




Servicebots AI

# Comprehensive Personal Data Management Program

Version 2.0


Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

Control de Emisión		
Prepared By	Reviewed By	Approved By
Analyst Systems	CTO	CEO

## VERSIONS

VERSIÓN	DATE	CHANGES
1.0	22-03-2023	Initial Version
2.0	18-04-2023	Changes of document



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

## TABLE OF CONTENTS

VERSIONS.....1

TABLE OF CONTENTS .....2

1. INTRODUCTION.....3

2. SCOPE .....4

3. DEFINITIONS .....4

4. TRAINING AND AWARENESS .....5

5. DATA PROCESSING POLICY.....6

6. DATA PROCESSING PRINCIPLES.....7

7. DATA CONTROLLERS, DATA PROCESSING AND DUTIES.....8

8. CLASSIFICATION OF PERSONAL DATA .....9

9. PERSONAL DATABASES .....10


10. PROCESSING OF DATABASES.....13

11. PROCEDURES .....15

12. DATA PROCESSING AUDIT POLICY.....17

13. CHANGES .....20

14. VALIDITY.....20

Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

## 1. INTRODUCTION

We are a company committed to protecting private and confidential information obtained in the ordinary course of our business relationships and in the development of our corporate purpose.

The data processing policy is developed in compliance with Articles 15 and 20 of the Political Constitution; Articles 17 (k) and 18 (f) of Statutory Law 1581 of 2012, which establishes general provisions for the Protection of Personal Data (LEPD); and Article 13 of Decree 1377 of 2013, which partially regulates the aforementioned law. This policy will apply to all personal data registered in databases subject to processing by the data controller.


Our policies and procedures are based on the aforementioned legal framework, aimed at protecting the information entrusted to us. It is our intention to collect only the information voluntarily provided by our Clients, Contractors, Suppliers, Employees, Former Employees, Visitors, among others.

This information may be obtained through any of the following channels or means:

- a) Commercial, contractual, or professional relationship with the respective Client, Supplier, or other third parties;
  - b) Employment relationship with Employees and Former Employees;
  - c) Application to selection processes;
  - d) Enrollment in training, contests, seminars, or courses;
  - e) Enrollment and access to educational platforms, pedagogical content, among others;
- and
- f) Sending emails requesting information.

We must mention that by providing, delivering, or sending any type of personal information to ServiceBots, the Data Owner accepts that such information will be used in accordance with this Personal Data Processing Policy.

We establish this Personal Data Processing Policy in compliance with the provisions of Law 1581 of 2012 and Decree 1377 of 2013. It details the mechanisms by which our Company ensures the proper and strict handling of the Personal Data collected in its databases, allowing Data Owners to exercise their right to **habeas data**. Similarly, the main purpose of

Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

this policy is to inform Data Owners of their rights, the procedures, and mechanisms provided by ServiceBots to enforce those rights, and to make them aware of the scope and purpose of the Processing to which their Personal Data will be subjected, in case the Data Owner grants their express, prior, informed, and voluntary Authorization.

## 2.SCOPE


Define the guidelines and procedures by which **Servicebots IA** commits to protecting the personal information it collects, processes, and stores, whether in digital or paper format, in compliance with Law 1581 of 2012 and its regulatory decrees. Additionally, it aims to implement demonstrated accountability for the processing of personal data through the implementation, development, and monitoring of the Comprehensive Personal Data Management Program.

## 3.DEFINITIONS

Established in Article 3 of Law 1581 of 2012 and Article 3 of Decree 1377 of 2013.

- **Authorization:** The prior, express, and informed consent of the Data Subject for the processing of personal data.
- **Privacy Notice:** A verbal or written communication generated by the data controller, directed to the Data Subject for the processing of their personal data, informing them of the existence of applicable data processing policies, how to access them, and the purposes of the processing intended for the personal data.
- **Database:** An organized set of personal data that is subject to processing.
- **Financial Data:** Any personal data related to the origin, execution, and termination of monetary obligations, regardless of the nature of the contract that gives rise to them, and whose processing is governed by Law 1266 of 2008 or regulations that complement, modify, or add to it.
- **Personal Data:** Any information linked or that can be associated with one or more identifiable natural persons.
- **Public Data:** Data that is not semi-private, private, or sensitive. Public data includes, among others, information related to an individual's marital status, profession or trade, and status as a merchant or public servant. By nature, public data may be



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


found in public records, public documents, official gazettes, and duly executed judicial decisions not subject to confidentiality.

- **Private Data:** Data that is only relevant to the Data Subject.
- **Sensitive Data:** Data that affects the privacy of the Data Subject or whose misuse could lead to discrimination, such as data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, membership in trade unions or social organizations, human rights organizations, or those promoting the interests of political parties, as well as data related to health, sexual life, and biometric data.
- **Data Processor:** A natural or legal person, public or private, who, alone or jointly with others, processes personal data on behalf of the data controller.
- **Former Employee:** A natural person who was previously employed by **ServiceBots**.
- **Supplier:** A natural or legal person who provides goods or services to **ServiceBots** under an existing commercial or contractual relationship.
- **Data Controller:** A natural or legal person, public or private, who, alone or jointly with others, decides on the database and/or the processing of personal data.
- **LEPD:** The Statutory Law for data protection.
- **Data Subject:** A natural person whose personal data is subject to processing.
- **Transfer:** The transfer of data occurs when the data controller and/or data processor, located in Colombia, sends the information or personal data to a recipient who is also a data controller, either inside or outside the country.
- **Processing:** Any operation or set of operations on personal data, such as collection, storage, use, circulation, or deletion.

## 4. TRAINING AND AWARENESS

**Servicebots** will ensure that all employees are trained and made aware of personal data protection, their individual responsibilities in protecting such data, and the procedures and policies established in this plan or in the Information Security and Cybersecurity Training and Awareness Plan.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


## 5. DATA PROCESSING POLICY

The data processing policy of **Servicebots** is defined through the **Information Security Management System (ISMS)**, which is responsible for establishing the organization's policies, procedures, and plans.

The policies and privacy notice are reviewed annually by the Administration department and the Data Protection Officer (DPO). When adjustments are necessary, the following activities are carried out:

- The DPO, together with the ISMS, drafts changes or documents associated with the policy.
- The DPO presents the draft documents with adjustments at the monthly meetings of the **Information Security and Document Management Committee** to ensure their relevance.
- Once the committee approves the adjusted documents, the ISMS Manager validates them.
- The DPO delivers the validated documents to the ISMS.
- After the meeting and the formal approval, the personnel is informed through the necessary electronic means, and if required, it is also reported to the **National Registry of Personal Data (RNBD)** of the **Superintendence of Industry and Commerce**.
- The policy is then communicated to the different data owners, and their authorization is requested for data processing according to the new policy. If there are substantial changes in the content of the data processing policies related to the identification of the controller and the purpose of the processing of personal data, which may affect the content of the authorization, **Servicebots** must inform the data owner before or at the time of implementing the new policy. Additionally, the company must obtain new authorization from the data owner when the change relates to the purpose of the processing.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


## 6. DATA PROCESSING PRINCIPLES

**Servicebots** is committed to the proper processing of personal data. Therefore, all activities related to data handling must ensure the application of the following principles, which are aligned with those established in Article 4 and Article 2 of Law 1581 of 2012:

- **Legality Principle:** Throughout the personal data processing lifecycle—from capture, storage, to deletion—it is necessary to comply with legal provisions, using the data for purposes that are lawful and aligned with the regulatory framework.
- **Purpose Principle:** All personal data collected in the performance of educational and administrative functions must have specific purposes in line with the intended processing. Data owners must be informed about the purpose of the data processing.
- **Freedom Principle:** Personal data collection, storage, and processing can only be done with the prior, express authorization of the data owner, who must be informed about the data processing purpose. Disclosure or sharing of personal data without authorization or legal provision is prohibited.
- **Truthfulness or Quality Principle:** The organization must ensure that the personal data under processing is truthful, accurate, complete, and updated to avoid errors in the treatment.
- **Transparency Principle:** Data owners must be able to access information about their personal data being processed at any time.
- **Restricted Access and Circulation Principle:** Only authorized individuals or those allowed by law may process personal data.
- **Security Principle:** Personal data must be protected with adequate security standards, implementing operational, technical, and human measures to prevent loss, alteration, or unauthorized access.
- **Confidentiality Principle:** The organization must ensure the confidentiality of personal data that is not classified as public data. All individuals with access to personal data must handle it in a way that avoids exposure to unauthorized third parties.





Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

## 7. DATA CONTROLLERS, DATA PROCESSING AND DUTIES

### 7.1. Data Controller

- Without exception, any request, complaint, or claim related to data handling, as outlined in Law 1581 of 2012 and Decree 1377 of 2013, must be sent to:
- **Company: Servicebots S.A.S**
- **Address:** Carrera 19ª # 122-88
- **Email:** info@servicebots.ai
- **Phone:** (601) 9174722


### 7.2. Attention to Data Subjects

- From the **Administrative and Human Resources Department of SERVICEBOTS S.A.S.**, the Data Protection Officer will handle requests, consultations, and complaints submitted by the data owners, in accordance with Section 15, "Roles and Responsibilities."
- **Company: Servicebots S.A.S**
- **Address:** Carrera 19ª # 122-88
- **Email:** andres.marin@servicebots.ai
- **Phone:** (601) 9174722

### 7.3. Data Processing and Purpose of Databases

- **SERVICEBOTS**, in the course of its business activity, processes personal data related to individuals, which is contained in databases for legitimate purposes, complying with the Constitution and the Law.
- The personal data of end customers, suppliers, contractors, employees, former employees collected or stored in our databases will be processed with the following purposes:  
**End Customers:** ServiceBots will use the information provided for:
  - Executing the contractual relationship with customers, suppliers, and workers, including payment of contractual obligations.
  - Providing required services and/or products to users.
  - Informing about new products or services and changes to them.
  - Registering employee and/or pensioner information (both active and inactive) in the ServiceBots databases.
  - Sending promotional information via email, text message (SMS/MMS), or other analog/digital communication methods.
  - Sharing personal data with affiliated or related companies located in Colombia or abroad for the purposes indicated herein.
  - Supporting internal and external audit processes.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


- **Suppliers, Contractors, Employees, and Former Employees:** ServiceBots will use the information for:
  - Analyzing and selecting potential suppliers or contractors.
  - Communicating policies and procedures for supplier engagement.
  - Monitoring, auditing, and preventing fraud, among other legitimate business purposes.
  - For the processing of sensitive personal data and data related to children and adolescents, ServiceBots complies with Law 1581 and relevant regulations. The collection of such data requires the express authorization of legal representatives, especially for minors, and their best interest must be considered.

## 8. CLASSIFICATION OF PERSONAL DATA

**Servicebots S.A.S.** uses the classification of personal data listed in the **National Registry of Databases**, including general, identification, location, sensitive, socio-economic, and other data categories. The types of personal data processed by the organization are:

- **General identification data:** Name, surname, type of identification, identification number, date and place of issuance, marital status, gender, etc.
- **Specific identification data:** Nationality, other identification documents, place and date of birth or death, age, etc.
- **Morphological description data:** Skin color, iris color, hair color and type, particular marks, height, weight, body type, etc.
- **Location data related to private activity:** Address, telephone, email, etc.
- **Health-related data:** Orders and records of supplementary tests such as lab tests, imaging, endoscopic, pathological studies, etc.
- **Data on people with disabilities.**
- **Financial, credit, and/or economic rights data.**
- **Socioeconomic data:** Social stratum, homeownership, etc.
- **Data related to economic activity.**
- **Data related to educational level, training, and academic history.**
- **General data on affiliation and contributions to the Integrated Social Security System:** EPS, IPS, ARL, dates of enrollment/withdrawal from EPS, AFP, etc.
- **Personal data for access to information systems:** Usernames, IP addresses, passwords, profiles, etc.



Information Security Management System (ISMS)	 SERVICEBOTS Inteligencia Artificial Conversacional
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

## 9. PERSONAL DATABASES

### 9.1. Data Processing Officer

The following table lists the categories of databases along with the officer responsible, the medium in which the database is stored, and its location:


Database Name	Data Processing Officer	Database Medium	Database Location
Employees	Servicebots S.A.S. (HR Department)	Physical database, internal archive	Not applicable
Suppliers	Servicebots S.A.S. (Administration Department)	Physical database, internal archive	Not applicable
PQRS	Atlassian	Automated Database, external server managed by a third party	United States
call-api-database	Servicebots S.A.S. (AI Department)	Automated Database, external server in public cloud provider	United States
Operations	Servicebots S.A.S. (Digital Contact Center Department)	Archive database, external server in public cloud provider, used for managing calls in the digital contact center	United States
NLP	Servicebots S.A.S. (AI Department)	Automated Database, external server in public cloud provider	United States
Reports	Servicebots S.A.S. (Speech Department)	Automated Database, external server in public cloud provider, used for presenting management reports	United States
VB [ClientName]	Servicebots S.A.S. (Product Department)	Automated Database, external server in public cloud provider	Not applicable
VX Calls	Servicebots S.A.S. (Digital Contact Center Department)	Automated Database, external server in public cloud provider	Not applicable

### 9.2. Database Inventory

The following table lists the categories of databases along with their data collection methods and the purpose of personal data processing:

Database Name	Data Processing Officer	Data Collection Methods	Processing Purpose
Employees	Servicebots S.A.S. (HR Department)	Information collected via: CVs, hiring forms,	To comply with labor law, payroll, social security




Information Security Management System (ISMS)	
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

Database Name	Data Processing Officer	Data Collection Methods	Processing Purpose
		affiliation forms, bank certificates	affiliations, and safeguard information in accordance with this policy
Suppliers	Servicebots S.A.S. (Administration Department)	Information collected via: Supplier forms, supplier documentation	Administrative management of contracted services
PQRS	Atlassian	Information collected via: Web form in help desk system	Client or internal request management related to Servicebots S.A.S. products/services
call-api-database	Servicebots S.A.S. (AI Department)	Information collected via: Serverless Lambdas and API Gateway	Client service for speech analytics execution
Operations	Servicebots S.A.S. (Digital Contact Center Department)	Information collected via: Serverless Lambdas and API Gateway	Client service for managing digital contact center calls
NLP	Servicebots S.A.S. (AI Department)	Information collected via: Serverless Lambdas and API Gateway	Neural Language Processing system training
Reports	Servicebots S.A.S. (Speech Department)	Information collected via: Serverless Lambdas and API Gateway	Client service for generating and presenting speech system reports
VB [ClientName]	Servicebots S.A.S. (Product Department)	Information collected via: Serverless Lambdas and API Gateway	Client service for executing customer interaction transcriptions
VX Calls	Servicebots S.A.S. (Digital Contact Center Department)	Information collected via: Serverless Lambdas and API Gateway	Client service for managing digital contact center calls

### 9.3. Guidelines for Database Creation




Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

The databases listed above are considered primary databases for **Servicebots S.A.S.**, stored in digital archives or information systems. Controls for their identification, storage, protection, retrieval, retention period, and disposal are defined in the **ISMS - Asset Inventory document**, which includes the responsible individuals for their control.

When creating new databases, the following must be considered:

- Data collected must be related to personal data of data subjects (natural persons).
- There must be a defined purpose, aligned with the project for which it was assigned.
- A responsible party must be assigned to ensure its consultation, use, and access.
- A data processor must be assigned or it could be the same person responsible for the database.
- The database must have the necessary security technology resources for access, storage, protection, and recovery.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03
	Date: 18/06/2024

## 10. PROCESSING OF DATABASES

### 10.1. Collection

The methods used by the organization to collect personal data from data subjects are:

- **Physical forms:** When accessing services such as job applications, resumes, or other technical services.
- **Digital forms or applications:** When accessing services supported by information systems or institutional applications.
- **Chat or WhatsApp:** When requesting support or information through established channels on the website or mobile contact groups.
- **Voice recording:** When communication is conducted by phone.
- **Transcription:** When the transcription process is executed.

In the above-mentioned methods, **Servicebots S.A.S.** ensures that personal data collection is done with the voluntary, explicit, informed, and unequivocal authorization of the data subject. In cases where authorization is not required, these exceptions will comply with the provisions of **Law 1581 of 2012, Article 10.**

### 10.2. Storage

**Servicebots S.A.S.** uses the following methods for storing personal data:

- **Amazon Web Services Public Cloud Servers.**
- **Microsoft Azure Public Cloud Servers.**
- **Google Cloud Platform Public Cloud Servers.**


The protection and recovery of personal data is managed by **Servicebots S.A.S.**, specifically the **Product Department**. The management of these services is determined by the **Access Control Methodology** and **Information Asset Management Procedure** documents.

### 10.3. Usage

Personal data is used according to the purpose established for the project or the purpose detailed in the **Database Inventory** section.

### 10.4. Circulation

The circulation of personal data is restricted based on the need for access or consultation by employees through information systems. Access is exclusively provided to the information required for fulfilling their role in the relevant department. This access control

Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


is established in the **Access Control Methodology** and **Information Asset Management Procedures**.

Information shared across company departments via shared folders on **OneDrive** or **Sharepoint** is restricted to view-only access, and it is the responsibility of the information owner to ensure that access is granted only to individuals who need it for the development of their project or area.

### 10.5. Deletion

**Servicebots S.A.S.** deletes personal data when the purpose for which it was collected has been fulfilled or upon request by the data subject, following the procedures outlined in the **Procedures** section of this document.

The retention period of personal data is determined by the scope of the project or while a contractual agreement between the company and its suppliers is in place.

Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

## 11. PROCEDURES

### 11.1. Data Subject Rights

The data subjects whose personal data is registered in **ServiceBots** databases are granted the following rights, as stipulated by law and its decrees:

- To know, update, and correct their personal data with **ServiceBots** or the data processors.
- To request proof of authorization granted to **ServiceBots**, unless the law specifies that such authorization is not necessary.
- To submit requests regarding the use of their personal data and to receive information in response.
- To file complaints with the **Superintendence of Industry and Commerce** for legal violations.
- To revoke their authorization or request the deletion of their personal data from **ServiceBots'** databases, unless there is a legal or contractual obligation to retain the data.
- To access their personal data free of charge as outlined in **Decree 1377 of 2013, Article 21.**
- To be informed of any changes to the terms of this policy.
- To have easy access to this policy and any modifications.
- To easily access their personal data controlled by **ServiceBots** to exercise their rights effectively.
- To know the person or department responsible for handling requests, complaints, claims, or any other inquiries regarding their personal data.

### 11.2. Right to Access and Consultation


According to **Article 21 of Decree 1377 of 2013**, the data subject may consult their personal data for free at least once a month. **ServiceBots S.A.S.** can charge the data subject for delivery, reproduction, or certification costs for more frequent consultations. The costs must not exceed the material recovery expenses.

The data subject can exercise their right of access by submitting a written request to **ServiceBots S.A.S.** via email at [info@servicebots.ai](mailto:info@servicebots.ai), with the subject line "Exercise of Right to Access or Consultation."

### 11.3. Right to Complaints and Claims

**ServiceBots S.A.S.** guarantees the right of data subjects to consult and receive information about their individual record. The **Administrative and Human Resources Department** will handle these requests and forward them to the appropriate area for processing. Complaints will be addressed within 15 business days.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

#### 11.4. Data Transfer to Third Countries

In accordance with **Title VIII of Law 1581 of 2012**, the transfer of personal data to countries that do not provide adequate data protection is prohibited, unless specific exceptions apply, such as express authorization by the data subject, public health reasons, or international treaty requirements.

#### 11.5. Data Transfer to Third Parties

**ServiceBots S.A.S.** will not sell or transfer personal data to third parties, except to:


- Contractors, subcontractors, clients, or potential clients.
- Authorities or legal advisors if criminal conduct is suspected.

#### 11.6. Data Subject Rights

Data subjects have the following rights:

- **Access:** Request access to their personal data.
- **Rectification:** Request corrections to inaccurate or incomplete data.
- **Deletion:** Request the deletion of their personal data when no longer necessary.
- **Processing Limitation:** Request the restriction of data processing.
- **Data Portability:** Receive their data in a structured format and transmit it to another controller.
- **Opposition:** Object to the processing of their personal data.
- **Withdrawal of Consent:** Withdraw consent for data processing at any time.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


## 12. DATA PROCESSING AUDIT POLICY

The objective of the data protection audit policy of **ServiceBots** is to establish a framework and a series of procedures and guidelines to ensure compliance with the obligations and requirements set forth in **Law 1581 of 2012** regarding the processing and use of personal data. The policy aims to ensure the protection of personal data belonging to employees, customers, suppliers, and any other interested parties whose data may be processed by the company, while minimizing the risks of legal non-compliance, complaints, claims, and fines. The policy also seeks to establish a system for regular evaluation of the effectiveness of the technical and organizational security measures adopted by the company and a process for reviewing and updating these measures as necessary, in line with the obligations established by law.

### 12.1. Definitions

- **Personal Data:** Any information that refers to an identified or identifiable natural person, i.e., any information that allows direct or indirect identification of a person. This includes, for example, name, email address, postal address, date of birth, tax identification number, contact information, financial information, medical information, among others.
- **Processing of Personal Data:** Any operation or set of operations performed on personal data, such as collection, registration, organization, storage, use, disclosure, deletion, etc.
- **Technical and Organizational Security Measures:** Measures adopted to protect personal data from unauthorized access, disclosure, destruction, alteration, or loss, and to ensure their integrity, confidentiality, and availability. These may include physical, technical, organizational, and legal measures.
- **Data Processor:** A natural or legal person that processes personal data on behalf of the data controller.
- **Purpose of Processing:** The purpose or reason for which personal data is collected and processed.
- **Record of Processing Activities:** A document that records all personal data processing activities conducted by the company or organization.
- **International Transfers and Transfers:** The transfer or communication of personal data to third countries outside the European Union.
- **Data Access Contracts:** Written agreements between the data controller and the individuals or entities that have access to personal data, which establish conditions and obligations regarding the protection of personal data.
- **Data Protection Officer (DPO):** A person responsible for ensuring compliance with **Law 1581 of 2012** in a company or organization, and for acting as a point of contact between the company and the Data Protection Authority.



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

## 12.2. Responsibilities

### Responsibilities of the Audit Team

The audit team must perform the following activities:

- **Define the objectives and scope of the audit:** Establish the purpose and objectives of the personal data protection audit, including the areas and processes to be evaluated.
- **Identify personal data:** Identify the personal data managed by the company, its origin, the processes conducted with it, and the individuals who access it.
- **Evaluate risks:** Identify potential risks and threats that may affect the privacy of personal data by analyzing existing controls and their effectiveness.
- **Review documentation:** Review all documents related to personal data protection, such as policies and procedures, records of data processing, access authorizations, and security-related documentation.
- **Conduct compliance tests:** Perform tests to verify compliance with regulations regarding personal data protection and the effectiveness of implemented controls.
- **Document findings:** Document the findings and results of the audit, including recommendations to improve personal data protection.
- **Implement corrective actions:** Implement necessary corrective actions to address deficiencies identified during the audit and improve personal data protection.
- **Monitor and maintain:** Personal data protection auditing is a continuous process that must be monitored and maintained to ensure ongoing compliance with data protection regulations. Regular audits should be conducted to ensure the effectiveness of implemented controls and to update policies and procedures as necessary.

- 

### Responsibilities of Data Subjects


Data subjects must cooperate with the audit team during the personal information security audit, which includes providing access to personal information and responding to the audit team's questions.

## 12.3. Personal Information Security Audit Process

The personal information security audit process must follow these steps:

- **Identification and collection of personal data managed by the company:** Identify personal data to be processed, stored, and treated by Servicebots, as defined in the "Information Asset Management Procedure, section ASSET CLASSIFICATION"; verify that all data protection contracts are signed, that express consent from the data subjects is obtained for data processing, that the purposes for which the data was collected are fulfilled, and that necessary confidentiality agreements and contracts for data sharing with third parties are signed.
- **Audit planning:** Schedule interviews with personnel and gather all necessary documentation, including personal data, to clarify any questions regarding that



Information Security Management System (ISMS)	 <b>SERVICEBOTS</b> <small>Inteligencia Artificial Conversacional</small>
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024


documentation. Analyze the technical and organizational security measures implemented by the company and the processing systems used.

- **Analysis and documentation of the company's compliance level:** Analyze and verify the company's compliance with **Law 1581 of 2012**, using information and data collected in previous phases. Identify errors and vulnerabilities that need to be addressed.
- **Creation and delivery of the audit report with the obtained results:** Prepare a final report with the audit results, detailing aspects to be improved, possible deficiencies, and auditor proposals to enhance and resolve these issues to comply with regulatory requirements. This report should be presented to the company's management as well as to the security officer and the DPO for appropriate corrective measures. It is advisable to have an audit template to facilitate report preparation.

#### 12.4. Reviews and Updates

This policy must be reviewed and updated regularly to ensure it remains effective and complies with legal requirements at all times. To carry out this review and update, the following steps can be followed:

- **Establish a review schedule:** It is important to establish a frequency for reviewing the data protection audit policy. This frequency may vary depending on the company's size, the number of employees, and the type of data handled. It is specified that the review should take place at least once a year during the third quarter of Servicebots' fiscal year.
- **Review policies and procedures:** During the review, the audit policy and the procedures followed to ensure personal data protection should be examined. All aspects of the policy should be analyzed, including access controls, password management, data retention policies, among others.
- **Identify new regulations and legal changes:** During the review, new regulations and legal changes affecting the data protection audit policy must be identified. This may include reviewing new data protection laws, new EU guidelines, or local authority regulations, as well as other changes in the industry.
- **Evaluate compliance:** Assess compliance with the data protection audit policy and identify areas needing improvement. This evaluation should be thorough and consider all areas of the company that handle personal data.
- **Update the policy:** Once areas for improvement are identified, the data protection audit policy must be updated. This may include updating policies and procedures, implementing new security controls, and training staff.
- **Communication and training:** Once the data protection audit policy is updated, it is important to communicate these changes to all staff and ensure they are aware of the new policies and procedures. Awareness regarding information security is outlined in the "Information Security and Cybersecurity Training and Awareness

Information Security Management System (ISMS)	
Comprehensive Personal Data Management Program	Version: 03 Date: 18/06/2024

Plan" document. Additional training on data protection can also be offered to ensure all employees are updated and knowledgeable about compliance with regulations.

•

### 12.5. Audit Planning

Process	Responsible	Date
Review	ISMS	Q3 of the Current Fiscal Year
Deletion of Personal Data	of Data Controller	Executed at the request of the client following the Procedure to Exercise the Rights of the Data Subject in this document.

## 13. CHANGES

**Servicebots** will regularly review and update this plan to ensure it aligns with best practices and changes in data protection laws and regulations. The latest version of the Privacy Policy will always be available through the work portal or upon request. A new version is considered communicated to employees when the employee has received an email informing them of the new version or when the employee is informed in another manner about the new Privacy Policy.

## 14. VALIDITY

The databases under the responsibility of **SERVICEBOTS S.A.S.** will be processed for as long as is reasonable and necessary for the purposes for which the data was collected. Once the purpose or purposes of the processing have been fulfilled, and without prejudice to any legal provisions that require otherwise, **SERVICEBOTS S.A.S.** will proceed to delete the personal data in its possession unless there is a legal or contractual obligation that requires its retention. Therefore, this database has been created without a defined validity period. "This processing policy is effective from March 22, 2023."

