 01/10/2025

documents - regardless of the medium in which they were signed (physical or electronic), where personal data processing exists or may arise.

6.14. APPLICATION OF PERSONAL DATA PROTECTION LAW:

Matters not covered by this Policy will be governed by Law 1581 of 2012 and its implementing decrees, or any other applicable regulation that amends, supplements, or replaces them.

6.15. EFFECTIVE DATE:

This personal data processing policy of BLC Colombia S.A.S. takes effect upon publication.

BLC Colombia S.A.S. reserves the right to amend this document whenever it deems appropriate.

7. INDICATORS

Not Applicable.

8. RECORDS

Not Applicable.

9. APPENDICES

Not Applicable.

10. CHANGE CONTROL

Revision No.	Effective Date			Description
00	01	10	2025	Initial issue.



Carlos Alberto Cerrutti
Legal Representative
BLC COLOMBIA S.A.S.

Prepared by:	Reviewed by:	Approved by:
Crowe Co SAS	Carlos Cerrutti	Carlos Cerrutti