



PU-Specific Personal Data Protection Policy-v3-30Ago2022(EN)

APPROVAL SHEET

	Prepared by:	Reviewed by:	Approved by:
Position:	Personal Data Protection Officer	Legal adviser	General Manager
Date:	30 Aug 22	30 Aug 22	30 Aug 22

DISTRIBUTION LIST

Version	Date	Role
1.0	04 Mar 20	General Manager Product manager Infrastructure Leader Cari AI Cari AI Technical Architect
2.0	21 Jul 20	General Manager Product manager Infrastructure Leader Cari AI Cari AI Technical Architect
2.1	16Feb21	General Manager Product manager Infrastructure Leader Cari AI Cari AI Technical Architect
2.2	22Jun21	General Manager Product manager Infrastructure Leader Cari AI Cari AI Technical Architect
23	30Sep21	General Manager Legal adviser
2.4	May 20, 2022	All



PU-Specific Personal Data Protection Policy-v3-30Ago2022(EN)

3.0	05 Sept 2022	All
-----	--------------	-----

EXCHANGE CONTROL SHEET

Vers ion	Action	Date	Description of the Action	Numeral	Responsible
1.0	Creation	04 Mar 20	initial creation	All	Security officer
2.0	Update	21 Jul 20	Update according to the revision of the legislation	All	Security officer
2.1	Update	16Feb21	Update reference to current legislation	All	Security officer
2.2.	Update	21Jun 21	Expand to all Cari AI		
23	Update	30 Sep 21	Expand to all Cari AI		
2.4	Update	May 17, 2022	The entire document is modified	All	Personal Data Protection Officer
3.	Update	30 Aug 2022	The entire document is modified	All	Personal Data Protection Officer



PU-Specific Personal Data Protection Policy-v3-30Ago2022(EN)

Contents

1. Introduction	4
two. Principles	7
3. Purpose of data processing	8
3.1 Treatment of sensitive data	11
3.2 Video surveillance	11
3.3 Cases in which authorization is not required	11
4. Legitimation for the exercise of the rights of the owner.	12
5. Persons to whom information may be provided	12
6. Joint duties of Cari AI as RESPONSIBLE and those IN CHARGE of personal data processing	13
6.1 Duties of Cari AI	14
6.2 Duties of those in charge of processing personal data	15
7. Rights as holder of personal data	15
8. Special requirements for the processing of personal data of children and adolescents	16
9. Transfer and international transmission of personal data	17
10. Contact through the web portal	17
11. Attention to requests, request for consultation, updating, rectification and deletion of personal data	18
12. Procedure for exercising the right of habeas data	18
13. Treatment of personal data of the services contracted by Clients	20
14. Entry into force and term	22

1. Introduction

DEFYTEK SAS with registered trade name Cari AI, hereinafter referred to as Cari AI, is legally constituted, with Nit. 900723497-4 and web address <https://www.cariai.com> and email datospersonales@cariai.com, will act as responsible and in charge of the treatment and custody of personal data, informs that:

The collection of personal data and the treatment of these, carried out by Cari AI, is done in a responsible and legal manner, complying with the right to privacy, habeas data, and the protection of personal data, in accordance with the regulations, procedures and instructions adopted by Cari AI, also in accordance with:

Cari AI carries out a correct management of the processing of personal data required for the provision of its services, for this, it has defined the following policy giving it an adequate management that the Law provides, and it is available to the entire internal and external community.

For the purposes of the following personal data processing policy, and in accordance with the definitions of Colombian law 1581 of 2012, it is understood as:

Authorization : prior, express and informed consent of the owner to carry out the processing of personal data.

Privacy Notice : Verbal or written communication generated by the Responsible, addressed to the Owner for the Treatment of their personal data, through which they are informed about the existence of the information Treatment policies that will be applicable, the way to access to them and the purposes of the treatment that is intended to give personal data.

Database: organized set of personal data that is subject to treatment.

Personal data: any information linked or that can be associated with one or more specific or determinable natural persons.

General data : contact, such as: full name, address, landline, mobile phone, email.

Particular data : depending on the type of relationship: Income level, financial data, debt capacity, gross assets, dependents, composition of the family group, hobbies or hobbies, assets owned, employment information, marital status.

Public data: **Public** data is considered, among others, data related to the marital status of people, their profession or trade and their quality as a merchant or public servant.

Sensitive data: **Sensitive data** is understood as that which affects the privacy of the owner or whose improper use may generate discrimination, such as those that reveal racial or ethnic origin, political orientation, religious or philosophical convictions, membership in trade unions, social, human rights organizations or that promote the interests of any political party or that guarantee the rights and guarantees of opposition political parties, as well as data related to health, sexual life, biometric data and medical history, which will only be collected, incorporated and/or stored with the prior authorization of the owner of the information, and when it is necessary for the execution of the contractual relationship with the owner, as long as the law allows access to said information. Therefore, the access, circulation and treatment of sensitive data will be restricted and limited to the authorization of the owner and to the provisions of current regulations.

in charge of the treatment: natural or legal person, public or private, that by itself or in association with others, carries out the treatment of personal data on behalf of the person in charge of the treatment.

Responsible for the treatment : natural or legal person, public or private, that by itself or in association with others, decides on the database and/or the treatment of the data.

Holder: natural person whose personal data is subject to treatment.

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

Transfer : the transfer of data takes place when the person responsible and/or in charge of processing personal data sends the information or personal data to a recipient who is inside or outside the country.

Transmission: treatment of personal data that implies the communication of the same within or outside the territory of the Republic of Colombia, when its purpose is to carry out a treatment.

Likewise, it has made an evaluation of the commitments generated by this legislation in the document **Cari AI-Obligaciones de Cari AI as Data Processor**.

2. Beginning

Cari AI will comprehensively apply the following principles in accordance with the provisions of Colombian Law 1581 of 2012:

- a) **Principle of legality in matters of data processing:** the treatment is a regulated activity that must be subject to the provisions of the law and the other provisions that develop it.
- b) **Principle of purpose:** the treatment must obey a legitimate purpose in accordance with the Constitution and the law, which must be informed to the owner.
- c) **Principle of freedom:** the treatment can only be exercised with the prior, express and informed consent of the owner.
- d) **Principle of veracity or quality:** the information subject to treatment must be truthful, complete, exact, updated, verifiable and understandable.
- e) **Principle of transparency:** in the treatment, the right of the owner to obtain from the person in charge of the treatment or the person in charge of the treatment, at any time and without restrictions, information about the existence of data that concerns him or her must be guaranteed.
- f) **Principle of access and restricted circulation:** the treatment is subject to the limits that derive from the nature of the personal data. In this sense, the treatment can only be done by persons authorized by the owner and/or by the persons provided for by law.
- g) **Security principle :** the information subject to treatment by the person in charge of the treatment or in charge of the treatment, must be handled with the technical, human and administrative measures that are necessary to grant security to the records avoiding their adulteration, loss, consultation, use or access. unauthorized or fraudulent.
- h) **Principle of confidentiality:** all persons involved in the processing of personal data that are not of a public nature are obliged to guarantee the confidentiality of the information, even after their relationship with any of the tasks included in the processing has ended.

3. Purpose of data processing

Cari AI will treat the information provided and previously authorized by users in the following way:

a. Generally:

For all users, students, employees, partners, suppliers, customers; will be used for:

- Know prospectively the needs of its stakeholders in order to innovate in the provision of its services.
- Compliance with the obligations derived from existing contractual relationships with its stakeholders.
- The safety of visitors, collaborators and the general community that are in the Cari AI facilities.
- Communicate to users registered in our systems, the web portal and/or social networks information about new services, news, events, academic calls, publications, novelties, business innovation, special programs, user education campaigns, commercial events and advertising, always related to the objectives of the company.
- Constantly publicize the needs of registered users in the web portals, in order to strengthen relationships and promote business innovation.
- Develop social responsibility programs in accordance with the statutes and internal regulations.
- That the data provided by collaborators may be shared with other companies for contractual purposes and/or for proposals or commercial agreements, unless expressly revoked by the owner of the data.
- Achieve efficient communication related to our services and alliances.
- To be employed in the evolutionary process of Cari AI services and products.
- Inform marketing activities and/or promotion of their own services or with whom they have entered into commercial alliances.
- Have your data analyzed in studies related to artificial intelligence issues.
- Know the state of satisfaction and care provided.
- Carry out statistical studies and market trends.
- The control and prevention of fraud and money laundering.

Cari AI Personal data protection policy

v3 - 26 Aug 2022 - PUBLIC USE

- Exchange or send information by virtue of international conventions or treaties.
- Inform about changes in the data processing policy.

b. Users and Clients:

The information will be used to:

- Develop the functions of the company.
- Communicate to users registered in our systems, the web portal and/or social networks information about new services, news, events, academic calls, publications, novelties, business innovation, special programs, user education campaigns, commercial events and advertising, always related to the objectives of the company.
- Constantly publicize the needs of registered users in the web portals, in order to strengthen relationships and promote business innovation.
- Inform marketing activities and/or promotion of their own services or with whom they have entered into commercial alliances.

c. Contractors and Suppliers:

They will be used to complement the development of contracts for the provision of services, or civil and/or commercial relations, monitoring and managing their commercial behavior. In addition, verify the suitability and exchange information on a regular basis to facilitate knowledge of the services offered by Cari AI; As well as, make them participate in activities or commercial campaigns that may be of interest to them.

The information contained in our databases, current or future, will be used so that Cari AI has a perception, both objective and subjective, about said providers. The information will be transferred and/or transmitted to other entities only when it is necessary to comply with the applicable legal provisions, in case it is required by a public, administrative entity and/or supervisory entities in labor matters in the exercise of their legal functions or by court order.

The corporate emails of providers and/or suppliers will be used in order to facilitate contact with employees, send internal communications of interest and make them participate in corporate activities, in addition, to comply with the laws applicable to suppliers.

d. Employees:

The information contained in our databases of former employees, employees, future job candidates, will be used so that Cari AI has a perception, both objective and subjective, about the personnel. Said information will be transferred and/or transmitted to other entities only when it is necessary to comply with the applicable legal provisions, in case it is required by a public, administrative entity and/or supervisory entities in labor matters in the exercise of their legal functions or by court order.

Corporate emails will be used in order to facilitate contact between employees and interest groups, send internal communications and make them participate in corporate activities.

In the case of collaborators, in addition to the above, they will allow access to transmit their data to companies that request to verify labor data, authorization of money credits or commercial credits, studies, for security studies prior verification of source and use of data and in accordance with Legal reserves will also be used to carry out internal promotion processes, verification of titles, request information from other companies or educational institutions, training, direct contact if required and in general to carry out all administrative and financial procedures directly related with the work for which he will be hired.

They will also be used to offer welfare programs to employees and plan business activities for the owner and his beneficiaries.

3.1 Treatment of sensitive data

As it is sensitive data and minors, the owner will be informed explicitly and in advance that he is not obliged to authorize its treatment.

They can only be treated when:

1. The owner of the personal data has given his explicit authorization to said treatment, except in cases where the granting of said authorization is not required by law.
2. The processing is necessary to safeguard the vital interest of the owner of the personal data and the latter is physically or legally incapacitated.
3. The treatment refers to data that is necessary for the recognition, exercise or defense of a right in a judicial process.
4. The treatment has a historical, statistical or scientific purpose. In this event, the measures leading to the suppression of the identity of the holders must be adopted.

The treatment of personal data of children and adolescents will be carried out under the parameters previously stated in this policy.

3.2 Video surveillance

The Processing of personal data has been defined as "any operation or set of operations on personal data, such as the collection, storage, use, circulation or deletion". In the case of images of specific or determinable persons, operations such as the capture, recording, transmission, storage, conservation, or reproduction in real time or later, among others, are considered as Processing of personal data, and consequently, they are subject to the General Regime for the Protection of Personal Data.

Cari AI does not capture your personal data through video surveillance for legitimate interest. Cari AI does not have physical infrastructure for the development of its functions, therefore, video surveillance is not carried out.

3.3 Cases in which authorization is not required

In accordance with article 10 of Law 1581 of 2013, the authorization of the holder will not be necessary in the case of:

- a) Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- b) Data of a public nature.
- c) Cases of medical or health emergency.
- d) Treatment of information authorized by law for historical, statistical or scientific purposes.
- e) Data related to the Civil Registry of persons.

Whoever accesses personal data without prior authorization must in any case comply with the provisions contained in the Law.

4. Legitimation for the exercise of the rights of the owner.

The rights of the holders established in the law, may be exercised by the following persons (article 20 decree 1377 of 2013; CHAPTER IV Of the Exercise of the Rights of Access, Rectification, Cancellation and Opposition Article 28):

1. By the holder, who must prove his identity.
2. By their successors in title, who must prove their quality.
3. By the representative and/or proxy of the holder, prior accreditation of the representation or power of attorney.
4. By stipulation in favor of another or for another.

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

5. Persons to whom the information may be provided

The information that meets the conditions established in this policy may be provided by Cari AI to the following people:

1. To the owners, their successors in title or their legal representatives.
2. To public or administrative entities in the exercise of their legal functions or by court order.
3. To third parties authorized by the Owner or by law.
4. To providers for the purposes authorized by the owner or those provided by law, for this Cari AI will ensure to establish conditions that link the provider to their privacy policies in such a way that the personal information of users is protected, likewise, confidentiality agreements will be established for the handling of the information and obligations responsible-in charge when the type of delivery warrants it.

6. Joint duties of Cari AI as RESPONSIBLE and those IN CHARGE of the processing of personal data

1. They must establish simple and agile mechanisms that are permanently available to the Holders so that they can access personal data and exercise their rights over them.
2. Reasonable measures must be taken to ensure that the personal data stored in the databases are accurate and sufficient and, when requested by the Holder or when the Responsible Party has been able to notice it, they are updated, rectified or deleted, in such a way that they satisfy the purposes of the treatment.
3. They must designate a person or area that assumes the function of personal data protection, who will process the requests of the Holders, for the exercise of the rights referred to in Law 1581 of 2012 and Decree 1377 of 2013.
4. Guarantee the Holder, at all times, the full and effective exercise of the right of habeas data;
5. Keep the information under the necessary security conditions to prevent its adulteration, loss, consultation, use or unauthorized or fraudulent access;
6. Adopt information security and privacy policies and procedures to guarantee adequate compliance with this law and, especially, for the attention of queries and claims by the Holders;
7. Duly inform the Holder about the purpose of the collection and the rights that assist him by virtue of the authorization granted.
8. The optional nature of the answer to the questions that are asked, when they deal with sensitive data or the data of children and adolescents;
9. Disclose contact information to resolve requests about data processing.

10. They must keep proof of compliance with their duties and, when the Holder requests it, deliver a copy of it.
11. Request and keep, under the conditions provided in this law, a copy of the respective authorization granted by the Holder;
12. Process queries and claims formulated in the terms indicated in this law;
13. Adopt policies and procedures in the areas/processes that apply, to guarantee adequate compliance with this law and especially, for the attention of queries and claims;
14. Comply with the instructions and requirements issued by regulatory entities and other government provisions.
15. Preserve evidence of the publication of the privacy notice and the information treatment policies, when they are published on the Internet.
16. Carry out timely updating, rectification or deletion of data under the terms of this law;
17. Process queries and claims made by the Holders in the terms indicated in this law;
18. Register in the legend "claim in process" in the way in which the law is regulated; "information under judicial discussion" once notified by the competent authority about judicial processes related to the quality of the personal data;
19. Refrain from circulating information that is being controversial by the Owner and whose blocking has been ordered by any regulatory entity.
20. Allow access to information only to people who can have access to it;
21. Inform the regulatory entities when there are violations of the security codes and there are risks in the administration of the information of the Holders; Comply with the instructions and requirements issued by regulatory entities.

6.1 Duties of Cari AI

Cari AI as the person in charge of the Treatment, at the moment of requesting the Holder the authorization, must inform him clearly and expressly of the following:

1. Comply with the provisions of the numeral 6 of this policy.
2. Guarantee that the information provided to the Treatment Manager is true, complete, accurate, updated, verifiable and understandable;
3. Update the information, communicating in a timely manner to the Person in Charge of the Treatment, all the news regarding the data that you have previously provided and adopt the other necessary measures so that the information provided to it is kept up to date;
4. Rectify the information when it is incorrect and communicate what is pertinent to the Treatment Manager;
5. Provide the Person in Charge of Treatment, as the case may be, only data whose Treatment is previously authorized in accordance with the provisions of this law;

6. Require the Treatment Manager at all times, respect for the security and privacy conditions of the Holder's information;
7. Inform the Person in Charge of Treatment when certain information is under discussion by the Owner, once the claim has been filed and the respective procedure has not been completed.
8. Keep proof of the authorization granted by the Holders of personal data for the Treatment of the same. For these purposes, Cari AI will deploy the physical and electronic means necessary to preserve the proof of the authorization granted by the holders of the personal data for the treatment of the same, regardless of the means through which said authorization has been obtained.

6.2 Duties of those in charge of processing personal data

1. Comply with the provisions of the numeral 6 of this policy.
2. Update the information reported by Cari AI within five (5) business days from its receipt;
3. Inform Cari AI about any update/change of the personal data protection policy, and privacy notice.
4. Inform Cari AI where the personal data protection policy and the privacy notice can be consulted.
5. Inform Cari AI of the means of contact to process queries and claims regarding the protection of personal data.
6. Inform Cari AI immediately of any information security and privacy incident to the contact [support@cari.ai.com](mailto:support@cari.ai).

7. Rights as the holder of personal data

The owner of the personal data will have the following rights:

1. Know, update and rectify your personal data in front of the Treatment Managers or Treatment Managers. This right may be exercised, among others, against partial, inaccurate, incomplete, fragmented, misleading data, or those whose Treatment is expressly prohibited or has not been authorized;
2. Request proof of the authorization granted to the company, except when expressly excepted as a requirement for treatment, in accordance with the provisions of Article 10 of Law 1581/2012;
3. Whoever exercises habeas data must accurately provide the requested contact information, in order to process and attend to your request and deploy the charges for the exercise of your rights.
4. Be informed by Cari AI, upon request, regarding the use it has given to your personal data;

5. Submit complaints to the competent authorities and regulatory entities for violations of the provisions of the law and other regulations that modify, add or complement it;
6. Free access to personal data that has been processed.

8. Special requirements for the processing of personal data of children and adolescents

Cari AI, in compliance with Law 1098 of 2006, Law 1581 of 2012 and Constitutional rights, recognizes that it has the possibility of acquiring data from minors, which are granted by its collaborators who are parents or legal representatives. Cari AI assumes the obligation to respect and provide guarantees so that minors can exercise their right to freedom of expression, free development of personality and information, as established by Law 1098 of 2006.

In compliance with Colombian regulations regarding minors and the responsible behavior that Cari AI is obliged to with the company, we assume the following commitments:

1. Exclude from our information system any minor, who has claimed to be older than this, at the time of registering as a user.
2. That responds and respects the best interests of children and adolescents.
3. To ensure respect for their fundamental rights.
4. Report to the authorities any criminal situation of which you are aware that endangers the integrity of a minor. For this, it will provide all the collaboration required by the State security organs.
5. Minors who are interested in acquiring our services, using electronic payment methods, must carry out the economic transaction electronically through their guardians or legal representatives, after registering and contracting with them.
6. Cari AI in the treatment of personal data of children and adolescents, delivered by our collaborators, will ensure their proper use.

9. Transfer and international transmission of personal data

In order to provide you with a better service, and to execute the purposes described in this privacy policy, your personal data may be transmitted and/or transferred to foreign entities and/or servers hosted in foreign countries, under security conditions that will guarantee the compliance with the provisions of law 1581 of 2012, and other regulatory decrees.

For the transmission and transfer of personal data, the following rules will apply:

1. International transfers of personal data must comply with the provisions of article 26 of Law 1581 of 2012; that is, the prohibition of the transfer of personal data to countries that do not provide adequate levels of data protection and the exceptional cases in which said prohibition does not apply.
2. The international transmissions of personal data that are made between a person in charge and a person in charge to allow the person in charge to carry out the

treatment on behalf of the person in charge, will not require to be informed to the owner or have his consent when there is a contract in the terms of article 25 of Law 1581 of 2012.

3. It is understood that a country offers an adequate level of data protection when it complies with the standards set by the Colombian regulatory entities. Exceptionally, Cari AI may transfer personal data in the following cases: a) Information for which the holder has granted his express and unequivocal authorization for the transfer. b) Transfers agreed within the framework of international treaties to which the Republic of Colombia is a party, based on the principle of reciprocity.
4. Transfers and/or transmissions necessary for the execution of a contract between the owner and Cari AI, or for the execution of pre-contractual measures, as long as they have the authorization of the owner.
5. Transfers legally required to safeguard the public interest, or for the recognition, exercise or defense of a right in a judicial process.

10. Contact through the web portal

The need to grant security to people when requesting demos, being part of our community or requesting more information about our products and services through our contact form or our chatbot, personal data of users is required, data that is also necessary for contact, sending information, as well as for fraud prevention and attention to security incidents.

Cari AI as administrator of the web portal www.cariai.com, will not keep a user's record when he has not provided truthful information, when he treats the information in a manner contrary to the honest uses that should be given to it or when he breaches the policies here contained or any of the obligations, duties and charges that you acquire at the time of registering or contacting us on the web portal.

The user who registers on this web portal will be responsible for any inaccurate, false or untrue data that they provide, for which they must be truthful and reliable, otherwise it may give rise to compensation for the damages that I will cause with this behavior to Cari AI and/or third parties. The person who uses personal data that is not their own, contrary to this policy or the law, will be responsible for the sanctions that Colombian and/or international legislation establishes in relation to the violation of personal data. This is how Cari AI assumes in good faith that the information provided by the user who registers is true, accurate and reliable, therefore exempting Cari AI from any responsibility for said information.

This document is an integral part of the Terms and Conditions of the website www.cariai.com and the legal agreement of the corporate web portals that provide services to external and/or internal users of Cari AI.

11. Attention to requests, request for consultation, updating, rectification and deletion of personal data

The continuous improvement process is in charge of processing the requests of the owners to make their rights effective.

This policy applies to all databases managed within each and every one of its dependencies. Cari AI expresses to users, clients, service providers, collaborators and suppliers, as well as to users of web portals and/or other tools, that in the event of any dispute it will be resolved amicably, through mechanisms autocompositive, such as negotiation or conciliation in the city of Bogotá.

12. Procedure for exercising the right of habeas data

a) **Queries:** the query will be made through the means enabled by Cari AI (see literal C), and will be answered within a maximum term of ten (10) business days from the date of receipt of the query. When it is not possible to attend the query within said term, the interested party will be informed, stating the reasons for the delay and indicating the date on which their query will be attended, which in no case may exceed five (5) business days following the expiration of the first term.

b) **Claims:** the owner or persons authorized by law who consider that the information contained in the databases should be corrected, updated or deleted, or when they notice the alleged breach of any of the duties contained in the aforementioned law, may file a claim with the institution, which will be processed under the following rules:

1. The claim will be made through a request addressed to Cari AI, with the identification of the owner, the description of the facts that give rise to the claim, the address, and accompanying the documents that you want to assert. If the claim is incomplete, the interested party will be required within five (5) days after receipt of the claim to correct the faults.
2. After two (2) months from the date of the request, without the applicant submitting the required information, it will be understood that the claim has been withdrawn.
3. In the event that the person who receives the claim within the company is not competent to resolve it, it will be forwarded to the appropriate person within a maximum term of two (2) business days and the interested party will be informed of the situation.
4. Once the complete claim is received, a legend will be included in the database that says "claim in process" and the reason for it, in a term not exceeding two (2) business days. Said legend must be kept until the claim is decided.
5. The maximum term to address the claim will be fifteen (15) business days from the day following the date of receipt. When it is not possible to address

the claim within said term, 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 finished.

c) **Contact to resolve your requests:** the owners may exercise their rights to consult, know, update, rectify and delete their personal data by sending their request to [datospersonales@cari.ai.com](mailto:datospersonales@cari.ai), or through the link: <https://site.cari.ai.com/#contact/> who will process the request in accordance with articles 14 and 15 of Law 1581 of 2012 and 20 to 23 of Decree 1377 of 2013; Said request must contain at least:

- Full name and surnames.
- Contact information (Physical and/or electronic address and contact telephone numbers).
- Means to receive a response to your request.
- Reason(s)/event(s) giving rise to the claim with a brief description of the right you wish to exercise (know, update, rectify, request proof of the authorization granted, revoke it, delete it, access the information) Signature (if applicable) and identification number. The signature of the person requesting the information.

d) **Controls:** Cari AI informs through its data protection policy to all its users, holders of data that are in the databases and/or files that the necessary technical, human and administrative measures have been implemented to provide security to our services. records avoiding their adulteration, loss, consultation, use or unauthorized or fraudulent access, the above, due to the nature of the data stored and the risks to which they may be exposed.

13. Treatment of personal data of the services/app contracted by Clients

The companies that contract the services of Cari AI are considered CLIENT of the service. The CLIENT who hires each Cari AI service is RESPONSIBLE FOR THE PROCESSING of their data.

Cari AI is IN CHARGE OF THE PROCESSING of the data of the CUSTOMERS of its products and/or services. The natural persons who use the services of the products contracted by the CLIENTS ARE end users; These are likely to be considered the DATA HOLDERS for the processes defined by each CLIENT.

Cari AI Personal data protection policy

v3 - 26 Aug 2022 - PUBLIC USE

Cari AI will implement the security conditions that the treatment defined by the RESPONSIBLE FOR THE TREATMENT determines, as reported through the channels and roles agreed upon during the project.

Cari AI will only carry out the indicated actions on personal data that the RESPONSIBLE FOR THE TREATMENT officially informs.

Cari AI will send any request related to personal data to the DATA CONTROLLER so that it is he who validates the relevance, origin, validity, authenticity and any other element that determines if said request should be carried out.

Cari AI will allow access to the information it has of the HOLDERS that the RESPONSIBLE FOR THE TREATMENT has validated.

Cari AI will develop the agreed actions within the parameters that the legislation determines and according to the service level agreements that have been agreed with each CLIENT.

Cari AI will implement internal awareness processes so that its personnel act in accordance with the requirements of the applicable legislation.

Cari AI has defined related contact points in literal C of the Item of procedures and queries. The Cari AI DATA PROTECTION OFFICER will be responsible for handling all Cari AI requests defined in this policy.

Considerations for each service in the transfer of information; Although Cari AI has its technological infrastructure in AWS ¹through IaaS ²and PaaS services ³, in datacenters in the USA; never transfers control of the information to another manager or data controller. The service that Cari AI uses from AWS maintains full control responsibility for the data and technology in Cari AI.

The responsibilities of the IaaS and SaaS services that AWS has are explained in this table, where BLUE is managed by Cari AI and RED is managed by the service provider (QSS in the case of IaaS and PaaS).

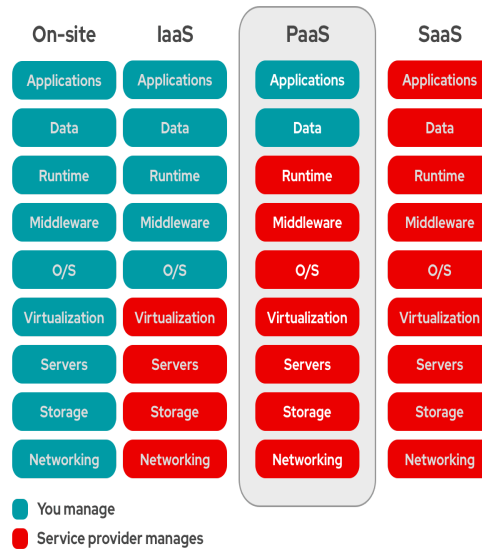
¹AWS: Amazon Web Services

²IaaS: Infrastructure as a Service

³PaaS: Platform as a Service

Cari AI Personal data protection policy

v3 - 26 Aug 2022 - PUBLIC USE



Therefore, Cari AI is a SaaS for its clients and uses IaaS and PaaS services to provide that service. This technical configuration does not change the fact that Cari AI is in charge of processing the data and that these have not been transferred to a third party, even if they have been transmitted to the USA.

"In the use of applications, information received from Google APIs will comply with the Google API Services User Data Policy, including limited use requirements."

"In the use of applications, information received from Meta APIs will comply with the Meta API Services User Data Policy, including limited use requirements."

Cari AI reads and stores public comments from Google and Meta applications, the data is used for reporting, reporting and other purposes as defined by our customers according to their service.

14. Entry into force and term

This policy has been approved on August 30, 2022, replaces the previous one and will come into effect from the date of publication on the intranet and website.

Cari AI will keep the information of each user for as long as it is required within the purposes described in this policy, unless there is a request for deletion by the interested party, notwithstanding the foregoing, personal data must be kept when so required. required for the fulfillment of a legal or contractual obligation.

Cari AI reserves the right to modify this policy at any time, any modification will be informed and published in a timely manner on the website <https://www.cariai.com>.