PERSONAL DATA PROCESSING POLICY

Date: 2024-02-07

TABLE OF CONTENTS

1. LEGAL BASIS AND SCOPE OF APPLICATION

- The information processing policy is developed in compliance with articles 15 and 20 of the Political Constitution, as well as based on articles 17 literal k) and 18 literal f) of Statutory Law 1581 of 2012, which establishes general provisions for the Protection of

Personal Data (LEPD). Additionally, in compliance with article 2.2.2.25.1.1 section 1 chapter 25 of Decree 1074 of 2015, which partially regulates Law 1581 of 2012.

- This policy will be applicable to all personal data registered in databases that are subject to processing by the Data Controller.

- **Scope**

- This document will apply to all personal data or any other type of information that is used or stored in the databases and files of AH MEDTECH SAS, respecting the criteria for obtaining, collecting, using, processing, processing, exchanging, transferring and transmitting personal data, and establishing the obligations and guidelines of AH MEDTECH SAS for the administration and treatment of personal data stored in its databases and files. This Manual is applicable to the processes of AH MEDTECH SAS that must process data (public data, semi-private data, private data, sensitive data, data of children and adolescents), as Controller and Manager.

1.2 Applicable Regulations

- Political Constitution of Colombia

- Law 1581 of 2012

- Decree 1074 of 2015 Chapter 25 and Chapter 26 compilation of the decrees:
  -Decree 1377 of 2013
  -Decree 886 of 2014

- Law 1266 of 2008 “By which the general provisions of Habeas Data are dictated”.

- Administrative acts issued by the Superintendence of Industry and Commerce.

2. DEFINITIONS

The following definitions are established in article 3 of the LEPD and article 2.2.2.25.1.3 section 1 Chapter 25 of decree 1074 of 2015 (Article 3 of decree 1377 of 2013).

2.1 Authorization:
Prior, express and informed consent of the Holder to carry out the processing of personal data.

2.2 Database:
Organized set of personal data that is subject to processing, belonging to the same context and systematically stored for later use.

2..3 Personal data:
Any information linked to or that can be associated with one or more specific or identifiable natural persons. These data are classified as public, semi-private, private and sensitive:

2.3.1 Public data:
This is data that is not semi-private, private or sensitive. Public data includes, among others, data relating to the marital status of individuals, their profession or occupation, and their status as a merchant or public servant.
Due to its nature, public data may be contained, among others, in public records, public documents, official gazettes and bulletins, duly executed court rulings that are not subject to confidentiality.

2.3.2 Semi-private data:
This is data that is not of an intimate, reserved, or public nature and whose knowledge or disclosure may be of interest not only to its owner but also to a certain sector or group of people or to society in general, such as: Databases containing financial, credit, commercial, service information, and information from third countries.

2.3.3 Private data:
This is personal data that, due to its intimate or reserved nature, is of interest only to its owner and requires prior, informed, and express authorization for its processing. Databases containing data such as personal telephone numbers and email addresses; employment data, administrative or criminal offences, managed by tax authorities, financial institutions and management entities and common services of Social Security, databases on financial or credit solvency, databases with sufficient information to assess the personality of the holder, databases of the persons responsible for operators that provide electronic communication services.

2.3.4 Sensitive data:
Sensitive data is understood to be data that affects the privacy of the Holder or whose improper use may lead to discrimination, such as data that reveal racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in unions, social organisations, human rights organisations or that promote the interests of any political party or that guarantee the

rights and guarantees of opposition political parties, as well as data relating to health, sexual life, and biometric data.

2.4 Data processor:
Natural or legal person, public or private, who by itself or in association with others, processes personal data on behalf of the Data Controller.

2.5 Data controller:
Natural or legal person, public or private, who by itself or in association with others, decides on the database and/or the processing of data.

2.6 Database administrator:
Collaborator in charge of controlling and coordinating the proper application of data processing policies once stored in a specific database; as well as putting into practice the guidelines issued by the Data Controller and the Data Protection Officer.

2.7 Data Protection Officer:
Natural person who assumes the function of coordinating the implementation of the legal framework for the protection of personal data, which will process the requests of the Holders, for the exercise of the rights referred to in Law 1581 of 2012.

2.8 Holder:
Natural person whose personal data is subject to processing.

2.9 Treatment:
Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion.

2.10 Privacy notice:
Verbal or written communication generated by the Controller, addressed to the Owner for the processing of his/her personal data, through which he/she is informed about the existence of the information processing policies that will be applicable to him/her, the way to access them and the purposes of the processing that is intended to be given to the personal data.ç

2.11-Transfer:
Data transfer takes place when the Controller and/or Processor of personal data, located in Colombia, sends the information or personal data to a recipient, who is also the Controller and is located within or outside the country.

2.12 -Transmission:
Processing of personal data that involves the communication of the same within or outside the territory of the Republic of Colombia when its purpose is to carry out a treatment determined by the processor on behalf of the controller.

3. PRINCIPLES OF DATA PROTECTION

- Article 4 of the LEPD establishes principles for the processing of personal data that must be applied, in a harmonious and comprehensive manner, in the development, interpretation and application of the Law. The legal principles of data protection are the following:

3.1 Principle of Legality:
- The processing of data is a regulated activity that must be subject to the provisions of the LEPD, Decree 1377 of 2013 Compiled in Chapter 25 of Decree 1074 of 2015 and in the other provisions that develop it.

3.2 Principle of Purpose:
- The processing must obey a legitimate purpose in accordance with the Constitution and the Law, which must be informed to the Owner.

3.3 Principle of Freedom:
- The processing can only be carried out with the prior, express and informed consent of the Owner. Personal data may not be obtained or disclosed without prior authorization, or in the absence of a legal or judicial mandate that reveals consent. The processing of data requires the prior and informed authorization of the Owner by any means that allows it to be consulted later.

3.4 Principle of Truthfulness or Quality:
- The information subject to processing must be truthful, complete, accurate, updated, verifiable and understandable. The processing of partial, incomplete, fractioned or misleading data is prohibited.

3.5 Principle of Transparency:
- In the processing, the right of the Owner to obtain from the Data Controller or the Data Processor, at any time and without restrictions, information about the existence of data

that concerns him/her must be guaranteed. At the time of requesting authorization from the owner, the data controller must inform him/her clearly and expressly of the following, keeping proof of compliance with this duty:

- The processing to which his/her data will be subjected and the purpose thereof.
- The optional nature of the Owner's response to questions asked when these concern sensitive data or data of children or adolescents.
- The rights that assist you as Owner.
- The identification, physical address, email and telephone number of the person responsible for the treatment.

3.6 Principle of Restricted Access and Circulation:

The processing is subject to the limits arising from the nature of the personal data, the provisions of the LEPD and the Constitution. In this regard, the processing may only be carried out by persons authorized by the Holder and/or by the persons provided for in the Law. Personal data, except for public information, may not be available on the Internet and other means of dissemination or mass communication, unless access is technically controllable to provide restricted knowledge only to the Holders or authorized third parties in accordance with the Law.

3.7 Security Principle:

The information subject to processing by the Data Controller or Data Processor must be handled with the technical, human and administrative measures necessary to ensure the security of the records, avoiding their adulteration, loss, consultation, unauthorized or fraudulent use or access. The Data Controller is responsible for implementing the corresponding security measures and for making them known to all personnel who have direct or indirect access to the data. Users who access the Data Controller's information systems must be aware of and comply with the security rules and measures that correspond to their functions. These security rules and measures are included in PL-02 Internal Security Policies, which are mandatory for all users and company personnel. Any modification of the rules and measures regarding the security of personal data by the Data Controller must be made known to users.

3.8 Confidentiality Principle:

All persons involved in the processing of personal data that are not public in nature are obliged to guarantee the confidentiality of the information, even after their relationship with any of the tasks that comprise the processing has ended, and may only provide or communicate personal data when this corresponds to the development of the activities authorized in the LEPD and in the terms thereof.

4. AUTHORIZATION FOR THE USE OF PERSONAL DATA

In accordance with article 9 of the LEPD, the processing of personal data requires the authorization of the Owner, except in cases expressly indicated in the regulations governing the protection of personal data. Prior to and/or at the time of collecting personal data, AH MEDTECH SAS will request the Owner's authorization to collect and process it, indicating the purpose for which the data is requested, using automated technical means, written or oral, to preserve proof of the authorization and/or the unequivocal conduct described in article 2.2.2.25.2.2. section 2 of chapter 25 of Decree 1074 of 2015.

The Owner's authorization will not be necessary when it concerns:

Information required by a public or administrative entity in the exercise of its legal functions or by court order. Data of a public nature.

Cases of medical or health emergencies.

Processing of information authorized by law for historical, statistical or scientific purposes. - Data related to the Civil Registry of persons.

5. REQUEST FOR AUTHORIZATION FROM THE OWNER OF PERSONAL DATA

Authorization for the use and/or processing of data will be managed by AH MEDTECH SAS, through mechanisms that guarantee its subsequent consultation and the manifestation of the will of the Owner through the following means:

-In writing.
-Orally.
-Through automated channels.
-Through unequivocal conduct of the owner that allows to reasonably conclude that he/she granted the authorization.

AH MEDTECH SAS, in advance and/or at the time of collecting personal data, will clearly and expressly inform the Owner of the following:

a) The Processing to which his/her personal data will be subjected and the purpose thereof;

b) The optional nature of the response to the questions asked, when these are about sensitive data or about the data of girls, boys and adolescents;
c) The rights that assist him/her as Owner;
d) The identification, physical or electronic address and telephone number of AH MEDTECH SAS.

6. DATA CONTROLLER

The data controller of the databases covered by this policy is AH MEDTECH SAS, whose contact details are as follows:

- Address: CR 15 83 33 OFFICE 203, BOGOTÁ D.C - BOGOTÁ D.C
- Email: gerenciadminmedtech@alfredohoyos.com
- Phone: 0 - 3185310789

7. DATABASE PROCESSING AND PURPOSES

In the course of its business activity, AH MEDTECH SAS processes personal data relating to natural persons that are contained and processed in databases intended for legitimate purposes, in compliance with the Constitution and the Law. The processing to which personal data will be subjected includes collection, storage, use, circulation or deletion. The processing of data will be subject to the purposes authorized by the Owner, to the contractual obligations between the parties, as well as to cases in which there are legal obligations that must be fulfilled.

Annex 2 PL-01 Purposes of Databases contains information relating to the different databases under the responsibility of the company and the purposes assigned to each of them for processing.

8. VALIDITY OF THE DATABASE

The personal data incorporated in the databases will be valid for the period necessary to fulfill the purposes for which their processing was authorized and the special regulations that govern the matter, the current regulations related to the conservation period will also be taken into account.

9. RIGHTS OF DATA SUBJECTS

In accordance with Article 8 of the LEPD, Article 2.2.2.25.4.1 Section 4 Chapter 25 of Decree 1074 of 2015 (Articles 21 and 22 of Decree 1377 of 2013), Data Subjects may exercise a number of rights in relation to the processing of their personal data. The Data Subject shall have the following rights:

a) To know, update and rectify your personal data with regard to the Data Controllers or Data Processors. This right may be exercised, among others, in relation to partial, inaccurate, incomplete, fragmented data, which may lead to error, or data whose processing is expressly prohibited or has not been authorized;
b) To request proof of the authorization granted to the Data Controller, except when it is expressly excepted as a requirement for processing, in accordance with the provisions of article 10 of this law;
c) To be informed by the Data Controller or Data Processor, upon request, regarding the use that has been given to your personal data;

d) Submit complaints to the Superintendency of Industry and Commerce for violations of the provisions of this law and other regulations that modify, add to or complement it;

e) Revoke the authorization and/or request the deletion of the data when the Processing does not respect the constitutional and legal principles, rights and guarantees. The revocation and/or deletion will proceed when the Superintendency of Industry and Commerce has determined that in the Processing the Controller or the Processor has engaged in conduct contrary to the law and the Constitution;

f) Access free of charge to their personal data that have been subject to Processing.

These rights may be exercised by the following persons.

1. By the Holder, who must prove his identity sufficiently by the different means made available to him by the Controller.
2. By his successors in title, who must prove such status.
3. By the representative and/or attorney of the Holder, after proving the representation or power of attorney.
4. By stipulation in favor of another and for another.

The rights of children or adolescents will be exercised by the persons who are authorized to represent them.

9.1 Right of access or consultation

- This is the right of the Data Subject to be informed by the data controller, upon request, regarding the origin, use and purpose for which their personal data have been processed.

9.2 Right to complaints and claims

- The Law distinguishes four types of claims:

- Claim for correction: the right of the Data Subject to have partial, inaccurate, incomplete, fragmented data, which are misleading, or data whose processing is expressly prohibited or has not been authorized, updated, rectified or modified.
- Claim for deletion: the right of the Data Subject to have data that is inadequate, excessive or does not respect the constitutional and legal principles, rights and guarantees deleted.

- Revocation request: the right of the Data Subject to revoke the authorization previously granted for the processing of his/her personal data.
- Infringement request: the right of the Data Subject to request that the breach of the Data Protection regulations be remedied.

9.3 Right to request proof of the authorization granted to the Data Controller

Except when it is expressly excepted as a requirement for processing in accordance with the provisions of article 10 of the LEPD.

9.4 Right to submit complaints to the Superintendence of Industry and Commerce for violations

The Holder or successor in title may only submit the request (complaint) to the SIC – Superintendence of Industry and Commerce, once he or she has exhausted the consultation or claim process before the Data Controller or Data Processor.

10. PROCESSING OF DATA OF MINORS

AH MEDTECH SAS in accordance with article 7 of Law 1581 of 2012, carries out processing of personal data of children and adolescents within the framework of the criteria indicated in article 2.2.2.25.2.9 section 2 of chapter 25 of the Decree 1074 of 2015 (Article 12 of Decree 1377 of 2013), with observance of the following parameters and requirements:

1. That the use of data responds to and respects the best interests of children and adolescents.
2. That in the use of data, respect for the minor's fundamental rights is ensured.

Once the above requirements have been met, AH MEDTECH SAS will request the legal representative of the child or adolescent for authorization prior to the minor's exercise of his or her right to be heard, an opinion that will be valued taking into account maturity, autonomy and ability to understand the matter. As Responsible and/or Manager, you will ensure the appropriate use of the data of children and adolescents, applying the principles and obligations established

in Law 1581 of 2012 and regulatory standards. Likewise, it will identify the sensitive data collected or stored in order to increase the security and processing of the information.

11. DUTIES AS DATA CONTROLLER

AH MEDTECH SAS, as Data Controller, will comply with the following duties, without prejudice to the other provisions set forth in this law and in other laws that govern its activity:

11.1. In front of the Holder:

a) To guarantee the Holder, at all times, the full and effective exercise of the right of habeas data;

b) To request and retain, under the conditions provided for in this law, a copy of the respective authorization granted by the Holder;

c) To duly inform the Holder about the purpose of the collection and the rights that assist him by virtue of the authorization granted;

d) To process the queries and claims formulated in the terms indicated in this law;

e) To inform the Holder at his request about the use given to his data;

11.2. In front of the Manager:

a) Ensure that the information provided to the Data Processor is true, complete, accurate, up-to-date, verifiable and understandable;

b) Update the information, communicating in a timely manner to the Data Processor all the new developments regarding the data previously provided and adopt the other measures necessary so that the information provided to the Data Processor remains up-to-date;

c) Rectify the information when it is incorrect and communicate the relevant information to the Data Processor;

d) Inform the Data Processor when certain information is being discussed by the Owner, once the claim has been submitted and the respective process has not been completed;

e) Provide the Data Processor, as the case may be, only with data whose processing is previously authorized in accordance with the provisions of this law;

f) Demand from the Data Processor at all times, respect for the security and privacy conditions of the Owner's information;

11.3. Regarding the principles and other obligations:

a) Observe the principles of Legality, purpose, freedom, quality, truthfulness, transparency, restricted access and circulation, security and confidentiality
b) Adopt an internal manual of policies and procedures to ensure proper compliance with this law and especially for the handling of queries and complaints;
c) Inform the data protection authority when violations of security codes occur and there are risks in the management of the information of the Holders.
d) Comply with the instructions and requirements issued by the Superintendence of Industry and Commerce.
e) Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, unauthorized or fraudulent use or access;

12. DUTIES AS DATA PROCESSOR:

AH MEDTECH SAS, as Data Processor, will comply with the following duties, without prejudice to the other provisions set forth in this law and in others that govern its activity:

a) Guarantee the Holder, at all times, the full and effective exercise of the right of habeas data;

b) Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, unauthorized or fraudulent use or access;

c) Perform timely updating, rectification or deletion of the data in accordance with the terms of this law;

d) Update the information reported by the Data Controllers within five (5) business days from its receipt;

e) Process the queries and complaints made by the Holders in the terms indicated in this law;

f) Adopt an internal manual of policies and procedures to guarantee the proper compliance with this law and, in particular, for the attention of queries and complaints by the Holders;

g) Register in the database the legend “complaint in process” in the manner regulated in this law;

h) Insert the legend “information under judicial discussion” into the database once notified by the competent authority about judicial processes related to the quality of personal data;

i) Refrain from circulating information that is being disputed by the Holder and whose blocking has been ordered by the Superintendency of Industry and Commerce;

j) Allow access to information only to persons who may have access to it;

k) Inform the Superintendency of Industry and Commerce when violations of security codes occur and there are risks in the management of the Holders' information;

l) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce.

13. ATTENTION TO DATA OWNERS

To handle requests, queries and complaints regarding personal data protection, AH MEDTECH SAS has appointed a Data Protection Officer. Data Owners may submit their requests or queries through the following channels:

Email: gerenciaradminmedtech@alfredohoyos.com

Address: CR 15 83 33 OFFICE 203, BOGOTÁ D.C - BOGOTÁ D.C. Phones: 0 - 3185310789

14. PROCEDURES FOR EXERCISING THE RIGHTS OF THE OWNER

14.1 Right of access or consultation

AH MEDTECH SAS will guarantee the Owner free consultation of his/her personal data in the following cases (Article 2.2.2.25.4.2. Section 4 Chapter 25 of Decree 1074 of 2015):

1. At least once every calendar month.
2. Every time there are substantial modifications to the information processing policies that motivate new consultations.

For consultations whose frequency is greater than one per calendar month, AH MEDTECH SAS may charge the Owner shipping, reproduction and, where applicable, certification of documents. Reproduction costs may not be greater than the costs of recovery of the corresponding material. For this purpose, AH MEDTECH SAS will demonstrate to the Superintendence of Industry and Commerce, when required, the support for said expenses.

The Data Owner may exercise the right to access or consult his/her data by writing to AH MEDTECH SAS, sent by email to: gerenciadminmedtech@alfredohoyos.com, indicating in the Subject “Exercise of the right of access or consultation”, or by post sent to CR 15 83 33 OFFICE 203, BOGOTÁ D.C - BOGOTÁ D.C. The request must contain the following information:

- Name and surname of the Owner.
- Photocopy of the Citizenship Card of the Owner and, where applicable, of the person representing him/her, as well as the document accrediting such representation.
- Petition specifying the request for access or consultation. - Address for notifications, date and signature of the applicant.
- Documents accrediting the request made, where applicable.

The Owner may choose one of the following ways to consult the database to receive the requested information:

- On-screen display.
- In writing, with a copy or photocopy sent by certified mail or not.
- Email or other electronic means.

- Another system appropriate to the configuration of the database or the nature of the treatment, offered by

AH MEDTECH SAS.

Once the request has been received, AH MEDTECH SAS will resolve the request for consultation within a maximum period of ten (10) business days counted from the date of receipt of the same. When it is not possible to attend to the query within said term, the interested party will be informed, stating the reasons for the delay and indicating the date on which his query will be attended to, which in no case may exceed five (5) business days following the expiration of the first term. These terms are set out in article 14 of the LEPD.

Once the consultation process has been exhausted, the Owner or successor in title may file a complaint with the Superintendency of Industry and Commerce.

14.2 Complaint and claim rights

The Data Owner may exercise the right to claim his/her data by writing to AH MEDTECH SAS, sent by email to gerenciaradminmedtech@alfredohoyos.com, indicating in the Subject “Exercise of the right of access or consultation”, or by post sent to CR 15 83 33 OFFICE 203, BOGOTÁ D.C - BOGOTÁ D.C. The request must contain the following information:

- Name and surname of the Holder.
- Photocopy of the Holder's Citizenship Card and, where applicable, of the person representing him/her, as well as the document accrediting such representation.
- Description of the facts and petition in which the request for correction, deletion, revocation or infringement is specified.
- Address for notifications, date and signature of the applicant.
- Documents accrediting the request made that you wish to assert, where applicable.

If the claim is incomplete, the interested party will be required within five (5) days following receipt of the claim to correct the deficiencies. After two (2) months from the date of the request, if the applicant does not submit the required information, it will be understood that the claim has been withdrawn.

Once the complete claim has been received, a legend stating “claim in process” and the reason for it will be included in the database, within a period of no more than two (2) business days. This legend must be maintained until the claim is decided.

AH MEDTECH SAS will resolve the claim request within a maximum period of fifteen (15) business days from the date of receipt of the same. When it is not possible to address the claim within said period, the interested party will be informed of the reasons for the delay and the date on which his claim will be addressed, which in no case may exceed eight (8) business days following the expiration of the first term.
Once the claim process has been exhausted, the Owner or successor in title may file a complaint with the Superintendency of Industry and Commerce.

14.3 Facultados para recibir información

AH MEDTECH SAS will provide the information of the Owners of its databases to the following persons authorized or empowered to receive it, in accordance with article 13 of Law 1581 of 2012:

- To the Owners, their successors in title or their legal representatives;
- To public or administrative entities in the exercise of their legal functions or by court order;
- To third parties authorized by the Owner or by law.

14.3.1 Verification of the authority to request or receive information

In order to process the request for consultation or claim, the applicant must provide the following documents to prove his/her ownership or the authority to receive the required information, in accordance with the following cases:

- Owner: Copy of the identity document.
- Successor in title: Identity document, civil registry of death of the Owner, document proving the capacity in which he/she acts and copy of the identity document of the Owner.
- Legal representative and/or attorney: Valid identity document, document proving the capacity in which he/she acts (Power of Attorney) and copy of the identity document of the Owner.

15 DATA PROCESSING IN VIDEO SURVEILLANCE SYSTEMS

AH MEDTECH SAS will inform people about the existence of video surveillance mechanisms, by posting visible notices within reach of all owners and installed in video surveillance areas, mainly in the entrance areas to the places that are being watched and monitored and inside them. In these notices, it will inform who is the Data Controller, the purposes of the processing, the rights of the Owner, the channels enabled to exercise the rights of the Owner, as well as where the Information Processing Policy is published.

On the other hand, it will keep the images only for the time strictly necessary to fulfill the purpose of the and will register the database that stores the images in the National Database Registry, unless the Processing consists only of the reproduction or broadcast of images in real time.

Access to and disclosure of images will be restricted to persons authorized by the Owner and/or by request of an authority in the exercise of its functions. Consequently, the disclosure of the information collected will be controlled and consistent with the purpose established by the Data Controller.

16 SECURITY MEASURES

In order to comply with the security principle enshrined in article 4, letter g) of the LEPD, AH MEDTECH SAS has implemented the necessary technical, human and administrative measures to guarantee the security of the records, avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access.

Furthermore, AH MEDTECH SAS, by signing the corresponding transmission contracts, has required the data processors with whom it works to implement the necessary security measures to guarantee the security and confidentiality of the information in the processing of personal data.

Below are the security measures implemented by AH MEDTECH SAS that are collected and developed in its PL-02 Internal Security Policies (Tables I, II, III and IV).

TABLE I: Common security measures for all types of data (public, private, confidential, reserved) and databases (automated, non-automated)	
Document and media management	1. Measures to prevent improper access or recovery of data that has been discarded, deleted or destroyed. 2. Restricted access to the place where the data is stored. 3. Authorization of the person responsible for managing the databases for the output of documents or media by physical or electronic means. 4. Labeling or identification system for the type of information. 5. Inventory of media.
Access control	1. User access limited to data necessary for the performance of their functions. 2. Updated list of authorized users and accesses. 3. Mechanisms to prevent access to data with rights other than those authorized. 4. Granting, changing or canceling permissions by authorized personnel
Incidents	1. Incident log: type of incident, time of occurrence, notification issuer, notification recipient, effects and corrective measures. 2. Incident notification and management procedure.
Personal	1. Definition of the functions and obligations of users with access to the data. 2. Definition of the control functions and authorizations delegated by the data controller. 3. Dissemination of the rules and the consequences of non-compliance among staff.
Internal Security Manual	1. Preparation and implementation of the mandatory manual for staff. 2. Minimum content: scope of application, security measures and procedures, functions and obligations of staff, description of databases, procedure for incidents, identification of data processors.

TABLE II: Common security measures for all types of data (public, private, confidential, reserved) according to the type of database	
Non-automated databases	
Archive	1. Documentation file following procedures that guarantee correct conservation, location and consultation, which allow the exercise of the rights of the Holders.
Document storage	1. Storage devices with mechanisms that prevent access by unauthorized persons.
Custody of documents	1. Duty of diligence and custody of the person in charge of documents during their review or processing.
Automated databases	

Identification and authentication	1. Personalized user identification to access information systems and verify their authorization. 2. Identification and authentication mechanisms; Passwords: assignment and expiration.
Telecommunications	1. Access to data through secure networks.

TABLE III: Security measures for private data according to the type of database	
Non-automated databases	
Audit	1. Ordinary audit (internal or external) every two months. 2. Extraordinary audit for substantial changes in information systems. 3. Report on detection of deficiencies and proposal for corrections. 4. Analysis and conclusions of the security officer and the data controller.
Security Officer	1. Appointment of one or more Database Administrators. 2. Appointment of one or more persons in charge of controlling and coordinating the measures in the Internal Security Manual. 3. Prohibition of delegation of the responsibility of the Data Controller to Database Administrators.
Internal Security Manual	1. Periodic compliance checks.
Automated databases	
Document and media management	1. Record of entry and exit of documents and media: date, issuer and receiver, number, type of information, method of shipment, person responsible for receipt or delivery.
Access control	1. Access control to the place or places where the information systems are located
Identification and authentication	1. Mechanism to limit the number of repeated unauthorized access attempts. 2. Data encryption mechanisms for transmission.
Incidents	1. Record of data recovery procedures, person performing them, restored data and manually recorded data. 2. Authorization of the data controller to perform recovery procedures.

TABLE IV: Security measures for sensitive data according to the type of database
Non-automated databases

Access control	1. Access only for authorized personnel. 2. Access identification mechanism. 3. Log of access by unauthorized users. 4. Destruction that prevents access or recovery of data.
Document storage	1. File cabinets, cupboards or other items located in access areas protected with keys or other measures. 2. Measures that prevent access to or manipulation of physically stored documents.
Automated databases	
Access control	1. Confidential labeling system.
Identification and authentication	1. Data encryption mechanisms for transmission and storage.
Document storage	1. Access log: user, time, database accessed, type of access, record accessed 2. Access log control by the security officer. Monthly report.
Telecommunications	1. Access and transmission of data through secure electronic networks. 2. Data transmission through encrypted networks (VPN).

17 COOKIES OR WEB BUGS

AH MEDTECH SAS may collect personal information from its Users while they use the Website, the Application or the Linked Pages (Landing Page). Users may choose to store this personal information on the website, the application or the linked portal (Landing Page), in order to facilitate transactions and services to be provided by AH MEDTECH SAS and/or its linked portals (Landing Page). Therefore, AH MEDTECH SAS uses different tracking and data collection technologies such as, its own and third-party Cookies, this is the analysis tool that helps website and application owners understand how visitors interact with their properties. This tool may use a set of cookies to collect information and offer website usage statistics without personally identifying visitors to Google.

This information allows us to know your browsing patterns and offer you personalized services.

MEDTECH SAS may use these technologies to authenticate you, to remember your preferences for the use of the website, the application and the linked pages (Landing Page), to present offers

that may be of interest to you and to facilitate transactions, to analyze the use of the website, the application or the linked pages and their services, to use it in the aggregate or combine it with the personal information we have and share it with authorized entities.

If a user does not want their personal information to be collected through Cookies, they can change the preferences in their own web browser. However, it is important to note that if a web browser does not accept Cookies, some of the functionalities of the website, the application and/or the linked pages (Landing Page) may not be available or may not function correctly. You can allow, block or delete the cookies installed on your device by configuring the options of the browser installed on your device, as follows:

- Chrome: https://support.google.com/accounts/answer/61416?co=GENIE.Platform%3DDesktop&hl=es
- Microsoft Edge: https://support.microsoft.com/es-es/microsoft-edge/permitir-temporalmente-las-cookies-y-losdatos-del-sitio-en-microsoft-edge-597f04f2-c0ce-f08c-7c2b-541086362bd2
- Firefox: https://support.mozilla.org/es/kb/habilitar-y-deshabilitar-cookies-sitios-web-rastrear-preferencias - Safari: https://support.apple.com/es-es/HT201265

18. PROTOCOL FOR NOTIFICATION, MANAGEMENT AND RESPONSE TO SECURITY INCIDENTS

AH MEDTECH SAS has an incident reporting procedure for communication and notification between collaborators, personal data protection officer, data processors, data owners, surveillance and control entity, as well as judicial entities: for the management and response to security incidents from the moment they are detected in order to be evaluated and manage the identified vulnerabilities, ensuring that the systems, networks, and applications are sufficiently secure.

All users and those responsible for managing databases, as well as any person who has a relationship with the collection, storage, use, circulation or any treatment or consultation of the databases, must know the procedure to act in case of security incidents to guarantee the

confidentiality, availability and integrity of the information contained in the databases under their responsibility.

Some examples of security incidents are: failure of security systems that allow access to personal data by unauthorized persons, unauthorized attempt to remove a document or medium, loss of data or total or partial destruction of media, change of physical location of databases, knowledge by third parties of passwords, modification of data by unauthorized personnel, among others.

In the event of a security incident, the response team or committee will take into account the following criteria:

Strategy to identify, contain and mitigate security incidents.

- Apply measures to contain and reverse the impact that the security incident may have.
- Adequately evaluate the security incident and its impact on the Data Subjects.
- Verify the legal or contractual requirements with service providers associated with the security incident.
- Determine the level of risk for the Data Subjects and notify the occurrence.
- Verify the roles and responsibilities of the personnel responsible for the operation of the affected information or data.

Timeline for managing the security incident.

Apply the procedure to address security incidents, according to parameters that allow for adequate management and impact mitigation. Verify, according to the evaluation of the security incident, the need to notify entities such as: the Attorney General's Office, the Attorney General's Office, Gaula, National Police, Financial Superintendence of Colombia, Police Cybernetic Center, colCERT; Police CSIRT, Asobancaria CSIRT, Sectorial CSIRT, among others.

Progress of the security incident report

Monitor management by establishing deadlines, evaluate its progress and identify possible conflict points that may arise in the management of the security incident.

Evaluation of the response to the security incident
Once the security incident has been managed and controlled, the response team must review the actions executed to contain it and make the pertinent adjustments to implement an improvement plan.

Implemented actions and improvement plans
Establish the actions necessary to mitigate the impact of the security incident and prevent it from happening again, through corrective and preventive actions, as well as improvement plans that the response team must adopt.

Documentation and reporting to the monitoring and control entity
Document the information related to the security incident in an internal registry, as well as prepare a report with supporting documents for the actions taken, which must be filed with the Superintendence of Industry and Commerce, through the RNBD within 15 business days after the incident was detected.

Review
Evaluate the causes that led to the security incident and the success of its management to assess the effectiveness of the controls and actions implemented. Document the lessons learned to keep them in mind on future occasions.

19. RISK MANAGEMENT ASSOCIATED WITH DATA PROCESSING

AH MEDTECH SAS has identified risks related to the processing of personal data and established controls in order to mitigate their causes, through the implementation of PL-02 Internal Security Policies. Therefore, it will establish a risk management system together with the tools, indicators and resources necessary for its management, when the organizational structure, internal processes and procedures, the amount of databases and types of personal data processed by the organization are considered to be exposed to frequent or high-impact events or situations that affect the proper provision of the service or threaten the information of the owners.

The risk management system will determine the sources such as: technology, human resources, infrastructure and processes that require protection, their vulnerabilities and threats, in order to assess their level of risk. Therefore, to guarantee the protection of personal data, the type or group of internal and external persons, the different levels of access authorization will be taken

into account. Likewise, the possibility of occurrence of any type of event or action that may cause damage (material or immaterial) will be observed, such as:

- Criminality: Understood as actions caused by human intervention that violate the law and are penalized by it.
- Physical events: Understood as natural and technical events, as well as events indirectly caused by human intervention.
- Negligence and institutional decisions: Understood as actions, decisions or omissions by people who have power and influence over the system. At the same time, they are the least predictable threats because they are directly related to human behavior.

AH MEDTECH SAS in the risk management program will implement protection measures to avoid or minimize damage in the event that a threat materializes.

20. DELIVERY OF PERSONAL DATA TO AUTHORITIES

When a public or administrative entity in the exercise of its legal functions or by court order requests access and/or delivery of personal data contained in any of its databases from AH MEDTECH SAS, the legality of the request will be verified, as well as the relevance of the requested data in relation to the purpose expressed by the authority. For the delivery, a document will be signed indicating the data of the requesting entity and the characteristics of the personal information requested, specifying the obligation to guarantee the rights of the Holder, both to the official who makes the request, to the person who receives it, as well as to the requesting entity.

21. INTERNATIONAL TRANSFER AND TRANSMISSION OF PERSONAL DATA

AH MEDTECH SAS will transfer personal data to countries that provide adequate levels of data protection. A country is deemed to offer an adequate level of data protection when it complies with the standards set by the Superintendency of Industry and Commerce on the subject, which in no case may be lower than those required by Law 1581 of 2012 for its recipients. This prohibition shall not apply when it concerns:

- Information for which the Data Subject has given his/her express and unequivocal authorization for the transfer.

- Exchange of medical data, when required for the treatment of the Data Subject for reasons of public health or hygiene.
- Bank or stock transfers, in accordance with the legislation applicable to them.
- Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.
- Transfers necessary for the execution of a contract between the Data Subject and the data controller, or for the execution of pre-contractual measures, provided that the Data Subject's authorization is obtained.
- Transfers legally required to safeguard the public interest, or for the recognition, exercise or defense of a right in a judicial process.

In cases where the transfer of data is necessary and the destination country is not on the list of countries considered safe ports indicated by the Superintendency of Industry and Commerce, a declaration of conformity regarding approval for the international transfer of personal data must be requested from the same entity.

International transmissions of personal data carried out between AH MEDTECH SAS and a processor to allow the processor to carry out the processing on behalf of the controller, will not require the Holder to be informed or have his consent, provided that there is a personal data transmission contract. This personal data transmission contract must be signed between the Controller and the Processor to define the scope of the processing of personal data under their control and responsibility, as well as the activities that the processor will carry out on behalf of the Controller and the obligations of the Processor towards the holder. Additionally, the Processor must comply with the following obligations and apply the regulations in force in Colombia regarding data protection.

1. To process personal data on behalf of the Controller in accordance with the principles that protect them.
2. To safeguard the security of the databases containing personal data.
3. To maintain confidentiality regarding the processing of personal data.

The above conditions set for international data transmissions will also apply to national data transmissions.

22. BIOMETRIC DATA PROCESSING

The biometric data stored in the databases are collected and processed strictly for security reasons, to verify personal identity and to control access to employees, clients and visitors. Biometric identification mechanisms capture, process and store information related to, among others, the physical features of people (fingerprints, voice recognition and facial features), in order to establish or “authenticate” the identity of each subject.

The administration of the biometric databases is carried out with technical security measures that guarantee due compliance with the principles and obligations derived from the Statutory Law on Data Protection, also ensuring the confidentiality and reserve of the information of the owners.

23. NATIONAL DATABASE REGISTRY – RNBD

The term for registering databases in the RNBD will be the one established by law. Likewise, in accordance with article 12 of Decree 886 of 2014, Data Controllers must register their databases in the National Database Registry on the date that the Superintendency of Industry and Commerce enables said registry, in accordance with the instructions issued for this purpose by said entity. Databases created after that term must be registered within two (2) months from their creation.

24. SECURITY OF INFORMATION AND PERSONAL DATA

Compliance with the regulatory framework for Personal Data Protection, the security, confidentiality and/or privacy of the information stored in the databases is of vital importance to AH MEDTECH SAS. For this reason, we have established policies, guidelines, procedures and information security standards, which may change at any time to adjust to new regulations and needs of AH MEDTECH SAS, whose objective is to protect and preserve the integrity, confidentiality and availability of information and personal data.

We also guarantee that in the collection, storage, use and/or treatment, destruction or elimination of the information provided, we rely on technological security tools and implement security practices that include: transmission and storage of sensitive information through secure mechanisms, use of secure protocols, securing technological components, restricting access to information only to authorized personnel, information backup, secure software development practices, among others.

If it is necessary to provide information to a third party due to the existence of a contractual relationship, we sign a transmission contract to guarantee the confidentiality and reserve of the information, as well as compliance with this Data Processing Policy, the information security policies and manuals and the protocols for attention to the owners established in AH MEDTECH SAS. In any case, we adopt commitments for the protection, care, security and preservation of the confidentiality, integrity and privacy of the stored data.

25. DOCUMENT MANAGEMENT

Documents containing personal data must be easily recoverable, which is why the location of each physical and digital document must be documented. These storage routes must be inspected frequently. Their conservation must be guaranteed by defining the support on which they are stored and under what conditions, taking into account environmental conditions, storage locations, risks to which they are exposed, among others. The retention time of documents is determined based on legal requirements, if applicable. Otherwise, each organization defines it according to its needs. Likewise, the final disposition of the documents must be clear, identifying whether they are recycled, reused, preserved, digitized, among others.

Documents related to the protection of personal data must be prepared by personnel or a competent entity for this purpose. Likewise, the organization must be the one to review and approve all documents and record them in the document approval box.

In order to be easily traceable, documents must be coded, updated and modified by the responsible personnel. This modification will be carried out whenever necessary. For the elimination of a document, there must be a justification for it described in the history which is found at the bottom of all documents.

Both physical and digital documents containing personal data must be protected from external or internal agents that may alter their content, following the guidelines described in PL-02 Internal Security Policies

The distribution of documents containing personal data will be carried out by the person responsible for the treatment, who will leave documented evidence of said distribution, where, among other things, the type of document and the identification of the person to whom the information was delivered are specified

A person responsible for guaranteeing the confidentiality of the personal data of the owners must be designated. This person will be the one who will guard documents, guarantee their protection both physically and digitally, avoid alterations of the information, and will also guarantee that the documents that leave their custody are identified and easily traceable.

26. VALIDITY

This update of the Policy will be valid from 2024-05-21, the databases under the responsibility of AH MEDTECH SAS will be processed for as long as is reasonable and necessary for the purpose for which the data is collected and in accordance with the authorization granted by the Owners of the personal data.

27. APPENDIX

Not applicable

PREPARATION AND APPROVAL OF THE DOCUMENT

REVIEW AND APPROVAL OF THE DOCUMENT			
Prepared by:	PROTECDATA COLOMBIA S.A.S	**Approved by:**	
		Post	
Date:	**2024-05-21**	**Date:**	

HISTORICAL DOCUMENTS

DATE	VERSIÓN	DESCRIPTION OF CHANGE
2024-03-18	01	General legal and technical update of the document.