TABLE OF CONTENSTS

DATECSA S.A. PERSONAL DATA PROCESSING MANUAL

1. BASIS AND SCOPE OF APPLICATION

DATECSA S.A., headquartered in Yumbo, Valle del Cauca, identified with Tax Identification Number (NIT) 800.136.505-4, in its capacity as the Data Controller, hereby issues this Manual of Policies and Procedures for the Processing of Personal Data (hereinafter, the "Manual"), in compliance with the following:

- Articles 15 and 20 of the Political Constitution of Colombia.
- Article 17, paragraph (k), and Article 18, paragraph (f) of Statutory Law 1581 of 2012, which sets forth general provisions for the Protection of Personal Data (LEPD).
- Decree 1074 of 2015, which consolidates the provisions of Decree 1377 of 2013, regulating Law 1581 of 2012.
- Guidelines for the Implementation of the Accountability Principle, issued by the Superintendence of Industry and Commerce (SIC).

This Manual sets forth the principles, procedures, and mechanisms for the protection of personal data and for ensuring compliance with applicable regulations, while safeguarding the rights of data subjects.

This policy is mandatory and applies to all personal data databases and processing activities managed by DATECSA S.A., whether in physical or digital format, and to all individuals, employees, contractors, and third parties who access, manage, or carry out any type of processing of such data in the course of their duties and business activities.

2. SCOPE

- This document applies to all personal data and confidential information that is collected, stored, used, processed, transmitted, transferred, or exchanged within the databases and records of DATECSA S.A., whether in physical or digital formats.

- It applies to employees, contractors, suppliers, clients, shareholders, and third parties who are connected to DATECSA S.A. and who, by virtue of this relationship, access or manage personal information.

- Guidelines are established for the acquisition, collection, use, storage, processing, exchange, transfer, and transmission of personal data, ensuring respect for data subjects' rights and the application of the principles of legality, confidentiality, security, and restricted access.

- DATECSA S.A. and its employees are obligated to strictly comply with the provisions of Law 1581 of 2012, its regulatory decrees, and any other applicable regulations, ensuring the proper and secure handling of the information contained in its databases.
- This manual encompasses DATECSA S.A.'s internal data processing procedures, as well as the protection mechanisms applied in interactions with clients, suppliers, and any third party engaging with the organization.

3. APPLICABLE REGULATIONS

The processing of personal data by DATECSA S.A. is governed by the provisions established in both national and international regulations, ensuring respect for data subjects' rights and adherence to the guiding principles of personal data protection.

In Colombia, the primary regulatory framework includes:

Political Constitution of Colombia

- Article 15: Fundamental right of every individual to know, update, and rectify information collected about them in databases or records.
- Article 20: Right to receive truthful and impartial information and assurance of personal data protection.

Law 1581 of 2012

- General regulation on the protection of personal data in Colombia.
- Establishes the principles, rights, and obligations governing the processing of personal data.

Decree 1074 of 2015 (Chapters 25 and 26)

- Compiles and regulates decrees related to data protection in the country:
  - ✓ Decree 1377 of 2013: Regulates consent for the processing of personal data.
  - ✓ Decree 886 of 2014: Regulates the National Database Registry (RNBD).

Circular 01 of November 8, 2016 – SIC

- Issues accountability guidelines for companies to adopt technical, human, and legal measures to ensure the protection of personal data.

Accountability Guideline – SIC

- Advisory document issued by the Superintendence of Industry and Commerce that sets out management and control criteria for compliance with Law 1581 of 2012.

4. DEFINITIONS

DATECSA S.A. adheres to the following definitions in the processing of personal data, as established in Article 3 of Law 1581 of 2012 and Article 2.2.2.25.1.3 of Decree 1074 of 2015 (formerly Article 3 of Decree 1377 of 2013):

TERM	DEFINITION
Authorization	Prior, express, and informed consent of the Data Subject for the Processing of personal data.
Database	An organized set of personal data that is subject to Processing.
Cookies	Small pieces of information sent by a website and stored in the user's browser, allowing the website to track the user's previous activity. Their primary functions are: i) To manage session control when a user enters their username and password, so that they do not have to re-enter them on each page. However, cookies do not identify an individual but rather a combination of computer, browser, and user. ii) To gather information about the user's browsing habits, and potentially enable spyware attempts by advertising agencies and others. This can raise privacy concerns and is one of the main reasons why cookies have detractors.
Personal Data	Any information that is linked or may be associated with one or more identified or identifiable natural persons.
Public Data	Data that is not classified as semi-private, private, or sensitive. Public data includes, among others, information related to a person's marital status, profession or occupation, and their status as a merchant or public servant. By nature, public data may be found, among other sources, in public records, official documents,

TERM	DEFINITION
	gazettes and government bulletins, and duly finalized judicial rulings that are not subject to confidentiality.
Semi private Data	Data that is neither intimate nor reserved nor public in nature, and whose knowledge or disclosure may be of interest not only to the data subject but also to a specific sector, group of individuals, or society at large—such as financial, credit, and commercial information.
Private Data	Personal data that, due to its intimate or reserved nature, is of interest solely to its data subject.
Sensitive Data	Sensitive data refers to information that affects the privacy of the Data Subject or whose improper use could lead to discrimination. Examples of such data include: Information revealing racial or ethnic origin Political orientation Religious or philosophical beliefs Membership in trade unions, social or human rights organizations, or organizations that promote the interests of any political party or safeguard the rights and guarantees of opposition parties Data related to health, sexual life, and biometric information
Data Processor	A natural or legal person, whether public or private, who, independently or in association with others, processes personal data on behalf of the Data Controller.
Data Controller	A natural or legal person, whether public or private, who, independently or in association with others, determines the purposes and means of the database and/or the Processing of personal data.
Database Administrator	An employee responsible for overseeing and coordinating the proper implementation of data processing policies once the data has been stored in a specific database, as well as for executing the directives issued by the Data Controller and the Data Protection Officer.
Data Protection Officer (DPO)	The natural person responsible for coordinating the implementation of the legal framework for personal data protection and for handling requests from Data Subjects in the exercise of their rights as established under Law 1581 of 2012.
Data Subject	The natural person whose personal data is subject to Processing.
Processing	Any operation or set of operations performed on personal data, such as collection, storage, use, circulation, or deletion.

TERM	DEFINITION
Privacy Notice	A verbal or written communication issued by the Data Controller and addressed to the Data Subject regarding the Processing of their personal data, through which the subject is informed of the existence of applicable data processing policies, how to access them, and the purposes for which the personal data will be processed.
Transfer	A data transfer occurs when the Data Controller and/or Data Processor, located in Colombia, sends personal data or information to a recipient who, in turn, acts as a Data Controller and is located either within or outside the country.
Transmission	The Processing of personal data that involves its communication within or outside the territory of the Republic of Colombia, for the purpose of Processing by the Data Processor on behalf of the Data Controller.

5. PRINCIPLES

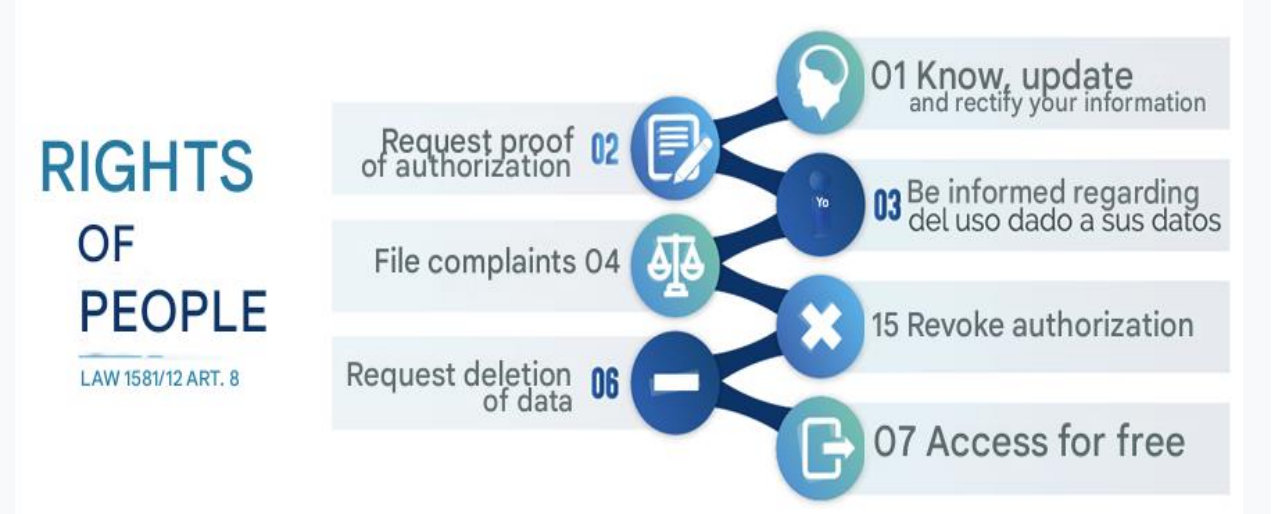
Article 4 of Law 1581 of 2012 sets forth the guiding principles for the processing of personal data. These principles shall be applied harmoniously and comprehensively in the development, interpretation, and enforcement of the Law, ensuring the respect for and protection of data subjects' rights.

The principles governing the processing of personal data at DATECSA S.A. are as follows:

PRINCIPLE	DESCRIPTION
Legality	The processing of data is a regulated activity that must comply with the provisions of Law 1581 of 2012, Decree 1074 of 2015 (which consolidates Decrees 1377 of 2013 and 886 of 2014), as well as any other complementary or amending regulations.
Purpose	The processing of personal data must pursue a legitimate purpose, which must be communicated to the data subject.
Freedom	The processing of personal data may only be carried out with the prior, express, and informed consent of the data subject. Data may not be obtained or disclosed without the subject's authorization or without a legal or judicial mandate that waives the requirement for consent.
Accuracy or Quality	Information subject to processing must be truthful, complete, accurate, up-to-date, verifiable, and understandable. The processing of partial, incomplete, fragmented, or misleading data is prohibited.

PRINCIPLE	DESCRIPTION
Transparency	The data subject must be able to obtain, at any time and without restrictions, information from DATECSA S.A. regarding the existence of personal data concerning them.
Restricted Access and Circulation	Processing may only be carried out by individuals authorized by the Data Subject and/or by persons provided for under the Law. Personal data, except for public information, must not be made available on the Internet or through other means of mass dissemination or communication, unless access is technically controllable to ensure restricted knowledge for the Data Subjects or third parties authorized in accordance with the law.
Security	Information subject to processing must be protected through the necessary technical, human, and administrative security measures to prevent its adulteration, loss, consultation, unauthorized use, or fraudulent access.
Confidentiality	All individuals involved in the processing of personal data that is not of a public nature are obligated to maintain the confidentiality of the information, even after the termination of their relationship with any of the activities related to processing. The disclosure of personal data may only occur in connection with activities authorized under Law 1581 of 2012 and under the terms established therein.

6. RIGHTS OF DATA SUBJETCS



In accordance with Article 8 of Law 1581 of 2012 and Article 2.2.2.25.4.1 of Decree 1074 of 2015 (which consolidates Articles 21 and 22 of Decree 1377 of 2013), data subjects have a set of rights regarding the processing of their personal data.

These rights may be exercised by the following individuals:

- The Data Subject, who must verify their identity through the means provided by DATECSA S.A.
- Their successors, who must prove such status.
- The Data Subject's legal representative and/or attorney-in-fact, upon verification of representation or legal power of attorney.
- By stipulation in favor of or for the benefit of another.

The rights of children and adolescents shall be exercised by those legally authorized to represent them.

The rights of the Data Subject are as follows:

6.1 Right to Make Inquiries

Data Subjects have the right to be informed by the Data Controller about the origin, use, and purpose of their personal data.

Data Subjects or their successors may request to consult the personal information held in the databases of DATECSA S.A. To do so, they must submit a clear, precise, and detailed request including the identification of the Data Subject and the specific data being consulted.

DATECSA S.A.'s Data Protection Officer shall process such inquiries in accordance with the timeframes established under Law 1581 of 2012.

6.2 Right to File Complaints and Claims

The Data Subject or their successors may file claims if they believe that the information contained in the databases should be corrected, updated, deleted, the authorization revoked, or if they identify a potential violation of data protection regulations.

The types of claims include:

- **Correction Claim**: The right to update, rectify, or modify data that is partial, inaccurate, incomplete, fragmented, misleading, or subject to prohibited or unauthorized processing.

- **Deletion Claim:** The right to request the removal of data that is inappropriate, excessive, or that does not comply with constitutional and legal principles, rights, and guarantees.
- **Revocation Claim:** The right to revoke previously granted authorization for the processing of personal data.
- **Violation Claim:** The right to request the remediation of breaches in personal data protection regulations.

Important: Requests for the deletion of information and the revocation of authorization shall not be admissible when the Data Subject has a legal or contractual obligation to remain in the database.

6.3 Right to Request Proof of Authorization Granted to the Data Controller

The Data Subject has the right to request proof of the authorization granted to the Data Controller, except in cases where authorization is not required, in accordance with Article 10 of Law 1581 of 2012.

6.4 Right to file complaints with the Superintendence of Industry and Commerce

The Data Subject or their successors may file a complaint with the Superintendence of Industry and Commerce (SIC) when they believe their right to personal data protection has been violated.

Important: In order for the SIC to intervene, the Data Subject must first exhaust the internal consultation or claims process with DATECSA S.A.

Potential Sanctions for Non-Compliance

According to Chapter 2 of Law 1581 of 2012, the Superintendence of Industry and Commerce (SIC) may impose sanctions on the Data Controller or Data Processor in the event of non-compliance. These sanctions may include:

- Fines of up to 2,000 current legal monthly minimum wages (CLMMW), which may be imposed repeatedly while the non-compliance persists.
- Suspension of data processing activities for up to six (6) months.
- Temporary shutdown of data processing operations if corrective measures ordered by the SIC are not implemented within the designated timeframe.
- Immediate and permanent shutdown in cases of non-compliance involving the processing of sensitive data that affects the rights of the Data Subjects.

7. PROCEDURES FOR EXERCISING DATA SUBJECT RIGHTS

7.1 Right of Access of Inquiry

In accordance with Article 2.2.2.25.4.2, Section 4, Chapter 25 of Decree 1074 of 2015 (Article 21 of Decree 1377 of 2013), the Data Subject has the right to know, access, and request information stored in any database managed by DATECSA S.A.

Access to information shall be free of charge in the following cases:

- Once per calendar month.
- Whenever there are substantial modifications to the data processing policies that justify new inquiries.

For additional inquiries within the same calendar month, DATECSA S.A. may charge only the costs of reproduction, delivery, and document certification, ensuring that such charges do not exceed the actual cost of recovering the corresponding materials. If requested by the Superintendence of Industry and Commerce (SIC), DATECSA S.A. must provide evidence to support these expenses.

Procedure to Exercise the Right of Access or Inquiry:

The Data Subject may exercise their right of access by submitting a request to DATECSA S.A. through the following channels:

- **Email:** tratamientodatospersonales@datecsa.com, with the subject line "Exercise of Right of Access or Inquiry."
- **Postal Mail:** Calle 15 # 29 A-11, Módulo C, Parque Logístico Empresarial, Acopi Yumbo, Valle del Cauca.

The request must include the following information:

1. Full name of the Data Subject.
2. Copy of the Data Subject's ID card; if submitted by a representative, a copy of the representative's ID and the document proving representation.
3. A clear and precise description of the request specifying the access or inquiry being made.
4. Notification address and contact details of the requester.
5. Date and signature of the requester.
6. Any supporting documents relevant to the request, if applicable.

Means of Delivering the Response:

The Data Subject may choose one of the following methods to receive the requested information:

- Hard copy sent via certified or regular mail.
- Email or other electronic means.
- Another appropriate method offered by DATECSA S.A., depending on the nature of the processing and database setup.

Response Timeframe:

- Standard Response Time: DATECSA S.A. shall respond to the inquiry within a maximum of ten (10) business days from the date of receipt of the request.
- Extension: If the request cannot be addressed within the initial timeframe, the Data Subject will be informed before the deadline, with an explanation for the delay and a new response date, which shall not exceed an additional five (5) business days.

These timeframes are established under Article 14 of Law 1581 of 2012.

Appeal to the Superintendence of Industry and Commerce (SIC):

If, after completing the consultation process, the Data Subject or their successor believes that DATECSA S.A. has not properly addressed their right, they may file a complaint with the Superintendence of Industry and Commerce (SIC), in accordance with Law 1581 of 2012.

7.2 Right to File Complaints and Claims

The Data Subject or their representative may exercise their right to file a claim if they believe that the information contained in DATECSA S.A.'s databases should be corrected, updated, or deleted; if they detect an alleged breach of data protection regulations; or if they wish to revoke their authorization for data processing.

Procedure for Filing a Claim:

The claim must be submitted to DATECSA S.A. through the following means:

- Email: tratamientodatospersonales@datecsa.com (with the subject line "Exercise of the Right to File a Claim")

- Postal Mail: Calle 15 # 29 A-11, Módulo C, Parque Logístico Empresarial, Acopi – Yumbo, Valle del Cauca.

The claim must include the following information:

1. Full name of the Data Subject.
2. Copy of the Data Subject's ID; if submitted by a representative, a copy of the representative's ID and the document proving representation.
3. A clear and precise description of the facts supporting the claim and the specific request (correction, deletion, revocation, or breach).
4. Notification address and contact information.
5. Date and signature of the requester.
6. Any additional supporting documents, if applicable.

Timeframes for Processing the Claim:

- Incomplete Claims: If the claim is incomplete, DATECSA S.A. will request the missing information within five (5) business days of receiving the claim.
- Claimant's Response Period: If the claimant does not respond within two (2) months from the date of the request, it will be understood that they have withdrawn the claim.
- Database Annotation: Once a complete claim is received, DATECSA S.A. will include a note in the database stating "claim in process," along with the reason for the claim, within no more than two (2) business days. This annotation will remain until the claim is resolved.
- Response Period: DATECSA S.A. will respond to the claim within a maximum of fifteen (15) business days from the date of receipt.
- Extension: If the claim cannot be addressed within this timeframe, the claimant will be notified before the initial deadline, with an explanation of the delay and a new response date, which shall not exceed an additional eight (8) business days.

Appeal to the Superintendence of Industry and Commerce (SIC):

If, after completing the claims process, the Data Subject or their successor believes that DATECSA S.A. has not adequately addressed their right, they may file a complaint with the Superintendence of Industry and Commerce (SIC), in accordance with Law 1581 of 2012.

8. DATA CONTROLLER

In accordance with the provisions of Law 1581 of 2012, the Data Controller of the databases covered by this policy is DATECSA S.A., whose contact details are as follows:

Corporate Name: DATECSA S.A.
Tax Identification Number (NIT): 800.136.505-4
Registered Office: Yumbo, Valle del Cauca, Colombia
Address: Calle 15 # 29A - 11, Módulo C, Parque Logístico Empresarial Acopi
Email: tratamientodatospersonales@datecsa.com
Phone: (602) 6957070

Data Protection Officer (DPO)

DATECSA S.A. has appointed a Data Protection Officer (DPO) responsible for ensuring compliance with the provisions of Law 1581 of 2012 and its supplementary regulations, as well as for addressing inquiries, complaints, or claims from data subjects.

Name: Claudia Patricia Insuasty Rodríguez
Position: Compliance Officer
Email: tratamientodatospersonales@datecsa.com
Phone: (602) 6957070 Ext. 1128

Data subjects may exercise their rights of access, correction, update, deletion, or revocation of authorization by submitting their request to the Data Protection Officer (DPO) through the contact channels listed above.

9. DATA PROCESSORS

Data Processors are natural or legal persons, whether public or private, who carry out the Processing of personal data on behalf of DATECSA S.A., in accordance with Law 1581 of 2012 and its regulatory framework.

As the Data Controller, DATECSA S.A. may engage third parties (Data Processors) to process personal data on its behalf, in accordance with the purposes defined in this policy.

Obligations of Data Processors:

Data Processors must comply with the following obligations:

- Comply with the principles established in Law 1581 of 2012 and this Manual.
- Apply all applicable regulations regarding personal data protection.
- Implement technical, administrative, and organizational security measures to safeguard personal data.
- Ensure the security, confidentiality, and integrity of the information.
- Process personal data solely for the purposes authorized by DATECSA S.A.
- Follow DATECSA S.A.'s instructions and restrict data processing to the purposes defined in data transfer agreements.
- Adopt technical, organizational, and security measures to prevent unauthorized access, misuse, loss, or alteration of personal data.
- Limit access to personal data to individuals who require it for the performance of their duties.
- Immediately notify DATECSA S.A. of any security incident compromising the information, in accordance with the terms set out in this Manual.

Contractual Relationship with Data Processors:

Before engaging a Data Processor, DATECSA S.A. will verify that the entity has adequate security measures in place and will require the execution of a Personal Data Transfer Agreement, which shall include:

- The specific purposes for processing the personal data.
- The Data Processor's obligations regarding security and confidentiality.
- An express prohibition on using the data for purposes other than those authorized.
- Procedures for managing security incidents and reporting data breaches.
- A commitment to return, delete, or anonymize personal data once the processing purpose has been fulfilled.

Data Processors must report any incident involving misuse, unauthorized access, or compromise of personal data integrity, in compliance with DATECSA S.A.'s security protocols.

10. APPOINTMENT OF THE DATA PROTECTION OFFICER

DATECSA S.A. shall appoint a Data Protection Officer (DPO), who will be responsible for ensuring compliance with applicable personal data protection regulations, in accordance with Law 1581 of 2012, Decree 1074 of 2015, and other complementary regulations.

The Compliance Officer will assume this role, acting as the liaison between DATECSA S.A. and the supervisory authorities on matters related to personal data protection. The DPO's main responsibilities include:

- Ensuring compliance with the principles and obligations established in data protection regulations.
- Implementing, coordinating, and supervising internal policies and procedures related to personal data processing.
- Conducting monitoring and evaluation plans regarding the processing of personal data within DATECSA S.A.
- Addressing and managing inquiries, requests, and claims submitted by Data Subjects.
- Coordinating the implementation of security measures to safeguard personal information.
- Ensuring staff training and awareness regarding personal data protection.
- Serving as the point of contact with the Superintendence of Industry and Commerce (SIC) in the event of inspections or inquiries related to personal data processing.

For any inquiry or request regarding the processing of personal data, Data Subjects may contact the Data Protection Officer via email at: tratamientodatospersonales@datecsa.com.

11. DATA SUBJECT AUTHORIZATION

In accordance with Law 1581 of 2012, the processing of personal data requires the prior, express, and informed authorization of the Data Subject, which must be obtained by any means that allows for subsequent consultation.

DATECSA S.A. has implemented mechanisms to ensure that authorization is obtained in a clear and verifiable manner. Authorization may be obtained through the following means:

- Physical or digital registration forms
- Website
- Electronic data messages
- Any other mechanism that evidences the Data Subject's intent

To request the Data Subject's authorization, DATECSA S.A., in its capacity as the Data Controller, has adopted procedures to ensure the collection of consent, including:

- **F-P10-01** – Registration, Engagement and/or Update of Third Parties
- **F-P10-18** – Registration, Engagement and/or Update of International Third Parties
- **F-P10-22** – Client Engagement Form for Datecsa Express
- **F-P8-20** – Employee Registration and/or Update Form

If the purpose of data processing undergoes a substantial change, DATECSA S.A. shall request a new authorization from the Data Subject.
Pursuant to Article 10 of Law 1581 of 2012, authorization from the Data Subject shall not be required in the following cases:

- Information required by a public or administrative entity in the exercise of its legal duties or pursuant to a court order
- Prevention, detection, monitoring, and control of money laundering and terrorist financing (ML/TF)
- Publicly available data (as defined in Article 3 of Law 1581 of 2012)
- Medical or health emergencies
- Processing of information authorized by law for historical, statistical, or scientific purposes
- Data related to the Civil Registry of Persons

12. REQUEST FOR AUTHORIZATION FROM THE DATA SUBJECT

DATECSA S.A., in its capacity as the Data Controller, shall request the Data Subject's authorization prior to and/or at the time of collecting their personal data.

This authorization must be obtained expressly and in an informed manner, clearly indicating the specific purpose for which the data is requested, in accordance with Article 2.2.2.25.2.2 of Decree 1074 of 2015 (which consolidates Article 7 of Decree 1377 of 2013).

To ensure proper collection of authorization, DATECSA S.A. will implement mechanisms that allow for proof of consent, which may include:

- **Written:** Physical or digital forms signed by the Data Subject.
- **Automated:** Technological tools that record the Data Subject's express acceptance.

- **Unequivocal Conduct:** Actions that clearly demonstrate the Data Subject's consent, noting that silence shall not be construed as authorization.

Important Notes:

- If the purpose for processing personal data changes substantially, DATECSA S.A. will request a new authorization from the Data Subject.
- When personal data is collected through authorized third parties, DATECSA S.A. will ensure that such third parties have obtained the necessary prior authorizations.

13. PURPOSES OF DATA PROCESSING

In the course of its business operations, DATECSA S.A. processes personal data related to natural persons, which is stored and managed in databases designated for legitimate purposes, in accordance with the Constitution and the Law.

Document I-P1-04 Database Organization contains information regarding the various databases managed by the company and the specific purposes assigned to each for data processing.

The purposes for which personal data is processed include:

CUSTOMERS	SUPPLIERS	EMPLEADOS Y EX - EMPLEADOS
▪ Profile analysis ▪ Citizen/customer Service (Management of Queries, Requests, and Complaints -PQR) ▪ Data update campaigns and information about changes in personal data processing ▪ Opinion surveys ▪ Sending communications	▪ Citizen/customer Service (PQR management) ▪ Data update campaigns and information about changes in personal data processing ▪ Training ▪ Internal statistics management ▪ Administrative management ▪ Management of collections and payments ▪ Billing management	▪ Training ▪ Granting and management of permits, licenses, and authorizations ▪ Schedule control ▪ Health control and management ▪ Declaration and payment of social security contributions ▪ Exercise of rights ▪ Internal statistics managment

CUSTOMERS	SUPPLIERS	EMPLEADOS Y EX - EMPLEADOS
▪ Customer loyalty programs ▪ Internal statistics management ▪ Administrative management ▪ Client management ▪ Management of collections and payments ▪ Billing management ▪ Economic and accounting management ▪ Fiscal management ▪ Commercial relationship histories ▪ Marketing ▪ Offering of products and service ▪ Commercial prospecting ▪ Own advertising administrative procedures ▪ Reception and management of internal and external requirements concerning products and services ▪ Related to the corporate purpose of the organization ▪ Registration of document entries and exits ▪ Sending of information to data subjetcs	▪ Supplier management ▪ Economic and accounting management ▪ Fiscal management ▪ Commercial relationship histories ▪ Epidemiological research and related activities ▪ Social benefits ▪ Occupational risk prevention ▪ Administrative procedures ▪ Reception and management of internal and external requirements concerning products and services ▪ Registration of document entries and exits ▪ International comercial relations ▪ Related to the corporate purpose of the organization ▪ Sending of information to data subjetcs ▪ Reservations and issuance of transport tickets ▪ Security ▪ Verification of data and references, respecting at all times the basec principles established by the law.	▪ Sanctions management, admonishments, attention calls, exclusions ▪ Administrative management ▪ Collections and payments management ▪ Pensión fund management ▪ Economic and accounting management ▪ Personnel training ▪ Payroll management ▪ Management of personnel ▪ Temporary employment management ▪ Medical history ▪ Employee information ▪ Epidemiological research and similar activities ▪ Private investigations on individuals ▪ Social benefits ▪ Certification services provision ▪ Benefits, subsidies, and other economic benefits ▪ Administrative procedures ▪ Occupational risk prevention ▪ Prevention and promotion programs ▪ Employment promotion and management ▪ promoción y selección de personal ▪ Staff promotion and selection

CUSTOMERS	SUPPLIERS	EMPLEADOS Y EX - EMPLEADOS
▪ Reservations and issuance of transport tickets ▪ Market segmentation ▪ Decision Support systems ▪ Remote selling ▪ Verification of data and references		▪ Labor relations and working conditions ▪ Registration of document entries and exits ▪ Requests by regulatory bodies – Non -sensitive data ▪ Requests by regulatory bodies – Private and/or sensitive data ▪ Health ▪ Security ▪ Health risk verification ▪ Data and references verification ▪ Video surveillance

SHAREHOLDERS	VIDEO SUVEILLANCE
▪ Citizen/customer Service (management of queries, requests, and complaints – PQR) ▪ Data update campaigns and information on changes in personal data processing ▪ Administrative procedures ▪ Reservations and issuance of transports tickets ▪ Administrative management ▪ Collections and payments management ▪ Billing management ▪ Economic and accounting management ▪ Tax and collection management ▪ Notarial records ▪ Visa/reidency applications ▪ Registration of shares and obligations	▪ Security

- Verification of data and references, always respecting the fundamental principles established by the law.

14. DATA LIFECYCLE

The data lifecycle encompasses all stages through which personal data passes within DATECSA S.A., from its collection to its final disposition. Proper management of each phase ensures compliance with Law 1581 of 2012 and other applicable regulations.

14.1. Collection

Personal data will be collected through mechanisms authorized by DATECSA S.A., such as physical or electronic registration forms, contracts, counterparty records, digital consents, among others. It shall be ensured that:

- Prior, express, and informed authorization from the Data Subject is obtained.
- The Data Subject is informed about the purpose and processing of their data.
- Data collection is limited to that which is strictly necessary for the intended purposes.

14.2. Storage

- Collected data will be stored in physical or digital media with appropriate security measures.
- Access will be restricted to authorized personnel only.
- Security controls such as encryption and user authentication will be applied.
- The integrity and availability of the information will be guaranteed.

14.3. Use and Circulation

- The use of personal data must comply with the established purposes and data protection principles.
- Data may only be used by authorized departments or third parties.
- Unauthorized or improper use of information is prohibited.
- Data will be updated in accordance with current regulations.

14.4. Retention

- Personal data will be retained only for the time necessary to fulfill the purpose for which it was collected or as required by applicable regulations.
- DATECSA S.A.'s document retention schedule will determine retention periods.
- Data will be stored with security measures that ensure its integrity and confidentiality.

14.5. Final Disposition or Deletion

Once the data processing purpose has been fulfilled, the data will be securely deleted, unless there is a legal or contractual obligation requiring its retention.

The deletion of personal data will be documented and traceable.

Secure deletion methods will be applied, such as permanent deletion from digital databases and physical destruction for paper records.

In cases of data anonymization, it will be ensured that data cannot be reverted to its original state.

14.6. Responsibilities in Data Lifecycle Management

Data Controllers and Processors must apply the policies and controls established at each stage.

Periodic audits will be conducted to verify compliance with procedures for data collection, storage, use, and deletion.

Requests for access or deletion from Data Subjects will be handled according to the procedures outlined in this Manual.

15. BIOMETIC DATA PROCESSING

DATECSA S.A. processes biometric data exclusively for security purposes, identity authentication, and regulatory compliance. The processing of this data is carried out in accordance with Law 1581 of 2012 and other applicable data protection regulations, ensuring the confidentiality, integrity, and availability of the information.

15.1. Types of Biometric Data Processed

DATECSA S.A. collects and processes biometric data in the following cases:

- **Fingerprints:** Collected in contracts and supplier records, which may be stored in physical or digital format within the company's internal platforms.
- **Facial recognition:** Used exclusively for employees in counterpart onboarding processes.
- **Access control and security:** Use of video surveillance systems for monitoring and protecting company facilities.

15.2. Purpose of Processing

Biometric data is used solely for:

- Authentication and identity validation during contracting and counterpart onboarding processes.
- Access control and facility security through video surveillance systems.
- Enforcement of security policies established in the Data Processing Manual and Internal Security Policies.
- Identity verification of employees in counterpart due diligence processes to prevent fraud and identity theft.

15.3. Protection and Security of Biometric Data

To ensure the security of biometric data, DATECSA S.A. implements the following measures:

- Access to biometric data is restricted to authorized personnel only.
- Secure storage of contracts and counterpart records on internal platforms with controlled access.
- Use of video surveillance systems with limited access and monitoring in accordance with security protocols.
- Implementation of technical security measures to prevent unauthorized access, loss, alteration, or misuse.
- Compliance with data protection and information security regulations, ensuring the confidentiality and privacy of data subjects.

15.4. Retention and Deletion of Biometric Data

Biometric data will be retained only for as long as necessary to fulfill the purpose for which it was collected, in accordance with applicable regulations:

- Facial recognition data collected during counterpart onboarding will be retained only as long as needed for identity validation.
- Fingerprints included in supplier contracts and records will be stored according to the retention periods established in current regulations and the company's internal policies.
- Video surveillance recordings will be retained in accordance with the security guidelines outlined in the Internal Security Policies.

15.5 Transfer and Access to Third Parties

DATECSA S.A. will not share biometric data with third parties, except in the following cases:

- When legally or judicially required by a competent authority.
- For purposes of internal audits or regulatory compliance.
- When there is a data transfer agreement with third parties that guarantees adequate security measures.

16. PROCESSING OF MINORS' DATA

In compliance with Article 7 of Law 1581 of 2012, the processing of personal data of children and adolescents (minors) is prohibited, except in the exceptional cases provided in Article 2.2.2.25.2.9 of Decree 1074 of 2015 (which consolidates Article 12 of Decree 1377 of 2013), and under the following conditions:

- It must serve and respect the best interests of the child or adolescent.
- It must ensure respect for their fundamental rights.

Procedure for Processing Minors' Personal Data:

- **Authorization from the Legal Representative**

DATECSA S.A. will request the prior, express, and informed authorization of the minor's legal representative.

- **Exercise of the Right to Be Heard**

Before processing any data, the child or adolescent will be given the opportunity to express their opinion regarding the authorization of their personal data. This opinion will be assessed based on their maturity, autonomy, and level of understanding.

- **Responsibilities of the Data Controller and Processor**

DATECSA S.A., as well as any data processor, must ensure the appropriate and secure use of the personal data of minors, in full compliance with the principles and obligations set forth in Law 1581 of 2012 and its regulatory framework.

- **Commitment to Education and Prevention**

✓ It is the duty of the State and educational institutions to educate legal representatives about the risks of the improper use of minors' personal data.
✓ DATECSA S.A. will promote awareness of the responsible and secure use of minors' personal data, their right to privacy, and the protection of their information.

- **Exercise of Minors' Rights**

  The rights of access, correction, deletion, revocation, or claims for violations involving minors' data may only be exercised by individuals legally authorized to represent them, in accordance with applicable regulations.

17. DATA SECURITY IN PROCESSING

In compliance with the security principle established in Article 4 of Law 1581 of 2012 and Decree 1074 of 2015, DATECSA S.A. has adopted technical, human, and administrative measures to protect personal data from unauthorized access, alteration, loss, or fraudulent use.

These measures are aligned with the company's internal security policies, as well as its IT and cybersecurity policies, ensuring the confidentiality, integrity, and availability of information.

17.1 Data Processing Security

DATECSA S.A. ensures that personal data processing is carried out under the following guidelines:

- Implementation of access controls to restrict data use to authorized personnel only.
- Application of encryption and authentication measures for handling electronic data.
- Procedures for the detection, management, and reporting of security incidents involving personal data.
- Regular internal audits to assess compliance with data protection policies.

17.2. Security Controls Implemented

To safeguard personal data, DATECSA S.A. has implemented security measures at multiple levels:

Physical Security

- Access control to areas where sensitive information is handled.
- Implementation of video surveillance systems in facilities where personal data is processed.
- Restricted access to physical files containing confidential information.

Digital Security

- Use of encryption protocols for transmitting personal data.
- Implementation of two-factor authentication for access to databases and internal systems.
- Continuous monitoring of information systems to detect suspicious activities.
- Security controls applied to cloud storage tools.

Protection Against Cyberattacks

- Enforcement of secure usage policies for corporate devices and email.

- Use of firewalls, antivirus software, and intrusion prevention systems.
- Restriction on downloading sensitive information to unauthorized devices.

17.3. Documents Regulating Security Measures

The specific security measures applied to personal data processing are outlined in the following internal documents:

- **Internal Security Policies (PO-P10-02):** Document governing technical and administrative security measures for personal data protection at DATECSA S.A.
- **IT and Cybersecurity Policies (PO-P9-01):** Document setting forth rules and procedures for IT security and protection against cyber threats.
- **Information Assurance Controls (I-P9-01):** Specific controls applied in the management of personal data.

17.4. Access to Internal Security Policies

The Internal Security Policies include detailed information on the management of information security risks, including:

- Access control to personal data
- Authentication and encryption mechanisms
- Physical and logical security measures
- Management of security incidents
- Data backup and recovery procedures

These documents are for internal use and can be accessed by employees via DATECSA S.A.'s internal documentation platform, and by authorized contractors.

18. RISK MANAGEMENT ASSOCIATED WITH DATA PROCESSING AND CONTROL AND MONITORING MECHANISMS

DATECSA S.A. has identified risks related to the processing of personal data and has implemented controls to minimize potential negative impacts that could harm the organization. This is achieved through the implementation of internal security policies and a risk management system established under procedure **P-P11-09: Identification, Evaluation, Control, and Monitoring of Risks at DATECSA S.A.**, along with the necessary

tools, indicators, and resources for its administration. The system will be adapted according to changes in the organizational structure, internal processes, and the volume of personal data processed.

The risk management system identifies risk sources such as technology, human resources, infrastructure, and processes requiring protection, along with their vulnerabilities and threats, in order to assess risk levels. To ensure the protection of personal data, factors such as access authorization levels, identification of events that may compromise information, and the implementation of preventive measures will be considered.

Examples of events or situations that may pose risks include:

- **Criminal acts:** Actions that violate the law and are punishable, such as fraud or unauthorized access to information.
- **Physical incidents:** Natural or technical events, as well as those indirectly caused by human intervention.
- **Negligence or institutional failures:** Omissions or poor decisions that affect information security.

Control and Compliance Mechanisms

As part of its risk management approach, DATECSA S.A. will implement internal audit and oversight mechanisms to evaluate compliance with this Manual and data protection regulations. These controls aim to ensure that data is processed in accordance with applicable laws and the principles of security and confidentiality.

Control Measures:

- Periodic review of databases and procedures for the collection, storage, and deletion of personal data.
- Annual training sessions on personal data protection for employees with access to personal information.
- Annual request for data processing policies from Data Processors to verify their alignment with applicable regulations and contractual obligations established with DATECSA S.A.
- Internal audits to ensure compliance with the policies outlined in this document.
- Recording and analysis of security incidents, along with the development of improvement plans to prevent future data breaches.

These measures contribute to the continuous improvement of personal data processing security and help ensure compliance with data protection principles and accountability obligations.

19. INCIDENT NOTIFICATION, MANAGEMENT, AND RESPONSE PROCEDURE

Objective:

DATECSA S.A. has established a procedure for the notification, management, and response to incidents in order to ensure the confidentiality, availability, and integrity of the information contained in databases under its responsibility.

Scope of Application:

This procedure applies to all users, employees, contractors, suppliers, and other individuals who, in the course of their duties, access, store, process, or consult personal data managed by DATECSA S.A.

Incident Notification and Response Procedure:

- **Incident Identification:**

  If any individual becomes aware of an incident that affects or may affect the confidentiality, availability, or integrity of information protected by DATECSA S.A. or any of its Data Processors, they must immediately report it to the Compliance Officer.

Incidents include, but are not limited to:

- ✓ Loss or deletion of personal data without authorization.
- ✓ Theft or robbery of information from physical or digital databases.
- ✓ Unauthorized access to personal data.
- ✓ Alteration, modification, or leakage of personal data without authorization.
- ✓ Any other action that compromises personal data security.

- **Incident Notification:**

The notification must be made immediately and must include the following information:

- ✓ Type of incident.
- ✓ Date and time of occurrence.
- ✓ Affected area or process.
- ✓ Involved individuals (if applicable).
- ✓ Detailed description of the event and its impact.
- ✓ Initial measures taken to mitigate the impact.

Upon receipt of the notification, the Compliance Officer must issue an acknowledgment confirming receipt and detailing the information provided.

- **Incident Registration and Management:**

DATECSA S.A. will register the incident using Form F-P1-08 – Security Event Report, including:

- ✓ Report details.
- ✓ Description of the event.
- ✓ Actions taken in response to the incident.
- ✓ Identification of affected information assets.
- ✓ Person responsible for incident management.
- ✓ Impact analysis and risk assessment.

A responsible party will be assigned to investigate and analyze the security event or incident.

The process will be documented, and a Security Incident Report will be prepared, including lessons learned and recommendations.

- **Corrective Measures and Data Recovery:**

DATECSA S.A. will implement necessary procedures to recover any affected personal data, where possible.

If recovery is not possible, this will be recorded in the corresponding report.

- **Notification to the Superintendence of Industry and Commerce (SIC):**

In compliance with Law 1581 of 2012, when an incident compromises personal data, the Compliance Officer must notify the Superintendence of Industry and Commerce (SIC) via the National Database Registry (RNBD) within 15 business days of detecting the incident.

- **Notification to Data Subjects:**

When it is determined that an incident has significantly affected the rights of Data Subjects, DATECSA S.A. will promptly notify them, indicating:

- ✓ Type of incident.

- ✓ Compromised data.
- ✓ Measures taken to mitigate the impact.
- ✓ Recommendations for Data Subjects in case of risk

- **Monitoring and Continuous Improvement:**

- ✓ DATECSA S.A. will monitor incident management through the Continuous Improvement Procedure P-P11-03.
- ✓ Registered incidents will be evaluated to define preventive and corrective actions that strengthen information security.

20. TRANSFER OF DATA TO THIRD COUNTRIES

In compliance with Title VIII of Law 1581 of 2012 and Article 2.2.2.25.6.1 of Decree 1074 of 2015, DATECSA S.A. ensures that any transfer of personal data to third countries is carried out only to jurisdictions that provide adequate levels of personal data protection.

20.1 Restrictions on International Data Transfers

- **General Prohibition**

The transfer of personal data to countries that do not provide adequate levels of protection is prohibited, except when:

- ✓ Express authorization is obtained from the Data Subject.
- ✓ There is a data transfer agreement in place with adequate security measures.
- ✓ The Superintendence of Industry and Commerce (SIC) authorizes the transfer in exceptional cases.
- ✓ The data is required by a public authority in the exercise of its legal functions.

- **List of Countries with Adequate Protection Levels**

The Superintendence of Industry and Commerce (SIC) has recognized the following countries as providing an adequate level of personal data protection:

- ✓ **Americas:** United States, Costa Rica, Mexico, Peru, Argentina, Uruguay, Canada.

- ✓ **Europe and Asia:**

  Germany, Australia, Austria, Belgium, Bulgaria, Cyprus, Croatia, Denmark, Slovakia, Slovenia, Estonia, Spain, Finland, France, Greece, Hungary, Ireland, Iceland, Italy, Japan, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, United Kingdom, Czech Republic, Romania, Serbia, Sweden.

- ✓ **Other countries recognized by the European Commission as having adequate protection:** Switzerland, Guernsey, Isle of Man, Jersey, Faroe Islands, Andorra, Israel, New Zealand, Republic of Korea.

If DATECSA S.A. needs to transfer data to a country not listed above, it must obtain authorization from the SIC.

20.2 Accountability Principle

In accordance with the accountability principle, DATECSA S.A. ensures that any international transfer of personal data is based on:

- **Compliance assessment:** Verification that the receiving country meets adequate security and privacy standards.
- **Data transfer agreements:** Execution of agreements containing personal data protection clauses aligned with Colombian law.
- **Security measures:** Recipients will be required to implement technical and organizational measures to prevent unauthorized access, loss, or alteration of transferred data.
- **Supervision and audits:** Periodic reviews of the data processing conditions in the receiving countries.

To ensure compliance with these requirements, DATECSA S.A. will request that international data processors provide their personal data processing and information security policies.

21. DISCOSURE OF PERSONAL DATA TO AUTHORITIES

DATECSA S.A. guarantees the protection of personal data and compliance with applicable regulations. However, in cases where a public or administrative entity, in the exercise of its legal duties, or a judicial authority, requests access to and/or delivery of information contained in its databases, the following procedure shall be followed:

21.1. Request Validation

Before disclosing any information, DATECSA S.A. will verify the following:

- **Legitimacy of the request:** The request must come from an entity legally empowered to request the information.
- **Purpose of the request:** The request must be evaluated to ensure it aligns with the legitimate objectives of the requesting authority.
- **Relevance of the requested data:** The requested information must be strictly necessary and proportionate to the stated purpose.

21.2. Procedure for Data Disclosure

- **Receipt of the request:**

✓ The request must be submitted through an official channel and must include the legal basis for the request.
✓ It must clearly specify the data requested and the intended purpose.

- **Review and authorization:**

✓ The Compliance Officer or designated department will assess the legality and relevance of the request.
✓ If there is any doubt regarding the legitimacy of the request, additional clarification may be requested from the issuing authority.

- **Documentation and registration:**

✓ A **Personal Data Disclosure Record** will be prepared, containing:

  - Requesting authority and responsible official
  - Legal basis for the request
  - Supplied data
  - Commitment from the authority to uphold the Data Subject's rights
  - Signatures of the involved parties

- **Delivery of the information:**

✓ Data will be provided securely and in compliance with personal data protection regulations.
✓ Encryption or appropriate security measures will be used for digital transmissions.

- **Notification to the Data Subject (when applicable):**

- ✓ If permitted by law, DATECSA S.A. may notify the Data Subject of the request for their information.
- ✓ In cases where such notification could obstruct a judicial investigation, the company will refrain from informing the Data Subject.

21.3. Guarantee of Data Subject Rights Protection

DATECSA S.A. will ensure that any disclosure of personal data to authorities is carried out based on the principles of necessity, proportionality, and legality, guaranteeing the protection of the Data Subject's rights and minimizing the risk of any breach of their information.

22. NATIONAL DATABASE REGISTRY – RNBD

Registration Obligation

DATECSA S.A., as the Data Controller, is required to register and update its databases in the National Database Registry (RNBD), managed by the Superintendence of Industry and Commerce (SIC), in accordance with Law 1581 of 2012 and Decree 886 of 2014.

Deadlines for Registration

Databases must be registered within the following timeframes:

- Existing databases: Must be registered in the RNBD within the deadlines established by the Superintendence of Industry and Commerce (SIC).
- New databases: Must be registered within two (2) months of their creation.

Registry Updates

DATECSA S.A. will update the information registered in the RNBD in the following situations:

Change in the purpose of data processing.

Modification of the Data Controller's contact information.

Change in the structure of the database.

Implementation of new security measures.

Other significant modifications related to personal data processing.

Reporting of Security Incidents

If a security incident occurs that compromises the confidentiality, integrity, or availability of personal data, DATECSA S.A. must report it in the RNBD within fifteen (15) business days of its detection, in accordance with External Circular 02 of 2022 issued by the SIC.

Responsible Party for the Registry

The Compliance Officer is responsible for managing the registration and updating of databases in the RNBD, ensuring compliance with current regulations.

23. WEB POLICY

DATECSA S.A. ensures the protection of personal data collected through its website and sets forth the following provisions regarding the collection, processing, and storage of user information.

23.1. Browsing Data

It is possible to visit DATECSA S.A.'s website without providing personal information. However, the browsing system and the software required for the website's operation may collect certain personal data implicitly transmitted via Internet communication protocols.

Data collected may include:

- IP address or domain name of the device used to access the website
- Referring URL
- Date and time of access
- Operating system parameters and browser type
-

This data is used solely for statistical purposes, to improve the user experience, and to ensure the proper functioning of the website.

The information collected will not be used to personally identify users unless it is associated with third-party data in compliance with a legal or contractual obligation.

23.2. Contact and Registration Forms

When using the website's contact or registration forms, users may choose to provide personal information (name, email, phone number, etc.) Such data will be used exclusively to respond to inquiries, provide information, or process user requests.

DATECSA S.A. will ensure the protection of this information in accordance with applicable personal data protection regulations.

23.3. Use of Cookies and Web Analytics Tools

DATECSA S.A. uses session cookies and web analytics tools to enhance the user experience on its website.

Session cookies are not stored permanently on the user's device and are deleted upon closing the browser. Their purpose is to enable secure and efficient access to website content.

Users may configure their browsers to accept, reject, or delete cookies at any time. However, disabling cookies may affect the website's functionality.

DATECSA S.A. may use analytics tools such as Google Analytics to measure website traffic and improve its services.

If users wish to prevent their information from being collected by Google Analytics, they can install the opt-out browser add-on available at: https://tools.google.com/dlpage/gaoptout

23.4. Information Protection and International Transfers

Data collected through the website will not be shared with third parties, except in the following cases:

- When necessary to fulfill legal or contractual obligations
- When required by government authorities in the exercise of their legal functions
- When the user has provided express consent for the data transfer

DATECSA S.A. implements technical and administrative security measures to protect user information from unauthorized access or misuse.

23.5. Amendments to the Website Policy

DATECSA S.A. reserves the right to modify this policy at any time, in accordance with regulatory changes or improvements in website security. Any updates will be communicated through the website.

24. DOCUMENT MANAGEMENT

Documents containing personal data must be easily retrievable and managed under criteria of security and traceability. To this end, DATECSA S.A. has established mechanisms for the identification, storage, retention, inspection, and final disposition of physical and digital documents, ensuring compliance with applicable regulations.

24.1. Storage and Retention

- The storage location of each document must be recorded, whether in physical or digital format.
- Periodic inspections will be conducted along storage routes to verify integrity and accessibility.
- Document retention must be carried out under appropriate security conditions, considering environmental factors, storage locations, and associated risks.
- Retention periods will be determined based on applicable legal requirements and DATECSA S.A.'s internal policies.
- Final disposition of documents must be clearly defined—whether recycled, reused, retained, or digitized—in accordance with internal procedures:

  - ✓ P-P11-01 – Document Control
  - ✓ P-P11-02 – Records Control
  - ✓ P-P8-05 – File Organization in accordance with the Document Retention Schedule and Document Transfers

24.2. Document Control and Modification

- Documents containing personal data must be created and managed by authorized and qualified personnel.
- To ensure traceability, documents must be coded according to procedure P-P11-01 Document Control.
- The creation, modification, or deletion of documents may only be carried out by designated personnel and must be recorded using form F-P11-01 Document Management Request.
- Documents will only be modified when strictly necessary.

24.3. Document Protection and Security

- Both physical and digital documents must be protected against unauthorized access, alterations, or loss.
- The guidelines established in the following information security policies must be followed:

- ✓ PO-P9-01 – IT and Cybersecurity Policies
- ✓ PO-P10-02 – Internal Security Policies

- Digital documents must have encryption and restricted access measures according to their level of confidentiality.

24.4. Document Distribution and Custody

- The distribution of documents containing personal data will be carried out solely by the Data Controller, who will document evidence of the distribution.
- Each delivery must specify:
  - ✓ The type of document
  - ✓ The identity of the recipient
  - ✓ The purpose of the delivery
- All personnel are responsible for ensuring the confidentiality, integrity, and availability of documents containing personal data.
- Each staff member must safeguard the documents under their responsibility, ensuring both physical and digital protection.
- Documents removed from custody must be identified and easily traceable.

25. TRAINING

Proper handling of personal data is not only the responsibility of DATECSA S.A. as an organization but also of each of its employees. To ensure compliance with data protection regulations, all employees and individuals with access to databases containing personal information must receive regular training in this area.

25.1. Training Objectives

- The purpose of the training programs is to:
- Raise awareness among employees about the importance of personal data protection.
- Provide information on Law 1581 of 2012 and its regulatory decrees.
- Explain DATECSA S.A.'s data protection policy.
- Ensure compliance with security measures in the processing of personal data.
- Prevent incidents that may compromise the confidentiality, integrity, and availability of information.
- Inform staff about the consequences of non-compliance with the regulations.

25.2. Training Plan

DATECSA S.A. will implement a Personal Data Protection Training Plan, which will include:

- **Induction:** Initial training for new employees focused on the data protection policy and established security measures.
- **Periodic training:** Regular updates on new regulations, internal policies, and emerging risks in data protection.
- **Specialized training:** Targeted instruction for employees with access to sensitive data or who hold critical roles in personal data processing.
- **Drills and practical exercises:** To strengthen incident response related to information security.

25.3. Staff Obligation

- All DATECSA S.A. employees must attend and actively participate in scheduled training sessions.
- Each employee must understand and apply the security measures related to the processing of personal data, in accordance with their responsibilities.
- A culture of data protection will be promoted throughout the organization to reduce risks and ensure regulatory compliance.

25.4. Consequences of Non-Compliance

- Any failure to properly manage and protect personal data, whether due to ignorance or negligence, may result in disciplinary actions, including:
- Internal warnings or sanctions
- Termination of employment for just cause
- Potential legal actions, including administrative, civil, and/or criminal proceedings under applicable law

26. SANCTIONS

Failure to comply with personal data processing policies, information confidentiality, or any other obligation related to data protection established in this Manual or in applicable regulations shall be considered a serious offense and may lead to disciplinary, contractual, and legal sanctions, as appropriate.

26.1 Types of Sanctions

Depending on the severity of the violation and its impact, DATECSA S.A. may apply the following sanctions:

- **Internal disciplinary sanctions:**

- ✓ Verbal or written warnings
- ✓ Administrative or labor-related sanctions, as established in the Internal Work Regulations
- ✓ Temporary suspension from duties without pay
- ✓ Termination of employment for just cause, in accordance with the Colombian Labor Code

- **Legal actions:**
- ✓ Complaints or administrative proceedings before the Superintendence of Industry and Commerce (SIC), in accordance with Law 1581 of 2012
- ✓ Civil and/or criminal proceedings, when the violation constitutes a criminal offense, such as data leakage, unauthorized access to information systems, or misuse of personal data
- ✓ Fines or financial penalties resulting from regulatory non-compliance

- **Sanctions imposed by the Data Protection Authority (SIC):** Under Article 23 of Law 1581 of 2012, the Superintendence of Industry and Commerce may impose sanctions for violations in the processing of personal data, including:
- ✓ Fines of up to 2,000 current legal monthly minimum wages (CLMMW)
- ✓ Suspension or shutdown of operations involving personal data processing
- ✓ Immediate and permanent closure of operations in cases involving sensitive data breaches

26.2 Criteria for Applying Sanctions

To determine the appropriate sanction in each case, DATECSA S.A. will consider factors such as:

- Severity of the infraction
- Impact caused to the company, Data Subjects, or third parties
- Intent or negligence in the action
- Recurrence of non-compliance
- Corrective measures implemented by the offender after the breach

26.3 Staff Responsibility

All employees, executives, contractors, and third parties with access to personal data under the responsibility of DATECSA S.A. are required to comply with the provisions of Law 1581 of 2012, its regulatory decrees, this Manual, and the Internal Security Policies.
Lack of awareness of applicable rules and procedures does not exempt any individual from responsibility for actions or omissions that breach personal data processing regulations.

27. MANUAL UPDATES AND DISSEMINATION

To ensure compliance with current regulations and the continuous improvement of personal data management, DATECSA S.A. has established the following process for updating and disseminating the Personal Data Processing Manual:

- **Review frequency:** The Personal Data Processing Manual will be reviewed at least once a year or whenever regulatory changes require it.
- **Update process:** Any modifications must be approved by the Data Protection Officer and General Management. Changes will be documented, and the updated version will be recorded with the revision date, in accordance with the document control procedure **P-P11-01**.
- **Dissemination:** All employees and third parties with access to personal data will receive a digital copy and notification of any updates. The manual will be available on DATECSA's website at https://www.datecsa.com/gobierno-corporativo and on the internal DGNET platform.
- **Training sessions:** Internal training sessions will be held to reinforce knowledge on personal data protection.

28. VALIDITY

The databases under the responsibility of DATECSA S.A. will be processed for as long as reasonably necessary to fulfill the purpose for which the personal data was collected, in accordance with the principles of purpose and necessity established in Law 1581 of 2012.

Once the data processing purpose has been fulfilled, and without prejudice to any legal or contractual provisions to the contrary, DATECSA S.A. will proceed to delete the personal data in its possession, ensuring the secure disposal of the information in accordance with internal procedures and best information security practices.

Exceptions to data deletion include:

- When there is a legal obligation to retain the data for a specified period (e.g., labor, tax, or commercial regulations).

- When the data is required to comply with current contractual obligations.
- When the information is necessary for the exercise of the right to defense in administrative or judicial proceedings.

As such, the databases managed by DATECSA S.A. have been created without a defined expiration period, unless otherwise required by law.

Policy update and validity

This Personal Data Processing Policy shall enter into force on the date of its publication and will remain in effect until modified or repealed by DATECSA S.A. Any substantial changes to this policy will be communicated to Data Subjects via their registered contact channels, and published on the company's official website.

Version control			
Issue date	**Versión Number**	**Description of creation or modification**	**Approval**
March 19, 25	00	Moves from the P10 administrative and financial process to the P1 compliance process. Includes cookie definition and data lifecycle. Data processing manager point Includes data protection officer functions. Unifies with web processing policies.	Gerente General