PERSONAL DATA PROTECTION POLICY XPERIENCE CUSTOMER MANAGEMENT S.A.S.

"This is a translation made with specialized software. However, there may be some important differences and clarifications. We recommend comparing this policy with the original text in spanish. Please contact us if you have any doubts about our data processing policy".

•DESIGN
xperience

Tel:(+604) 322 2302 or 301 347 9069
Carrera 52 # 14-30 / Local 206
Centro Empresarial Olaya Herrera
Medellín - Colombia

Content

12.6 Technical measures: comprises measures and definitions associated with the following aspects.

13. INTEGRAL CORPORATE PROGRAM FOR THE PROTECTION OF PERSONAL DATA

14. OTHER ASPECTS ASSOCIATED WITH THE PROCESSING OF PERSONAL DATA

14.1 Use of the de mark for activities involving the processing of personal information

VERSION	DATE	REASON FOR THE UPDATE
003	11/08/2021	Update in accordance with the regulatory provisions applicable to the company regarding the processing of personal data for the accreditation of the Accountability principle.

1. OBJECTIVE

Define the general guidelines for the implementation, application, monitoring, maintenance and continuous improvement of the management system and compliance with the personal data protection regime in the operation of XPERIENCE CUSTOMER MANAGEMENT S.A.S.

2. SCOPE

XPERIENCE CUSTOMER MANAGEMENT S.A.S, identified with NIT 900.446.513-6, with its main address at Carrera 52 # 14 30 local 206, in the city of Medellin, Colombia, hereinafter XPERIENCE or The Company, in its capacity as Data Controller, recognizes the importance of security, privacy and confidentiality of the personal data of its employees, customers, suppliers, partners, business allies and in general of all its stakeholders with respect to whom it processes personal information. Therefore, in compliance with constitutional and legal mandates, presents the following document containing its policies for the processing and protection of personal data, for all its activities involving the processing of personal information at the national level, as well as the processing of personal data at the international level in accordance with legislation, agreements and international treaties.

3. GLOSSARY

- **Authorization:** Prior, express and informed consent of the Data Subject to carry out the Processing of personal data. Consent may be given in writing, orally or through unequivocal conduct of the Data Subject that allows concluding that he/she granted the authorization.

- **Privacy Notice:** Verbal or written communication whose purpose is to comply with the duty to inform the data subject about the activities, types of processing, purposes and other aspects associated with the handling of personal information.

- **Database:** Organized set of personal data that is the object of Processing stored in manual or automated means, whose content includes information of clearly identified or identifiable natural persons (e.g. Database of workers, Database of

Supplier data, training attendance database, among others).

- **Causee:** A person who has succeeded another by reason of the death of the latter (heir or legatee).

- **Personal Data:** Any information linked or that can be associated to one or several determined or determinable natural persons.

- **Private Personal Data**: Data whose knowledge is restricted to the public.

- **Public Data:** Data that is not semi-private, private or sensitive, which may be processed by any person, without the need for authorization to do so. Public are, among others, the data contained in the civil registry of persons (e.g. whether one is single or married, male or female) and those contained in public documents (e.g. contained in Public Deeds), in public records (e.g. the disciplinary record of the Attorney General's Office), in gazettes and oficial bulletins and in enforceable court rulings that are not subject to reserve.

- **Sensitive Data:** Are those that affect the privacy of the Data Subject or whose improper use may generate their discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or filosophical convictions, membership in trade unions, social organizations, of human rights or that promote interests of any political party or that guarantee the rights and guarantees of opposition political parties as well as data related to health, sexual life and biometric data, among others, the capture of fixed or moving image, fingerprints, photographs, iris, voice, facial or palm recognition, etc.

- **Privacy designees by areas:** Role assigned to an official from each of the different areas of the Company, with the objective of supporting and coordinating with the privacy officer the development of the different activities and internal procedures for compliance with the corporate provisions and regulations on personal data protection.

- **Preparation of perfiles:** Preparation of individual decisions based on automated data processing, aimed at evaluating personal aspects or analyzing or predicting a person's professional performance, economic situation, health, personal preferences or interests, fiability, behavior, location or movements.

- **Data Processor:** Natural or legal person, public or private, who by itself or in association with others, performs the Processing of personal data on behalf of the Data Controller. For the purposes of this document, it is understood as that ally or supplier that carries out the Processing of personal data within the framework of the execution of a contract or agreement in accordance with the instructions, guidelines and purposes established by the Company.

- **Data Protection Delegate:** Corporate role in charge of monitoring, controlling and promoting the application of the Personal Data Protection Policy as well as the execution of the corporate program for the sustainability of the personal data protection model.

- **Public interest:** Justification that motivates the Processing of personal data based on one or more of the following events:
    - Treatments carried out by public authorities or agencies in the exercise of their functions.
    - Treatments for public interest purposes based on current legislation.
    - Treatments for historical, statistical or scientific research purposes.

- **Data Controller:** Natural or legal person, public or private, that by itself or in association with others, decides on the database and/or its processing.

- **Data Subject or Interested Party:** Natural person whose personal data is the object of Processing.

- **Data Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion, whether involving all or any of them.

- **International data transfers:** Transfer of data to persons, companies or other entities in third countries or international organizations not established in the territory of the Union. In accordance with the guidelines of the Organization's corporate data protection rules, these transfers may be addressed to a Controller (international data transfer) or a Processor (international transmission of personal data).

4. REGULATORY FRAMEWORK

- **Law 1581 of 2012**. Whereby the general provisions for the protection of personal data are issued.

- **Law 1266 of 2008.** Whereby general provisions on habeas data are issued and the handling of information contained in personal databases is regulated, especially financial, credit, commercial, services and information from third countries and other provisions are issued.

- **Sole Decree 1074 of 2015.** Whereby the Sole Regulatory Decree of the Commerce, Industry and Tourism Sector is issued.

- **REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL OF THE EUROPEAN UNION**
  COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

- **Royal Decree 3/2010**, of January 8, **2010**, which regulates the National Security Scheme in the field of Electronic Administration.

- **LSSICE - Law 34/2002**, of July 11, **2002,** on information society services and electronic commerce.

5. GENERAL PRINCIPLES, POSTULATES and SPECIFIC PRINCIPLES

5.1 GENERAL PRINCIPLES AND POSTULATES.

- XPERIENCE promotes the protection of rights such as Habeas Data, privacy, intimacy, good name, honor and personal image, for this purpose, all actions shall be governed by the principles of good faith, legality, computer self-determination, freedom and transparency.

- XPERIENCE recognizes that its legitimate right to Process the personal data of Data Subjects must be exercised within the specific framework of the law, the consent of the Data Subject and the specific instructions given by the Controllers where applicable, seeking at all times to preserve the balance between the rights and duties of Data Subjects, Controllers and other Processors linked to its operation.

- Whoever in the exercise of its activity provides any type of information or personal data to the Company in its capacity as processor or data controller, may exercise its rights as a data subject to know, update and rectify it in accordance with the procedures established in the applicable law and this policy.

5.2 SPECIFIC PRINCIPLES

XPERIENCE will apply the following specific principles set forth below, which constitute the rules to be followed in the collection, handling, use, Processing, storage, exchange and deletion of personal data:

- Loyalty: Loyalty and transparency with the Stakeholder.

- Limitation of fines: Collected for specified, explicit and legitimate fines and not further processed in a manner inconsistent with those fines.

- Data minimization: Adequate, relevant and limited to what is necessary in relation to the fiends for which they are processed.

- Accuracy: updated without delay with respect to the findings for which they are intended.

- Limitation on the retention period: Kept in a form that permits the identification of the Data Subject for no longer than is necessary for the purposes for which they are processed, except if the Processing is carried out exclusively for archiving purposes in the public interest or for historical, statistical or scientific research.

- Integrity and confidentiality: Implementing appropriate technical and organizational measures to protect data against unauthorized or unlawful processing and accidental loss, destruction or damage.

- Proactive accountability: Being responsible and able to demonstrate compliance with all Treatment principles.

- Systematic incorporation: The principles of Personal Data Protection will be implemented and will radiate the interpretation of all XPERIENCE processes and procedures.

6. XPERIENCE'S STATUS AS DATA CONTROLLER AND PROCESSOR OF PERSONAL INFORMATION

The scenarios in which The Company holds the status of Controller or Processor vis-à-vis the different types of Data Subjects based on their ability to decide on the means or purposes of the Processing of personal data are defined below:

CHARGED:

XPERIENCE shall act as Data Processor of personal data whenever, for the development of its activities, it uses or processes personal information on behalf of a third party that holds the status of Data Controller of the processed data. According to the nature of the operation and the corporate purpose of the Company, the activities as Data Processor of personal data will be mainly performed on the data of the users of the clients of XPERIENCE, whose information is entrusted for the rendering of the services and technological capacities contracted according to the offer of commercial services that constitutes the mission of the Company.

Although XPERIENCE has technical and operational autonomy to make decisions about personal information, it may not decide or dispose about the databases themselves or the way they are processed, for example: delete, share or disclose the database without the consent or prior authorization of the Data Controller or the Data Subject. Therefore, it shall be the responsibility of whoever holds the title of Data Controller to prove the existence of the duty of information, to manage the consent, to prove the legal basis or legitimate interest on which the development of the database is based.

of the personal data processing activities required for the full execution of the activities entrusted to the Company.

RESPONSIBLE:

XPERIENCE shall act as Responsible for the Processing of personal data whenever, for the development of its activities, it uses or processes personal information, directly managing the duty to inform the Data Subject, the consent, legal basis or any other event of legitimate interest applicable in accordance with the applicable regulatory provisions.

7. REGISTRATION OF PERSONAL DATA PROCESSING ACTIVITIES

In the development of its missionary, strategic support and related activities, the Company carries out personal data processing activities with respect to the following categories of data subjects and processing activities for which the Company holds the status of both Data Controller and Data Processor:

INTERESTED	TYPE OF DATA PROCESSED
CUSTOMERS	CUSTOMER CATEGORIES: 1. Clients: Persons with whom it maintains a business relationship for the provision of corporate services, being necessary to know the data of legal representatives and contact persons. TYPES OF DATA 1. General data concerning your age of majority status,

	date and place of birth, age, sex, nationality. 2. Identity data such as names, surnames, ID card/ID card/identification document, firma, 3. Business contact information: Address, telephone numbers, e-mail address. 4. Socio-economic data: Data of an economic nature, such as tax data and economic activity, data necessary for invoicing.
	PURPOSE OF THE TREATMENT: 1 Commercial and administrative customer relationship management
	LEGITIMACY: 1 Execution of a contract 2 Consent
SHAREHOLDERS	CATEGORIES OF STAKEHOLDERS: 1 Shareholders: Corresponds to persons with an equity interest in the Company, regardless of their percentage. TYPES OF DATA 1 General data concerning your age of majority, date and place of birth, age, sex, nationality. 2 Identification data such as names, surnames, DNI/NIF/ID card/identification document, firma 3 Private and commercial contact information: address, telephone numbers, e-mail address. Socioeconomic data: Data of an economic nature, such as tax data and economic activity, direct debit of payments.
	PURPOSE OF TREATMENT

	1 Manage commercial, corporate, corporate affairs and bylaws.
	LEGITIMACY 1 Overriding legitimate interest of the responsible party. - Relation to the activity of the person in charge. Legal obligation for the responsible party
SUPPLIERS	CATEGORIES OF INTERESTED PARTIES Suppliers: Persons with whom there is a commercial contractual relationship for the acquisition of goods or services required by the Company for the development of its corporate purpose. TYPES OF DATA 1 General data concerning your age of majority, date and place of birth, age, sex, nationality. 2 Identity data such as names, surnames, ID card/ID card/identification document, firma, 3 Business contact data: address, telephone numbers, e-mail address Socioeconomic data: Economic data, such as tax data and economic activity, direct debit of payments.
	PURPOSE OF TREATMENT 1 Manage the commercial relationship with suppliers
	LEGITIMACY 1 Contract execution Consent
EMPLOYEES	CATEGORIES OF STAKEHOLDERS: 1 Employees: Personnel directly linked to the Company through an employment contract. 2 Workers on assignment: Person who provides temporary services to the company.

	Company through intermediation of a third party TYPES OF DATA 1 General data concerning your age of majority, date and place of birth, age, sex, nationality. 2 Identification and contact data including image, voice, photograph, video, firma information. 3 Private and corporate contact information: Address, telephone, email, etc. 4 Socioeconomic data: Economic data, tax information, property data, labor data, educational level, work experience. 5 Bank details for direct debit of payroll payments 6 Judicial or disciplinary background data. 7 Data associated with passwords and users of information systems Sensitive Data associated with occupational medical fitness, disability and health events relevant to compliance with the provisions on occupational hazards and health prevention.
	PURPOSE OF TREATMENT 1 Management of the labor relationship with employees
	LEGITIMACY 1 Management of the labor relationship with employees
VISITORS TO COMPANY FACILITIES	1 Visitors: Individuals who access the Company's physical locations for the development of commercial or operational activities. DATA TYPES: 1 General data concerning the condition of majority.

	2 Identification data including image, photograph and video information. Private or business contact information: telephone number
	PURPOSE OF TREATMENT 1 Management of physical security and access control to facilities
	LEGITIMACY 1 Consent Overriding legitimate interest of the Controller associated with the management of the security of the Company's physical facilities and information.
BUSINESS AND LABOR CONTACTS	

As Data Processor:

INTERESTED	TYPE OF DATA PROCESSED

Customer users	CUSTOMER CATEGORIES: 2. Clients: Persons with whom it maintains a business relationship for the provision of corporate services, being necessary to know the data of legal representatives and contact persons. TYPES OF DATA 5. General data concerning your age of majority, date and place of birth, age, sex, nationality. 6. Identity data such as names, surnames, ID card/ID card/identification document, firma, 7. Business contact information: Address, telephone numbers, e-mail address. 8. Socioeconomic data: Data of an economic nature, such as tax and social security data.
	economic activity, data necessary for invoicing.
	PURPOSE OF TREATMENT 1 Manage compliance with contractual obligations commissioned by the customer Responsible for the treatment associated with technical support and information processing transactional information of its customers and users
	LEGITIMACY 1 Execution of a contract. 2 Legitimate prevailing interest of the responsible. Relationship with the activity of the responsible.

8. Legal basis for the processing of personal data:

The development of personal data processing activities that the Company performs in its capacity as Responsible and Charged, supports its lawfulness in the following legal basis:

a) The Processing is necessary for the performance of a contract with the Data Subject or with the Controller of personal data when the Company holds the status of Data Processor:

   - Commercial contract.
   - Employment contract.

b) The Processing is necessary to comply with a legal obligation applicable to the Data Controller, based on the fiscal, business, labor, commercial and other regulations that are applicable according to the territory in which it operates.

9. MAIN SCENARIOS AND SPECIFIC PURPOSES TREATMENT OF PERSONAL INFORMATION

The personal data processing activities carried out by the Company are associated with the scenarios and specific purposes detailed below:

1. **Purchasing and procurement management:**

a) Verify commercial and reputational background and possible relationship risks associated with Money Laundering and Terrorist Financing.

b) To legally and commercially link the supplier or partner with the Company, allowing the development of accounting, logistical and financial procedures of the operation.

c) Formalize the contractual relationship with the supplier or business partner, controlling the full execution of the obligations assumed.

d) Evaluate the performance and results of the supplier or partner with a view to strengthening contracting or sourcing procedures.

2. **Human talent management and labor relations:**

a) Verify commercial and reputational background and possible relationship risks associated with Money Laundering and Terrorist Financing.

b) Evaluate the labor perfil of applicants with a view to the selection and formalization of the employment relationship, filling vacancies or personnel requirements of the different areas and functions of the Company.

c) Verify academic, work, personal and family background, and other significant socioeconomic elements of the labor applicant, according to the requirements of the position to be filled.

d) Manage before the administrative authorities, the linking, affiliation or reporting of new developments associated with the social security system, as well as other welfare and benefit obligations of a labor nature.

e) Register the employee in the Company's computerized management systems, allowing the development of the accounting, administrative and financial activities inherent to the labor relationship.

f) Manage labor developments with an impact on the settlement and payment of payroll.

g) Promote the development of wellness and integral development activities for employees and their work and family environment.

h) Manage training and education programs according to the requirements of the position and corporate guidelines.

a) To administer the occupational health and safety management system, aiming at risk mitigation, as well as the adequate attention to incidents.

b) Evaluate the performance and analyze the functional competencies of the employees with a view to determining the career and integral development plan.

c) Manage termination procedures, as well as the fulfillment of the corresponding economic obligations.

d) Manage the development and fulfillment of the operational and functional tasks associated with the perfil of the position.

e) Implement the internal procedures required for the application of the provisions of the internal work regulations.

f) Monitor compliance with labor obligations and measures for proper use of corporate tools provided by the Company, including communications, messages, traceability of uploading and downloading files from information systems and corporate applications.

g) Forward information of a semi-private nature such as payroll supports, competency evaluation results, through the employee's private means of contact in order to promote the privacy of his or her personal information.

h) Back up information managed through corporate systems and applications in order to guarantee the registration and access to information.

The Company's historical and relevant operations, as well as the continuity of its operations even after the termination of the employee's employment.

i) Use the image and voice of the collaborator through various audiovisual media for fines dissemination through the various physical or digital corporate communication media.

3. **Customer relationship management:**

a) Verify commercial and reputational background and possible relationship risks associated with Money Laundering and Financing of Terrorism (ML/FT).

b) To support the commercial relationship with customers and prospects, allowing their registration in the Company's management systems for the development of accounting, logistic, commercial and financial procedures of the operation.

c) Manage communication activities and customer loyalty, as well as the timely attention of Petitions, Complaints, Claims and Suggestions PQRS, which allow evaluating the quality of products and services offered by the Company.

d) To develop marketing and market intelligence activities, seeking to strengthen the commercial management of the Company.

e) Convene, sponsor or organize the participation of current or potential customers in events or commercial or promotional activities of the different services of The Company or its allies, eventually keeping the record of the attending Stakeholders through recording, photography or any other physical or automated means.

f) Deploy business intelligence, customer prospecting, analytics, research and market trends to better understand your current or potential customers.

g) Create and send to its customers behavioral advertising, i.e., that based on the interests that customers show in social networks and/or in interaction with XPERIENCE and/or its partners.

4. **Administrative management, governance, risk and compliance:**

a) Register and control access to the Company's facilities, mitigating physical and information security risks.

b) Verify, control and monitor the development of processes, activities and products in accordance with the guidelines and objectives established by the internal or external audit.

c) Verify, control and monitor the development of processes, activities and services in accordance with environmental guidelines, quality management and information security management.

d) Manage compliance with legal obligations and requirements associated with the development of the Company's operations.

e) Manage complaints associated with corporate malpractices or those affecting corporate ethics or transparency.

f) Support the development of the operation through the provision, management and maintenance of the Company's IT tools and applications.

g) Manage the development of jurisdictional or extra-procedural actions or proceedings associated with alternative dispute resolution mechanisms, either in own cause or as legal representative.

h) Manage compliance with corporate and corporate obligations before internal bodies and external authorities.

5. Accounting and treasury management

a) To allow the control of the Company's economic movements through the recording of accounting vouchers and causability.

b) Facilitate decision making and knowledge of the Company's economic situation by managers and other competent positions through the generation of reports, information and indicators supported by aggregated or individualized information.

c) To comply with the legal provisions that oblige the Company to submit reports and financial statements to the competent authority.

d) Establish and implement control mechanisms associated with supplier payment validation.

e) Manage good relations between the company and the State entities with which it is obliged to maintain constant communication.

10. REQUEST FOR AUTHORIZATION AND CONSENT OF THE DATA SUBJECT

For those cases in which personal information is collected by XPERIENCE in its capacity as data controller, the following aspects will be taken into account.

10.1 Means and manifestations to grant the authorization.

The authorization for the Processing of the required personal information is obtained through the applications and privacy notices made available to the Interested Party in each of the channels or points of capture of physical, verbal or digital information, which have been arranged through forms, notices or statements that inform the Interested Party about the capture and subsequent Processing of their personal data, their finalities, rights, channels for the exercise of their rights and if applicable, the way to access this policy.

The data subject's authorization for data processing shall be granted expressly and its manifestation may be given under the different modalities established by law, taking into consideration the nature of each of the information collection channels, being written, verbal or through unequivocal actions or conduct of the data subject.

10.2 Proof of authorization.

The authorization for the processing of data collected in the development of the activities described in this policy will depend on the nature of the channel or point of information collection. The means of proof to accredit the effective authorization of the Processing will depend on the type of mechanism used.

to obtain the authorization, such as the signed form, the record of acceptance or access to the web page, the recording of the conversation, among others. In the events of acceptance by means of unequivocal conduct, the integrated set of the following elements shall be taken as sufficient proof of acceptance by the Interested Party:

a) The authorization request form will be made available to the Interested Party at the time he/she enters his/her data.

b) The express indication in the authorization request form of the unequivocal conduct of the Data Subject that constitutes authorization for the Processing.

c) The evidence of the performance of the unequivocal conduct by the Stakeholder, being feasible to accredit the information provided by the Stakeholder or other type of evidence of express acceptance according to the nature of the channel.

10.3 OBLIGATIONS OF THIRD-PARTY SUPPLIERS

Without prejudice to the specific provisions agreed in each particular case, those third parties in charge of the Processing with contractual or conventional link with XPERIENCE, are subject to compliance with the following obligations regarding the protection of personal data:

a) Adopt, abide by and maintain in force a policy for the treatment of personal information applicable to the development of its operation.

b) Adopt, abide by and maintain in force a manual of internal policies and procedures for the Treatment of personal information, including the elements for the effectiveness of the policy.

c) Define and maintain enabled the channels for the timely and complete attention of eventual queries and claims of the Stakeholders of information regarding personal data protection, for which it shall have at least a physical address, a fixed or mobile telephone line and an e-mail.

10.4 OBLIGATIONS OF EMPLOYEES

Without prejudice to the obligations agreed in each particular case, the employees or direct and indirect collaborators must comply with the following obligations:

a) To know and abide by this personal data protection policy, as well as the other conditions, limitations, purposes and rights that you have as a Data Subject of personal information, among which is the right to make requests, complaints or claims regarding the processing of your personal data by the Organization, rights that may be exercised through the means, mechanisms and procedures described in section 11.3 of this policy.

b) Safeguard the security of personal data subject to Processing, which will be carried out on behalf of XPERIENCE in accordance with the principles that protect it.

11. PROCEDURES FOR MANAGING AND ATTENDING TO THE RIGHTS OF INTERESTED PARTIES

Data Subjects, representatives or their successors in title may exercise their rights to request access, rectification, deletion, portability of their personal data, limitation and opposition to the Processing, as well as their right not to be subject to automated individual decisions in accordance with the following procedure:

a) At any time and free of charge, the Data Subject or his representative may make requests regarding the personal data that are subject to Processing by XPERIENCE upon proof of identity.

b) When the request is formulated by a person other than the Interested Party, due proof must be provided of his or her legal standing or representation to act on behalf of the Interested Party.

c) The requests received directly by any third party in charge of the Processing of XPERIENCE shall be sent by such third parties to the Company no later than the next working day after its receipt through the email described in section 11.1 of this policy. XPERIENCE shall act in the same way when it holds the condition of Data Processor before the respective Data Controller.

d) The request must contain at least the following information:

- The name and contact address of the Interested Party or any other means to receive the response.

- Documents proving the identity and capacity of its representative, as indicated in the following cases:

    - Interested party: Identification document.
    - Causahabiente: Civil registry and identification document.
    - Legal representative in case of minors:

        - Parents: Birth certificate and identity card.
        - Guardians: Court ruling that confirms legal representation.

- Legal representative authorized by the Interested Party: Broad and sufficient power of attorney for the formulation of the request associated with the exercise of the right to be exercised.

- The clear and precise description of the personal data in respect of which the petitioner is exercising the right

- The clear and precise description of the right that the petitioner, his successors in title or representatives wish to exercise.

- Provide documentation to support your request if the nature of the data is appropriate.

- If necessary, other elements or documents that facilitate the location of the personal data.

e) If the request made by the Interested Party is incomplete, XPERIENCE will require the Interested Party within five (5) days from the receipt of the consultation to correct the faults.

f) In the case of queries submitted in full, XPERIENCE will respond to the petitioners within a term of 30 calendar days from the date of receipt thereof. When it is not possible to attend the consultation within such term, the Interested Party will be informed within the previously described term, expressing the reasons for the delay and indicating the date on which the consultation will be attended, which in no case may exceed five to 60 days in addition to the additional term when the number of requests or the nature of the request implies an inordinate effort, prior notification and justification before the Spanish Agency for Personal Data Protection (AEPD) or competent authority.

If required, the Data Subject may communicate through XPERIENCE's data protection channels, in order to request the format for the realization of his request, which should be considered as an aid or support to the Data Subject, but not as a mandatory requirement for the exercise of the rights.

In the event of a decision not to act on the request of the Stakeholder, the reasons for non-action and the possibility of lodging a complaint with a supervisory authority and of taking legal action shall be provided without delay, and at the latest one month after receipt of the request.
12.4 RGPD).

All information provided by the Company (from Articles 13 to 22 and 34 RGPD) in the context of the exercise of the rights of the Stakeholders must be given free of charge. However, when requests are manifiestly unfounded or excessive, especially due to their repetitive nature, the Company may:

a) Charge a reasonable fee based on the administrative costs incurred to provide the information or communication or to carry out the requested action, or

b) Refuse to act on the request.

The management of requests associated with the exercise of Stakeholder rights shall be governed by the following specific guidelines according to the type of right exercised by the Stakeholder:

c) For the right of access (Art.15), data subjects shall be provided with a list of the personal data in its possession together with the purpose for which they have been collected, the identity of the recipients of the data, the retention periods, and the identity of the Controller to whom they can request rectification, deletion and opposition to the processing of the data.

- Scope. The request in which the request for access is specified, must specify whether information is requested relating to specific data, to data included in a particular file or processing, or to all of the data subject to processing.

- Justification: Not required, unless the right has been exercised within the last six months.

- Refusal: Reasons must be given and it must be indicated that the protection of the AEPD can be invoked. Grounds for refusal are that the right has already been exercised in the twelve months prior to the request (unless a legitimate interest to that effect is accredited) and that it is so provided by a Law or a directly applicable rule of community law or when these prevent the Data Controller from disclosing to the data subjects the Processing of their data.

- Approval: Communication to the interested party through the means of contact indicated in the request.

d) For the right of rectification (Art.16), we will proceed to modify the data of the Interested Parties that were inaccurate or incomplete in accordance with the purposes of the Processing.

- Justification: It must be indicated to which data it refers and the correction to be made by providing supporting documentation according to the nature of the request.

- Refusal: Reasons must be given and it should be indicated that the protection of the AEPD can be invoked.

- Approval: Communication to the interested party through the means of contact indicated in the request.

e) For the right of limitation of Processing (Art.18), the data of the Data Subject will not be processed when:

- The Data Subject challenges the accuracy of the personal data, for a period of time that allows the Controller to verify the accuracy of the personal data;

- The Processing is unlawful and the Data Subject objects to the deletion of the personal data and requests instead the limitation of its use;

- The Controller no longer needs the personal data for the purposes of the Processing, but the Data Subject needs them for the formulation, exercise or defense of claims;

- The Data Subject has objected to the Processing pursuant to Article 21(1) of the GDPR, while it is verified whether the legitimate reasons of the Controller prevail over those of the Data Subject.

Where the Processing of personal data has been restricted, such data may only be Processed, with the exception of their retention, with the consent of the Data Subject or for the purposes of the formulation, exercise or defence of claims, or for the protection of the rights of another natural or legal person or for reasons of substantial public interest of the Union or of a particular Member State. 4.5.2016 L 119/44 Official Journal of the European Union EN.

Any Data Subject who has obtained the limitation of the Processing shall be informed by the Controller prior to the lifting of such limitation.

- Justification: Concurrence of well-founded and legitimate reasons related to your specific personal situation.

- Refusal: Must be motivated and indicate that the protection of the AEPD can be invoked.

- Approval: Communication to the Interested Party through the means of contact indicated in the request

f) For the right of opposition (Art.21): The data of the Interested Parties will be blocked when they manifiest their refusal or opposition to the consent for the Processing of their data and there is no legal duty to prevent it.

- Justification: Concurrence of well-founded and legitimate reasons related to your specific personal situation.

- Refusal: Reasons must be given and it must be indicated that the protection of the AEPD can be invoked.

- Approval: Communication to the interested party through the means of contact indicated in the request.

g) For the right of suppression (Art.17): The data of the Interested Parties shall be suppressed when they manifest their refusal or opposition to the consent for the Processing of their data and there is no legal duty to prevent it and

the responsibilities of the Controller and the Processor(s) have been prescribed.

- Justification: The data to be cancelled and the reason for cancellation must be indicated, providing documentation.

- Refusal: Reasons must be given and it should be indicated that the protection of the AEPD can be invoked.

- The cancellation shall not proceed when the personal data must be kept for the periods provided for in the applicable provisions or, as the case may be, in the contractual relations between the person or entity Responsible for the Processing and the Data Subject that justified the Processing of the data.

- Approval: Communication to the interested party through the means of contact indicated in the request.

h) For the right of portability (Art.20): Data Subjects shall communicate their decision and inform the Controller, if applicable, about the identity of the new controller to whom to provide their personal data. Such transfer of data, will be feasible when:

The processing is carried out by automated means.

- It is technically possible.

- It is not necessary for the performance of a task carried out in the public interest or in the exercise of public powers vested in the controller.

- It shall not adversely affect the rights and freedoms of others.

i) For the right not to be subject to automated individual decisions (Art.22): Data Subjects must communicate their decision, and inform the Controller, that they do not wish to be subject to a decision based solely on automated Processing, including the processing of perfiles, which produces legal effects on them or significantly affects them in a similar way.

- The Data Controller shall inform all persons with access to personal data about the terms of compliance to meet the rights of data subjects, the form and procedure in which such rights will be met.

The Company shall communicate any rectification or erasure of personal data or restriction of Processing carried out pursuant to Article 16, Article 17(1) and Article 18 of the GDPR to each of the recipients to whom the personal data has been disclosed, unless this is impossible or would require a disproportionate effort. The Company will inform the Data Subject about such recipients, if the Data Subject so requests.

11.1 Exercise of rights under Law 1581 of 2012 Colombia Procedure for making inquiries:

a) At any time and free of charge, the holder or his representative may make inquiries regarding the personal data that are subject to processing by XPERIENCE upon proof of identity.

b) When the consultation is formulated by a person other than the owner, the legal capacity or mandate to act must be duly accredited.

c) Inquiries received directly by a third party in charge of the processing of information must be sent to the Company no later than the business day following their receipt through the e-mail address described in section 11.3 of this policy.

d) The consultation must contain at least the following information:

- The name and contact address of the owner or any other means to receive the response.

- Documents proving the identity and capacity of its representative, as indicated in the following cases:

  - Holder: Identity document.
  - Causahabiente: Civil registry and identification document.
  - Legal representative in case of minors:
    *Parents: Birth certificate and identity card.
    *Guardians: Court sentence that confirms legal representation.
  - Legal representative authorized by the owner: authenticated power of attorney.

- The clear and precise description of the personal data with respect to which the holder seeks to exercise the right of consultation.

- The clear and precise description of the consultation made by the owner of the information, its assignees or representatives.

- Provide documentation to support your request if the nature of the data is appropriate.

- If necessary, other elements or documents that facilitate the location of the personal data.

e) If the consultation made by the holder is incomplete, XPERIENCE will require the interested party within five (5) days from the receipt of the consultation to correct the faults. After two (2) months from the date of the request, if the applicant does not submit the required information, it will be understood that he/she has abandoned the request.

f) In the case of queries submitted in full, XPERIENCE will respond to the petitioners within ten (10) business days from the date of receipt of the request.

g) same. When it is not possible to attend the consultation within said term, the interested party shall be informed, stating the reasons for the delay and indicating the date on which the consultation will be attended, which in no case may exceed five (5) working days following the expiration of the first term.

If required, the Data Subject may communicate through XPERIENCE's data protection channels in order to request the format to carry out his/her consultation, which should be considered as an aid or support to the Data Subject, but not as a mandatory requirement for the exercise of his/her rights.

11.2 Exercise of rights in accordance with Law 1581 of 2012 Colombia, CLAIMS (Correction, updating, deletion).

The Data Subject or his/her successors in title who consider that the information contained in a database should be corrected, updated or deleted, or

when they notice the alleged breach of any of the duties contained in the Law, they may submit their claim through the personal data protection channels of XPERIENCE using any of the means of contact defined in this Policy.

Claims procedure:

a) At any time and free of charge, the holder or his representative may make claims associated with corrections, updates or deletion of personal data that are subject to processing by XPERIENCE, upon proof of identity.
b) When the claim is formulated by a person other than the owner, the legal capacity or mandate to act must be duly accredited.

c) Complaints received directly by a third party in charge of the processing of information must be sent to the Company no later than the business day following their receipt through the e-mail address described in section 11.3 of this policy.

d) The consultation, rectification, update or deletion must contain at least the following information:

- The name and contact address of the owner or any other means to receive the response.

- Documents proving the identity and capacity of its representative. As indicated for the following cases:

  - Holder: Identity document.
  - Causahabiente: Civil registry and identification document.
  - Legal representative in case of minors:
  - Parents: Birth certificate and identity card.
  - Guardians: Court ruling that confirms legal representation.
  - Legal representative authorized by the holder: Authenticated power of attorney.
  - By stipulation in favor of another: Manifestation in this sense.

- The clear and precise description of the type of claim made by the owner of the information (correction, update or deletion).

- The clear and precise description of the personal data with respect to which the holder seeks to exercise the right of claim, as well as the facts that give rise to the claim.

- Provide documentation to support your request if the nature of the data is appropriate.

- If necessary, other elements or documents that facilitate the location of the personal data.

e) If the claim made by the holder is incomplete, XPERIENCE will require the interested party within five (5) days following the receipt of the claim to correct the faults. After two (2) months from the date of the requirement, if the applicant does not submit the required information, it will be understood that he/she has abandoned his/her request.

f) In the case of claims (corrections, updates and deletions), XPERIENCE will respond to the owners of information within the term of (15) working days from the date of receipt of the claim, when it is not possible to address the claim within that period, the interested party will be informed, stating the reasons for the delay and indicating the date on which your query will be addressed, which in no case may exceed eight (8) working days following the expiration of the first term.

If required, the Data Subject may communicate previously through XPERIENCE's data protection channels, in order to request the form to make the claim, which should be considered as an aid or support to the Data Subject, but not as a mandatory requirement for the exercise of the rights.

11.3 CHANNELS ENABLED FOR THE EXERCISE OF THE RIGHTS OF THE INTERESTED PARTIES

For the management and attention of the rights of data subjects, the Company has designated Luisa Fernanda Salgado Ospina as the Delegate or official for the protection of personal data, who can be contacted through the following channels

- Address: Carrera 52 # 14 30 local 206, Medellín, Colombia
- Telephone: 60 + 4 + 3222302
- E-mail: "protecciondedatos@xperience.net.co"

In the event of the eventual use of other contact channels by the data subjects for the exercise of their rights regarding personal data protection, the Company reserves the right to refer or inform the data subject of the existence of the previously described channels in order to initiate the consultation or complaint procedure in a timely and complete manner.

12. OF THE SPECIAL PROVISIONS FOR THE PROCESSING OF PERSONAL DATA AND ACCREDITATION OF THE PRINCIPLE OF "ACCOUNTABILITY".

12.1 IDENTIFICATION AND UPDATING OF THE PERSONAL INFORMATION CYCLE

For proper compliance with the personal data protection regime, XPERIENCE will identify and keep updated the understanding of the life cycle of the personal information of its operation, identifying and validating especially the following elements:

a) Activities or processes that initiate or justify the processing of personal data.

b) Channels or points of capture of personal information, detailing the type of information collected, the means of collection and its finality.

c) Databases and other information repositories where the personal information collected is stored, specifying the physical or automated means of information processing.

d) Users or internal areas of XPERIENCE with access to information in databases and other repositories of personal information, specifying the purposes of the use or access to the information.

e) Nodes or exit points of the personal information, identifying third party recipients, type of responsibility of the third party, as well as the national or international scope of the transmission or transfer of the information.

f) Mechanisms for the disposal of personal information collected.

12.2 RELATIONS WITH THIRD PARTIES.

XPERIENCE, in line with its internal policies and provisions on personal data protection, will endeavor to link or relate labor and commercially with those third parties that show their commitment to the observance and application of the general regime of personal data protection in their respective operations.

Therefore, without prejudice to the use of the appropriate forms or models of request for authorization of processing, privacy notices and contractual coverage, the Company may request from third parties the relevant information that allows it to verify compliance with the provisions contained in this policy, as well as those enshrined in its own internal policies and procedures for the protection of personal data when it deems it necessary.

Third parties that on the occasion of the development of their contractual or conventional object, affect the Processing or have any impact on the life cycle of the personal information of XPERIENCE, must prove prior to the time of their connection, compliance with the requirements of the data protection regime, including but not limited to the existence and implementation of a policy for the Processing of personal information, the provision of channels for the handling of queries and claims for the Stakeholders of personal information, as well as the effective implementation and updating of the National Registry of Personal Information, but not limited to the existence and application of a policy for the Treatment of personal data, the habilitation of channels for the attention of queries and claims for the Stakeholders of personal information, as well as the effective completion and updating of the National Registry of Personal Data Bases before the Superintendence of Industry and Commerce in the established legal terms.

Likewise, the Company reserves the right to supervise, on an eventual or periodic basis, the compliance of its third parties with the legal and contractual requirements associated with the personal data protection regime, for which it may request evidence or support of compliance, make visits to the facilities or headquarters of the third party, among other measures it deems reasonable according to the criticality of the operation, the volume of data or the nature of the contractual object.

Upon termination for any reason of the legal, contractual or commercial relationship between XPERIENCE and any third party involved in the Processing of personal data, the relevant procedures shall be applied to ensure the safe and secure disposal of the personal information that has been subject to Processing, by means of deletion, return, dissociation or any other activity that XPERIENCE deems appropriate.

In the event of total or partial non-compliance with the provisions of the personal data protection regime or this policy by third parties with a contractual or conventional relationship, the Company may, at its discretion, terminate the contractual or conventional relationship with just cause or, failing that, agree on an action plan to achieve the minimum levels of compliance with the law, provided that the necessary contingency measures are adopted to prevent a serious impact on the rights of data subjects. In the event of agreeing an action plan with the third party with a view to compliance with the personal data protection regime, the same shall be understood as integrated to the content of the contract or agreement formalizing the relationship with the third party.

12.3 PRIVACY IMPACT ASSESSMENT

XPERIENCE recognizes the importance of privacy and the protection of its Stakeholders' information in the development of its operations. In order to promote the sustainability and continuous improvement of the current legal, technical and organizational coverage, XPERIENCE has adopted an internal procedure and prior to the development of its new operations or initiatives with impact on the current cycle of the Processing of its personal data, in order to determine Ex ante or in advance, the actions, measures and coverage necessary for the protection of information and the proper Processing of personal data.

The development of this proven diligence initiative is coordinated by the privacy officer, without prejudice to the transversal responsibility that concerns the entire human resource linked to the organization in accordance with the procedures described in the internal manual of policies and procedures for the Treatment of personal information of XPERIENCE.

Without prejudice to the specific requirements of each particular case, the privacy impact assessment shall take into consideration the legal, technical and organizational impact, implications and coverage associated with the following core elements:

a) Stakeholder: Analyzes the impact of the initiative or project against the consent of the Stakeholder, specifically against aspects such as the type of data involved, the type and purposes of the Processing, the means to obtain authorization, the need to create, modify or delete requests for authorization or existing privacy notices.

b) Impact on third parties: Analyzes the impact of a certain operation or initiative, specifically regarding the technical and legal coverage in the relationship with the third party, as well as the verification mechanisms before, during and after the link with XPERIENCE, the type of responsibility of the third party regarding the provision of the information, the national or international scope of the eventual transmission or transfer of the information. Among others.

c) Impact vis-à-vis the authorities: Determines the compliance measures or actions vis-à-vis the authorities that exercise control and surveillance in the area of personal data protection, such as consultation in the event of processing initiatives that imply a high risk to privacy or to the rights of data subjects.

d) Impact within the organization: Determines the measures, coverage or adjustments appropriate to the understanding and validation of the Company's information cycle, as well as the recording of processing activities, implementing internal legal, technical and organizational coverage and measures or making the appropriate adjustments to existing ones.

12.4 PRIVACY RISK MANAGEMENT BY DESIGN AND BY DEFAULT

Article 5.1.f of the General Data Protection Regulation (GDPR) determines the need to establish adequate security safeguards against unauthorized or unlawful processing, against loss of personal data, accidental destruction or damage. This implies the establishment of technical and organizational measures aimed at ensuring the integrity and confidentiality of personal data and the possibility (Article 5.2) to demonstrate that these measures have been put into practice (proactive liability).

These measures of active responsibility are included among those that must be applied by the data controller prior to the beginning of the processing and also when it is being developed.

This type of measures reflects very directly the proactive responsibility approach. It is about thinking in terms of data protection from the very moment a treatment, product or service involving the processing of personal data is designed.

OBLIGATIONS.

- From the outset, XPERIENCE must take organizational and technical measures to integrate safeguards in the processing to effectively implement the principles of the GDPR.

- XPERIENCE must take measures to ensure that only necessary data is processed (minimization) in terms of the amount of data processed, the extent of processing, retention periods and accessibility of data.

- The technical and organizational measures should be established taking into account:

    - The cost of the technique.
    - Application costs.
    - The nature, scope, context and fines of the treatment.
    - Risks to rights and freedoms.

The minimum security measures are listed in XPERIENCE's personal data security and privacy guideline, which takes into consideration the following general guidelines:

12.5 Organizational measures:

- Definition of the functions of the personnel according to their responsibility for information management:

    - Security Manager
    - System Administrator,
    - User
    - Personnel without processing of personal data

- Obligations that affect all the Company's personnel

- Administrative procedures:

- Telephone request for personal information
- Paper waste
- Sending e-mails
- Receipt of resumes
- Notification of incidents
- Criteria for manual processing archiving,
- Payroll delivery

ü Temporary storage ü Clean
table policies ü Clean table
policies
ü Sending advertising by mailing

12.6 Technical measures: Comprises the measures and definitions associated with the following aspects:

- Treatment centers and premises

    - Physical access measures to the computer system
    - Anti-theft system
    - Anti-fire system
    - Data Protection Center
    - Air conditioning
    - Physical access measures to the paper file cabinet
    - Destruction of media

- Image capture with security cameras

    - Location of cameras
    - Location of monitors
    - Image preservation
    - Duty of disclosure
    - Labor control measures
    - Right of access to images

- Measures against jobs
- Operating systems and communications environment
- Computer system or applications for accessing treatments
- Safeguarding and protection of personal passwords
- Incident management

- Media management
- Backup and recovery management
- Pseudonymization and anonymization

13. INTEGRAL CORPORATE PROGRAM FOR THE PROTECTION OF PERSONAL DATA

The Company has developed a comprehensive corporate program for the sustainability of the personal data protection management and compliance model. This program has the following minimum elements:

a) Organic component:

It comprises the definition of the roles and responsibilities of the entire administrative structure of the Company in terms of data protection, articulating the different internal procedures with the functional duties and responsibilities for its different operational and administrative levels.

Without prejudice to the transversal responsibility of each collaborator and manager of The Company, the privacy oficial assumes the role of coordinating the corporate model of personal data protection.

The privacy officer shall report to the legal representative, Privacy Committee or other body representing senior management, for the purpose of enabling strategic planning and management of information governance and in particular of the personal data protection and privacy policy.

b) Programmatic component:

It comprises the annualized definition of the main programs, activities and initiatives to be developed by the Company for the sustainability of the management and compliance model in terms of personal data protection within the framework of the principle of "Accountability" and continuous improvement.

The annual corporate personal data protection program shall be submitted by the privacy oficial and approved by the legal representative, committee of.

privacy or such other body as determined by the Company for senior management representation

Without prejudice to the inclusion of other elements, the annual corporate personal data protection program shall include and develop the following activities:

- Training for the Company's personnel.
- Support to the operation in the analysis of legal, technical and organizational coverage associated with the relationship with Stakeholders, third parties and authorities.
- Internal verification, control and measurement.
- Formulation of improvement plans and actions, as well as follow-up and support for their implementation.
- Compliance with external reporting and monitoring of the regulatory environment.
- Presentation of annual internal reports to senior management on the current status of the personal data protection management and compliance model.

14. OTHER ASPECTS ASSOCIATED WITH THE PROCESSING OF PERSONAL DATA

14.1 USE OF THE DE MARK FOR ACTIVITIES INVOLVING THE PROCESSING OF PERSONAL INFORMATION.

Users, employees, suppliers or any third party with direct or indirect relationship with the Company shall refrain from carrying out without prior written authorization, any initiative or activity that involves the use of its name, banner, corporate name, symbol, logo, symbol, brand or any other distinctive sign of the Company, whose execution involves the processing of personal information. Any activity or initiative that is carried out without compliance with this requirement shall be the sole responsibility of its author(s) and/or promoter(s) and shall not generate any effects, commitments or liability for XPERIENCE.

14.2 USE OF THE INTERNET, APPLICATIONS, WEBSITES AND OTHER DIGITAL MEANS OF COMMUNICATION

XPERIENCE may develop applications, platforms, web pages or in general any type of computer system for internal or external purposes for one or multiple users, hereinafter referred to collectively or generically as "Applications".

The development of the applications may be carried out directly by the Company or t h r o u g h third party developers that supply, support or advise in the different phases of the development or in the technological infrastructure for its operation and maintenance.

The development, operation, maintenance and updating of Applications shall be carried out taking into consideration the standards, procedures and controls necessary to promote the security, privacy and adequate Treatment of the personal data involved.

Each Application will require the development of special terms and conditions of use, including a specific section for privacy and personal data protection conditions. In the absence of terms of conditions or specific section on personal data protection, the principles, postulates and other elements described in this policy will be applied.

The Company shall refrain from publishing or disclosing through the Internet or any other mass media, personal information of a sensitive nature of the Stakeholders with respect to which it exercises Treatment, except in those cases in which it is ensured that access is technically controllable to provide restricted knowledge only to the Stakeholders or authorized third parties in accordance with the legal terms.

Likewise, XPERIENCE shall refrain from disclosing or publishing information of a discriminatory or offensive nature or that may affect the particular conditions of vulnerability or defenselessness of the Data Subject.

14.3 VIDEO SURVEILLANCE SYSTEM

In order to protect its patrimonial interests and promote security in its facilities, the Company has designed within its procedures a protocol for

the request, access, review and eventual release of personal information captured by internal and/or external surveillance cameras.

The company will ensure the custody and availability of video surveillance images in accordance with its technical capabilities and requests for review of images received in compliance with its protocol.

15. FINAL PROVISIONS AND VALIDITY

15.1 MODIFICATIONS TO THE POLICY

XPERIENCE reserves the right to modify this policy at any time. For this purpose, it will publish a notice on its website 5 working days prior to its implementation and during the validity of the policy. In case of disagreement with the new personal information management policies, the data subjects or their representatives may exercise their rights as data subjects in the terms previously described. The databases in which the personal data will be registered will have a validity equal to the time the information is kept and used for the purposes described in this policy. Once such finality(ies) is (are) fulfilled and provided that there is no legal or contractual duty to keep your information, your data will be deleted from our databases.

15.2 CURRENT

Effective from September 7, 2021