DP 1001.02-Privacy Policy Lleida.net Colombia

LLEIDA SAS - co@lleida.net

Documentary Control

Date	Version	Modifications	Author
01/07/2015	1.0	Creation	Eva Pané
25/05/2018	1.1	Updated: e-mail address	Eva Pané
15/10/2019	1.2	Updated: contact person's job title and postal address	Eva Pané
2/11/2020	1.3	Reviewed without changes	Eva Pané

Distribution list

Departments
Lleida .net

Classification and status of the document

Document classification	Public

Document status	Approved

Index

1 Introduction

1.1 Aim

The Aim of this policy is to set out the management's commitment to Lleida.net on the privacy of personal data processed by Lleida.net on the territory of Colombia.

1.2 Scope of application

All members of Lleida.net, as well as all third parties identified in the scope of the Information Security Management System (ISMS).

1.3 Distribution

Approved by the Lleida.net Steering Committee, this Policy must be accessible to all persons included in the distribution list specified in the documentary control, through the appropriate channels.

1.4 Review

This Service Policy shall be reviewed and approved annually by the Security Committee. However, in the event of any relevant changes within the Organisation, whether operational, legal, regulatory, or contractual, the Policy shall be reviewed as and when necessary, thus ensuring that it always remains relevant.

Lleida.net - Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) - Edifici H1, 2a planta B - 25003 Lleida (Spain) - (+34) 973 282 300 - info@lleida.net

2 Privacy policy

General Company Information

Lleida SAS (the "Company"), NIT 900571038-3 and main offices at Calle 81 # 1155 Piso 9 Bogotá, and contact telephone +57 1 3819903 is a company committed to protecting the privacy, integrity, security and confidentiality of all identification, contact, sensitive and biometric data, and all other information that might or that may be associated with one or more specific or determinable natural persons (the "Personal Data") such as its customers, suppliers, employees, contractors, potential or current, and, in general, all Data Subjects registered in the Company's databases, information to which it has access and processes in the development of its commercial activity.

The Company carries out the Processing of Personal Data through activities that include the collection, storage, management, processing, creation of databases, circulation, segmentation, transfer, transmission, use and/or utilisation thereof.

The purpose of this Information Processing Policy required by Decree 1377 of 2013 (the "Policy") is to inform Data Subjects of their legal rights with respect to their Personal Data, to disclose the mechanisms and procedures to make them effective, to disclose who is responsible within the Company for dealing with queries, questions, claims and complaints and, finally, to disclose the purposes and Processing to which Personal Data will be subjected in the development of the Company's business activities.

Scope of this Policy

This Policy shall apply to all Processing of Personal Data carried out in the territory of the Republic of Colombia by the Company, through its employees and, where applicable, those third parties with whom the Company agrees to carry out all or part of any activity relating to, or in connection with, the Processing of Personal Data for which the Company is the Controller (as defined below).

The Policy shall also apply to the third parties with whom the Company may enter into Transmission contracts (as defined below), so that such third parties are aware of the obligations that will apply to them, the purposes to which they must be subject and the security and confidentiality standards that they must adopt when processing on behalf of the Company.

Main definitions

The most relevant terms of this Policy are defined below:

Term	Definition
Authorisation	It is the prior, express and informed consent of the Data Subject to carry out the Processing.
Authorised	It is the Company and all persons who, by virtue of the Authorisation and this Policy, are entitled to carry out the Processing.

Privacy Notice	It is the verbal or written communication generated by the Controller, addressed to the Data Subject, by means of which he/she is informed about the existence of the Policy, the way to access it, his/her rights and the purposes of the Processing.
Database	Means the organised set of Personal Data that is the subject of Processing, whatever the modality of its formation, storage, organisation and access.
Personal Data	It is any piece of information of any kind, linked or linkable to a specific or identifiable natural person or persons.
Public Data	Means Personal Data qualified as such according to the provisions of the law or the Political Constitution and that which is not semi-private, private or sensitive. Public data includes, among others, data relating to the civil status of individuals, their profession or trade, their status as a businessperson or public servant, and data that may be obtained without any reservation whatsoever. By their nature, public data may be contained, inter alia, in public registers, public documents, official gazettes and bulletins, duly enforced court rulings that are not subject to confidentiality.
Sensitive Data	Personal Data that could affect the privacy of the Data Subject or whose improper use could lead to discrimination, such as those that reveal trade union affiliations, racial or ethnic origin, political orientation, religious, moral or philosophical convictions, membership of trade unions, social organisations, human rights organisations or organisations that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sex life and biometric data.
In charge	The natural or legal person, public or private, who, alone or in association with others, carries out the Processing on behalf of the Controller.
Enabled	It is the legitimation expressly and in writing by means of a contract or document that takes its place, granted by the Company to third parties, in compliance with the applicable Law, for the Processing, converting such third parties into Processors.
Legitimised	These are those persons who may exercise the rights of the Data Subject, such as the Data Subject, accrediting their identity by the means at their disposal, the successors in title who accredit this quality, the representative and/or proxy accrediting themselves by means of a power of attorney or legal representation, the representatives of minors Data Subjects and those who, by stipulation in favour of another or for another, are accredited.
Law	It is Law 1581 of 2012, Decree 1377, Sentence C-748 of 2011, and the jurisprudence of the Constitutional Court related to personal data, and any regulation issued by the government regulating the legal precepts, which are in force at the time the Processing by the Company commences, as such Law may be amended from time to time and such amendment applies to the Processing carried out by the Company.
Manual	It is the document in which the policies and procedures to ensure proper compliance with the Law are set out.
Policy	This document contains the information processing policy required by Decree 1377, which contains the guidelines and directives in relation to the protection of personal data.

Lleida.net - Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) - Edifici H1, 2a planta B - 25003 Lleida (Spain) - (+34) 973 282 300 - info@lleida.net

Responsible	Any person whose Personal Data Processing activities are subject to compliance with this Policy by performing decision-making activities on databases containing Personal Data.
Holder	The natural person to whom the Personal Data, which may be stored in a Database, refers and who is the subject of the right to habeas data.
Transfer	It is the Processing that involves sending the information or Personal Data to a recipient, who is a Controller and is located outside or inside the country. In the Transfer, the recipient will act as the Controller and will not be subject to the terms and conditions of this Policy.
Transmission	It is the Processing that involves the communication of Personal Data within or outside the territory of the Republic of Colombia when its purpose is the performance of a Processing by the Processor on behalf of the Controller. In the Transfer, the recipient will act as Processor and will be subject to the Policy and the terms established in the Transfer contract.
Treatment	It is any systematic operation and procedure, whether electronic or not, that allows the collection, conservation, ordering, storage, modification, relation, use, circulation, evaluation, blocking, destruction and, in general, the processing of Personal Data, as well as its delivery to third parties through communications, consultations, interconnections, assignments, data messages.

Principles

In all Processing carried out by the Company, the Company as Controller, and its Processors and/or third parties to whom Personal Data is Transmitted, the principles established in the Law and in this Policy shall be complied with, in order to guarantee the Data Subjects' right to habeas data. These principles are:

Principle	Description
Restricted access	The Company may not make Personal Data available for access via the Internet or other media, unless technical and security measures are in place to control access and restrict access to Authorised Persons only. Personal Data may not be made available on the Internet or other means of mass dissemination or communication, unless access is technically controllable so as to provide restricted knowledge only to Data Subjects or Authorised third parties or the information is public.
Restricted circulation	Personal Data may only be Processed by Company personnel who have been Authorised to do so in accordance with the provisions of the Company, or who, as part of their duties, are in charge of carrying out such activities. Personal Data may not be disclosed to third parties, within or outside the territory of the Republic of Colombia, without the Authorisation or without the execution of a contract, in case there is a Transmission.
Confidentiality	The Processing shall be subject to strict confidentiality requirements and, therefore, the persons involved in the Processing shall maintain the

	confidentiality of the information, even after the relationship that gave rise to the Processing has been terminated.
Consent	Processing requires Authorisation, by any means that may be subject to subsequent consultation, including by means of unequivocal conduct, as established by Decree 1377.
Sensitive Data and diligence	Sensitive Data collected in the course of the Company's activities shall be treated with the utmost diligence to preserve its integrity, restricted access and security.
Purpose	Any processing activity must be carried out for the legitimate purposes mentioned in this Policy, and the Data Subject must be informed at the time of obtaining his or her consent.
Integrity	The Personal Data subject to Processing must be truthful, complete, accurate, up-to-date, verifiable and comprehensible. When in possession of Personal Data that is partial, incomplete, fractioned or misleading, the Company shall refrain from Processing it or request the Data Subject to complete or correct the information. The Company shall make its best efforts to maintain the integrity of the Personal Data contained in its Databases and the veracity of the same, implementing measures to verify and update the Personal Data.
Security	The Company must always carry out the Processing using the technical, human and administrative security measures necessary to maintain the confidentiality and security of the Personal Data. The aforementioned measures prevent them from being adulterated, modified, consulted, used, accessed, deleted or known by unauthorised third parties. The Company will adjust the Processing to the security standards regulated in the future by the competent authorities.
Separability of Databases	The Company shall maintain separately the Databases in which it has the status of Data Controller from those in which it has the status of Data Controller.
Temporariness	The Company will not use the Personal Data beyond the reasonable period of time required by the purpose for which the respective Data Subject was informed and will implement measures to ensure the deletion of the Personal Data when the purpose for which it was collected has been exhausted.
Transparency	When the Data Subject so requests, the Company shall provide him/her with information about the existence of the Personal Data concerning him/her or in relation to which he/she is Legitimised. The response to the request shall be provided by the same means or, at least, by a means similar to the one used by the Data Subject to request information and within the terms established by Law.
Post-treatment	All Personal Data that is not Public Data must be treated by the Controllers and Data Processors as confidential and under the security parameters set by the Superintendence of Industry and Commerce. Upon termination of such relationship, such Personal Data must continue to be Processed in accordance with the Policy, the Manual and the Law.

Lleida.net - Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) - Edifici H1, 2a planta B - 25003 Lleida (Spain) - (+34) 973 282 300 - info@lleida.net

Processing and Purposes

The Company, in the development of its commercial activities, will process Personal Data for the purposes indicated below and for those purposes that are accepted by the Data Subjects at the time of collection of their Personal Data. These purposes shall also apply to all Data Processors or third parties who have access to the Personal Data by virtue of Law, contract or other document that links them to the Company:

Purposes
Corporate and Administrative
Providing electronic communications certification services.
Managing all information necessary to comply with the Company's tax obligations and commercial, corporate and accounting records.
Complying with the Company's internal processes for supplier and contractor management.
Providing information to third parties for evaluation and classification of suppliers.
To carry out the process of archiving, updating systems, protection and custody of information and databases.
Performing analysis for the control and prevention of fraud and money laundering, including but not limited to consulting and reporting to restrictive lists and financial risk information centres.
Managing the Company's human resources, including but not limited to: • the evaluation of candidates interested in becoming employees of the Company, • requesting employment references • the employment relationship with the Company, • Obtain judicial, prosecutorial and disciplinary records, • Conduct security studies during your employment relationship with Lleída. • Conduct home visits and training processes, • Conduct general medical examinations, • Conduct performance appraisals, • To advance social welfare and occupational health programmes, • Issuing labour certifications, • Provide employment references if requested, • To shape the human map of the personnel working in the Company, • To know family and household composition information, • Pay the payroll, social security, social security and any other payments required by law.
Conducting data update campaigns to ensure data integrity.
Conducting internal investigations in accordance with various company policies in case of suspicious activities that may affect the good name of the Company (only applies to employees or service providers of the Company).
Verifying, access and monitor computer equipment and technological tools to which he/she has access.
Conducting financial due diligence processes for the analysis and investigation of the employee's financial behaviour.
Conducting video surveillance activities in areas of public use, inside and outside the premises.
Commercial and Marketing Activity

Implement communication channels between the customer, suppliers and other persons (natural or legal) relevant to the development of the Company's commercial activity.
Conducting surveys and/or opinion polls on products and services.
Carrying out marketing activities.
Conducting customer satisfaction and service quality surveys.

General
Supplementing information and, in general, carrying out the necessary activities to manage requests, complaints and claims submitted by the Company's customers and third parties, and direct them to the areas responsible for issuing the corresponding responses.
Transmiting the Personal Data to third parties with whom contracts for this purpose have been concluded or documents have been signed, such as other agreements or declarations, which allow the Personal Data to be transmitted, for commercial, administrative and/or operational purposes.
To comply with the purposes mentioned above, to transfer, transmit, move, share, deliver, and/or disclose Personal Data to third parties, within and outside the national territory, including to countries that do not provide adequate levels of protection for Personal Data.
Sending the modifications to this Policy, as well as the request for new authorisations for the Processing of Personal Data.
Other purposes determined by the Controller in processes of obtaining Personal Data for its Processing, in order to comply with legal and regulatory obligations, and the development of the Company's commercial activity.

1. Authorisation

All Processing must be preceded by obtaining the Authorisation. To this end, prior to the collection of Personal Data, the Company and the Authorised Parties must obtain the Authorisation signed by the Data Subject and keep a copy of this document for future reference.

2. Rights of Personal Data Subjects

In accordance with the Law, Data Subjects have the following rights:

Law	Description
Update	To update the Personal Data held in the Company's Databases to maintain its integrity and accuracy.
Knowledge and Access	Knowing and accessing your Personal Data vis-à-vis the Company or the Processors. This access will be free of charge at least once a month.
Test	Requesting proof of the Authorisation granted to the Company, unless the Law indicates that such Authorisation is not required or the Authorisation has been validated in accordance with the provisions of Article 10 of Decree 1377.
Complaint	Filing complaints before the Superintendence of Industry and Commerce for breaches of the Law when the procedural requirement has been exhausted by going to the Company in the first instance.
Correction	Rectifying information and Personal Data under the Company's control.
Revocation	Requesting the revocation of the Authorisation, provided that there is no legal duty or contractual obligation of the Data Subject with the Company,

	according to which such Personal Data must remain in the Company's Databases.
Application	To submit requests to the Company or the Controller regarding the use they have made of your Personal Data, and for them to provide you with such information.
Suppression	Requesting the deletion of their Personal Data from the Company's Databases, provided that there is no legal duty or contractual obligation of the Data Subject with the Company, according to which such Personal Data must remain in the Company's Databases.

Data Subjects may exercise their legal rights and carry out the procedures established in this Policy by presenting their identity card or any other identification document. Minors may exercise their rights personally or through their parents or adults who hold parental authority or legal representation, who must prove it through the relevant documentation. Likewise, the rights of the Data Subject may be exercised by all the Legitimate Parties upon presentation of the respective document.

3. Sensitive Data

Within the framework of its business activities, the Company may collect and Process Sensitive Data, such as medical information, images, photographs and/or voice recordings and, in general, biometric data. Other Sensitive Data relating to health, sex and any information whose Processing affects privacy may also be Processed. In this case, the Company shall inform the Data Subjects so that they may give their **independent and free** consent to the Processing of such Sensitive Data.

Sensitive Data will be treated with the greatest possible diligence and with the highest security standards. To this end, the area in charge of the Company will develop internal procedures to maintain at all times the confidentiality and integrity required by this type of information. Limited access to Sensitive Data shall be a guiding principle to safeguard the privacy of such data, whereby only authorised personnel shall have access to this type of information.

The Authorisation for the Processing of Sensitive Data is **optional and entirely discretionary for the Data Subject**, and **therefore** no activity will be restricted or conditioned to the provision of such data.

Personal Data Protection Area

The Company has a unit in charge of receiving and attending to Requests, Complaints and Claims related to Personal Data. This unit will process queries and complaints regarding Personal Data in accordance with the Law and this Policy. Some of the particular functions of this area in relation to Personal Data are as follows:

- Attending and receiving all requests from Data Subjects, processing and responding to those that are based on the Law or this Policy, such as: requests for updating, knowledge, deletion, revocation of authorisation when, in accordance with Decree 1377, such revocation is appropriate; as well as requests for information on the Processing and purposes given to their Personal Data, and requests to obtain proof of the Authorisation granted, when it has been granted in accordance with the Law.
- To respond to Data Subjects on those requests that do not proceed in accordance with the Law.

The contact details of the Security Officer are:

Contact details of the person and/or area in charge	
Unit, person and/or area in charge of data protection issues	Eva Pané Vidal
Physical address	Calle 81 # 1155 Piso 9 Bogotá
E-mail address	gdpr@lleida.net
Telephone	+ 57 1 381 9903
Position of contact person	Compliance Director

Procedures for exercising the rights of Data Subjects

a. Consultations

The Company has various mechanisms for the Data Controller or the Legitimised Parties to formulate all types of Queries relating to:

- The Personal Data of the Data Subject held in the Company's Databases.
- The treatment to which they are subjected.
- The purposes to be achieved.

The mechanisms used to submit Queries may be physical, such as over-the-counter processing, or electromagnetic, such as e-mail lopd@lleida.net. Whatever the means used, the Company will keep proof of the query and its response.

Before proceeding, the person responsible for dealing with the enquiry shall verify:

1. The identity of the Data Controller or the Legitimised Party. For this purpose, it shall require the original identity card or any other original identification document of the Data Controller and the special or general powers of attorney, in its case.
2. The Authorisation or contract with third parties that gave rise to the Processing by the Company.
3. It shall state the date on which the enquiry was received by the Company.

If the applicant has the capacity to make the query, the person responsible for dealing with the query shall collect all the information about the Data Subject that is contained in the individual record of that person or that is linked to the identification of the Data Subject within the Company's Databases. Once the information has been compiled, it shall be provided to the Data Subject so that he/she may have access to it and become acquainted with it.

The person responsible for dealing with the consultation shall reply to the applicant, provided that the latter is entitled to do so as the Data Subject or the Legitimised Party. This response will be sent within **ten (10) working days from the date on** which the request was received by the Company.

This response shall be mandatory even in cases where the applicant is deemed not to have the capacity to make the enquiry, in which case the applicant shall be informed accordingly and given the option to demonstrate interest and capacity by providing additional documentation.

In the event that the request cannot be dealt with within **ten (10) working days**, the applicant will be contacted to inform him/her of the reasons why the status of his/her request is being processed and to indicate the date on which the consultation will be dealt with, which in no case may exceed **five (5) working days** following the expiry of the first term. For this purpose, the same means or one equivalent to that by which the consultation was submitted shall be used.

The final response to all requests may not take **longer than fifteen (15) business days** from the date the initial request was received by the Company. For this reason, the Company will follow up on the queries submitted.

b. Claims

The Company shall have mechanisms in place for the Data Subject or the Legitimate Parties to make Claims with respect to:

- Personal Data Processed by the Company that should be corrected, updated or deleted;
- Alleged breach of the Company's legal duties.

These mechanisms may be physical, such as over-the-counter procedures, or electronic, such as e-mail. Whatever the means, the Company must keep proof of the consultation and the response, in case it is necessary to consult it at a later date.

The Claim must be submitted by the Data Subject or the Legitimate Parties, as follows:

- The Security Officer should be contacted electronically at gdpr@lleida.net or physically at Calle 81 # 1155 Piso 9 Bogotá.
- It shall contain the name and identification document of the Holder.
- It shall contain a description of the facts giving rise to the complaint and the objective pursued (updating, correction or deletion, or fulfilment of duties).
- It should indicate the address, contact details and identification of the complainant.
- It must be accompanied by all documentation that the claimant wishes to assert.

Before proceeding, the Complaint Handler will verify:

1. The identity of the Data Controller or its representative. For this purpose, it may require the ID card or any other identification document of the Data Controller, and the special or general powers of attorney of the representative, as the case may be.
2. The Authorisation or contract with third parties that gave rise to the Processing by the Company.
3. The date on which the claim was filed shall be fixed.
4. If the claim or additional documentation is incomplete, the Company shall require the claimant to rectify the deficiencies once only within **five (05) working days** of receipt of the claim. If the claimant fails to submit the required documentation and information within **two (02) months** from the date of the initial claim, the claim shall be deemed to have been withdrawn.

5. If, for any reason, the person who receives the complaint within the Company is not competent to resolve it, he/she shall refer it to the Data Protection Area - Customer Service Coordination, within **two (02) working days** of receiving the complaint, and shall inform the complainant of such referral.
6. Once the claim with the complete documentation has been received, a legend stating "claim in process" and the reason for the claim shall be included in the Company's Database where the Personal Data of the Data Subject subject to the claim is stored, within a term not exceeding two **(02) working days**. This legend shall be maintained until the claim is decided.
7. The maximum term to deal with the claim will be **fifteen (15) working days from** the day following the date of receipt. When it is not possible to deal with the claim within this period, the interested party will be informed of the reasons for the delay and the date on which the claim will be dealt with, which in no case may exceed eight (08) working days following the expiry of the first period.

Security policy

Lleída.net takes effective, appropriate and reasonable measures to protect your Personal Data, as it is obliged to guarantee an adequate level of protection and security of the same.

Modifications

This Policy may be amended from time to time by the Company and shall form part of the contracts entered into by the Company, where applicable. Any substantial modification of this Policy must be previously communicated to the Data Subjects through the means available to the Company, such as the Company's website and/or e-mails. Substantial modification means, among others, the following situations:

1. Modification in the identification of the area, unit or person in charge of dealing with queries and complaints.
2. Evident modification of the purposes that may affect the Authorisation. In this case the Company will seek a new Authorisation.

Modifications will be informed on the Company's website and/or by means of an e-mail that will be sent to the Personal Data Subjects, provided that the Company has such information in its possession.

Validity

This Policy will come into force on 1 July 2015. The Personal Data that is Processed will remain in the Company's Database, based on the criterion of temporality, for as long as it is necessary to comply with the purposes mentioned in this Policy, and for which it was collected. Thus, the validity of the Database is closely related to the purposes for which the Personal Data were collected.

Lleida.net - Parc Científic i Tecnològic Agroalimentari de Lleida (PCiTAL) - Edifici H1, 2a planta B - 25003 Lleida (Spain) - (+34) 973 282 300 - info@lleida.net