

DATA PRIVACY POLICY

Itajaí, November/2022

INDEX

INDEX	
INTRODUCTION	2
DEFINITIONS	3
SUMMARY OF PRIVACY POLICY	4
Scope	4
Data Minimization	4
Right of holders	4
Retention period	4
Collection of personal data	4
YOUR PERSONAL DATA AND HOW WE USE IT	4
Collection	4
Children and Adolescents	5
Treatment	5
TRANSFER OF DATA TO THIRD PARTIES	7
STORAGE AND DELETION OF PERSONAL DATA	8
YOUR RIGHTS	8
COOKIES, IDENTIFIERS, TRACKERS AND THIRD-PARTY INFORMATION	9
INCIDENTS	10
DATA SECURITY AND GOOD PRACTICES	10
DATA PROCESSING OFFICER (“DPO”)	10
CHANGES TO THE DATA PRIVACY POLICY	11
OUR DATA	11

1. INTRODUCTION

This Personal Data Privacy Policy defines how Allog Group acts to protect the personal data processed and controlled within the scope of its activities, as well as the privacy of the related Data Subjects.

This policy applies when we act as controller of personal data and manifests Allog Group's constant efforts to act in accordance with the applicable legislation and the organization's internal regulations related to data privacy, as well as developing appropriate technical and organizational measures to protect personal data against unauthorized or unlawful treatment, as well as accidental loss, alterations, disclosure, access, destruction, accidental damage, among other situations related to confidentiality, availability and integrity of personal data under its control.

In situations where we act as operators, we act in compliance with applicable law, good data privacy practices and in accordance with the instructions provided by the related controller. To this end, we promote training, capacity building and awareness campaigns to disseminate Allog Group's good data privacy practices to all our employees and promote faithful compliance with applicable legal obligations.

2. DEFINITIONS

In the course of this policy, we adopt the terms listed below with the respective meanings:

National Authority for Data Protection (NADP): It is the body that will supervise and guide the application of the LGPD (GLPD), as well as being responsible for applying administrative sanctions in case of violation of the law.

Legal Basis for Processing: The processing of Personal Data is allowed by the LGPD (GLPD) in accordance with the legal bases provided, such as the consent of the Data Subject, compliance with legal and/or regulatory obligations by Allog Group, the existence of a contract between Allog Group and the Data Subject, analysis for credit protection, as well as the legitimate interests of Allog Group or the Data Subject.

Biometrics: A measurable physical feature or a personal behavioral trait used to recognize or verify a person's identity. Facial images, fingerprints and iris samples are examples of biometrics.

Cookie: A cookie is an electronic file that contains an identifier (a string of letters and numbers) that is sent by a web server to a web browser and is stored by the browser. The identifier is then sent back to the server every time the browser requests a page from that server. Cookies can be either "persistent" cookies or "session" cookies. A persistent cookie will be stored by a web browser and will remain valid until the set expiration date unless deleted by the user before the expiration date. A session cookie, on the other hand, will expire at the end of the user's session, when the web browser is closed.

Information Security and Privacy Committee Means Allog Group's people committee composed of representatives of the following departments: Commercial, Operation, Product, Quality, Human Resources, and Information Technology (IT), which aims to propose improvements, changes and adjustments related to the Data Subject.

Data Protection Officer (DPO): Person appointed by Allog Group to act as a communication channel between the controller, the data subjects and the NADP.

Consent: It is the free, informed, and unequivocal statement by which the Data Subject agrees with the processing of his Personal Data for a specific purpose.

Personal Data: It is any data related to the identified or identifiable natural person, such as: IP, geolocation, name, RG (ID), CPF (SSN), address, telephone, bank account, vehicle data, among others.

Sensitive Personal Data: It is personal data that presents racial or ethnic origin, religious conviction, political opinion, union membership, data referring to health or sex life, genetic or biometric data.

Intended purpose: This is the reason or motivation for processing Personal Data.

legitimate interest: Data processing carried out by the Controller, due to his interest, that of other companies or society, without the processing affecting the individual rights and freedoms of the Data Subject.

General Law for the Protection of Personal Data (GLPD): Law No. 13.709, of August 14, 2018.

Open access: Data Subject's right to have access to all information regarding the processing of their Personal Data.

Objection: It is the Data Subject's right not to want their data to be processed. This right can be exercised in certain specific situations.

Security: It means the use of technical and administrative measures capable of protecting Personal Data from unauthorized access and accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination.

Treatment: It is every operation carried out with Personal Data, such as: collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation, information control, communication, transfer, diffusion, or extraction.

Data subject: Natural person referred to by the Personal Data that are subject to processing.

Transparency: It is the guarantee, to the Data Subjects, of clear, precise, and easily accessible information about the performance of the treatment and respective treatment agents, observing the commercial and industrial secrets.

3. PRIVACY POLICY SUMMARY

3.1. 3.1. Scope

This policy applies when we act as a personal data controller. In situations where we or our employees act as operators, we act in compliance with applicable legislation, good data privacy practices and in accordance with the instructions provided by the related controller.

3.2. Data minimization

We collect only the personal data necessary for the proper execution of our activities, in accordance with related legal bases.

3.3. Right of Data Subject

The provisions of the LGPD (GLPD), which highlight the right of access, rectification, opposition to treatment, portability, claim before the competent authorities and withdrawal of consent.

3.4. Retention term

The personal data processed is kept only for the time necessary according to the applicable legal basis, of which we highlight: the period of existence of the relationship with the Data subject, during the period necessary to comply with our legal, contractual obligations and regular exercise of rights, or for as long as the consent of the data subject.

3.5. Personal data collection

In general, personal data is collected directly from the Data subjects themselves. In some situations, we may seek them from other sources, always bearing in mind the legal basis required for processing this data and applicable legislation.

4. YOUR PERSONAL DATA AND HOW WE USE IT

4.1. Collection

In general, the personal data processed by Allog Group is collected directly from the data subjects themselves, who have a contractual relationship or have shown an interest in developing a relationship with us. With the exception of information required by law or by the applicable internal policies of Allog Group, the data subject's decision to provide us with his personal data is voluntary. However, it is important to point out that if the data subject chooses not to provide certain information, eventually we will not be able to perform some of the actions that require the use of this data to be performed, given the nature of the related activities.

In some other situations, personal data may be sought from other sources, such as publicly available data or data provided by public authorities, suppliers, contracted parties, other business partners and related sources, always bearing in mind the legal basis required for processing this data and their respective applicable legislation.

Data collection can occur directly and indirectly. Directly, when registering to receive information, business contacts, filling out forms, sending job resumes, participating in recruitment and selection processes, preparing, and signing contracts, among other actions related to the execution of our activities. Indirectly, when collected through existing technology on our website and apps, to provide a more positive user experience.

In the event that you provide Allog Group with personal data of third parties, in accordance with the existing relationship between the parties, but also in different cases such as job vacancies and resume deposit, you are responsible for ensuring that the data subject is aware of the information contained in this Data Privacy Policy and must have the consent of the respective person to share the information with us.

4.2. Children and Teenagers

Data collection from children and teenagers, that is, individuals under the age of 18, will only be carried out with the explicit authorization of the parent(s) and/or legal guardian(s) by means of a specific instrument, in person and informing the legitimate purposes for this. We do not deliberately collect personal data from children and adolescents in any other way.

If the user is under the age of 18, they must not register on our relationship platforms or provide us with any personal data. If we become aware that we have collected personal data from a child or teenagers, we will take reasonable steps to delete the personal data in question.

4.3. Treatment

Regarding the personal data processed within the scope of our activities, we highlight:

4.3.1. Registration data: Registrations may include name, e-mail address, address, CPF (SSN), telephone and cellular number, image, photo, audio, among other data related to the purpose of the registration in question and any related legal or contractual obligations (Employee File, Supplier Registration, Client Portfolio, Participants in Hiring Processes, Visitor Registration, among others).

4.3.2. Contact information: Information obtained through inquiries, requests and interactions gathered through our contact forms and means of communication, business, and relationship activities, among others.

4.3.3. Financial transaction data: Referring to transactions carried out through our services, including the purchase of products and/or services. Transaction data may include your address, CPF (SSN), financial and bank details, and credit card number, among others.

4.3.4. Data relating to the use of and through the use of our websites, products, cloud services and applications ("Computing Data"): Data usage may include your IP address, cookies, geographic location, browser type and version, operating system, time of visit to our websites, number of uses of Services, date of visit, among others

The collection of sensitive data takes place for clear purposes and with a legal basis for such, such as compliance with legal obligations, of which we highlight the Employee File, and legitimate interest for the operation of our activities, of which we highlight periodic examinations and biometric registration, and in this case, specific consent will be requested. Other purposes may be applied, as long as a specific term is applied for your knowledge and/or acceptance of the treatment in question.

It is important that you are aware of what we do with your data and what are the legal bases for this use. We highlight the following purposes of treatment:

Nº	FINS	BASE LEGAL
01	Trigger insurance	Consent
02	AD (Assets Directory) Contract Execution	Consent
03	Position Changes and Salary Adjustments	Contract Execution
04	Authentications/Recognition of Signature (notary office)	Legal Obligation
05	Building Access Registration (conciierge)	Consent
06	Marketing Activity Registration	Consent
07	Gifts Registration (shipments)	Consent
08	Customer base	Consent
09	Employee Registration (inclusion and maintenance of information) Legal Obligation	Legal Obligation
10	Driver Registration	Legal Obligation
11	Resumes Registration (candidates for vacancies)	Consent
12	Suppliers and Partners Registration	Contract Execution
13	Fleet Registration (vehicles)	Contract Execution
14	Registration Customer platform (customer portal)	Consent
15	User Registration (Software)	Contract Execution
16	Digital certification	Legal Obligation

17	Accounts Payable/Receivable	Contract Execution
18	Contracts	Contract Execution
19	Access Data to Publications (website/blog and social media)	Consent
20	Customs Clearance	Contract Execution
21	Sending documentation/orders (physical means)	Contract Execution
22	Deeds of assets/legal representatives	Legal Obligation
23	Performing psychological tests and profile analysis	Contract Execution
24	Training Management (internal/external training conducted through Allog)	Contract Execution
25	Pickup order (driver details)	Contract Execution
26	Satisfaction Survey (internal and external)	Contract Execution
27	Powers of Attorney	Contract Execution
28	Receiving and sending quotations	Contract Execution
29	Responsibility Term	Contract Execution

Personal data are processed for the purposes and in accordance with the bases mentioned above, not limited to these as long as a specific term is applied for knowledge and/or acceptance of the treatment in question by the data subject.

Upon electronic or physical acceptance of privacy terms, we consider that permission has been given by the data subject for the due treatment of their personal data, in compliance with legal and internal requirements related to data privacy.

Personal data under the control of Allog Group will not be used for purposes that are not compatible with those reported to their data subjects, except those required or authorized by law, as well as those of vital interest to the data subjects. In the event that other personal data is collected and processed, this document will be updated and disclosed in accordance with any legal requirements.

5. DATA TRANSFER TO THIRD PARTIES

We may disclose your personal data to any member of our group of companies (this means our subsidiaries, our controllers and all of their subsidiaries), to the extent reasonably necessary for the stated purposes and in accordance with applicable law, as well observing the legal bases of treatment informed in this policy.

We may disclose your personal data to our insurers and/or professional advisors, to the extent reasonably necessary for the purposes of obtaining or maintaining insurance coverage, managing risks, obtaining professional advice, or entering, exercising, or defending administrative, arbitration and/or legal. In addition, we may disclose your data to our suppliers and service providers to the extent reasonably necessary to provide you with our products and/or services and ensure security in their use and in the use of your personal data, such as suppliers, software companies, marketing and customer service services, network providers and cloud services. Such third parties may be located in other countries or have their servers located in different regions.

Financial transactions relating to our services and the purchase of our products and/or services are handled by our financial service providers, and we share transaction data with our payment service providers only to the extent necessary for the purposes of processing payments, refund

amounts, and handle complaints and queries related to these matters.

In addition to the specific disclosures of personal data established in this item, we may disclose your personal data whenever such disclosure is necessary to comply with a legal and/or regulatory obligation to which Allog Group is subject, as well as to protect its vital interests or the other Data Subject's vital interests. Prior to sharing, we will take the necessary precautions to ensure that related personal data will be adequately protected as required by applicable law.

Allog Group has offices and facilities in Itajaí, Porto Alegre, Campinas, Curitiba, São Paulo, Manaus, and Santos, as well as suppliers in other countries (website hosting, cloud services, payment gateways, technical support, development, modeling, customization, among others). In this way, we may transmit your data outside Brazil for the purposes indicated above. Allog Group adopts all appropriate measures and enters into the necessary contracts with its suppliers and offices to ensure that the processing of personal data outside Brazil is carried out in accordance with the LGPD (GLPD) and in compliance with Allog Group's policies.

You acknowledge that the personal data you provide to Allog Group through the existing relationship, services provided or our products and/or services may be transferred or accessible by operators internationally.

6. STORAGE AND DELETION OF PERSONAL DATA

6.1. We only keep personal data for as long as necessary, in accordance with specific procedures for retention and management of records in accordance with the existing legal basis, of which we highlight:

- a) During the relationship with the Data Subject.
- b) During the period necessary to comply with our legal, contractual obligations and regular exercise of rights, among other applicable legal bases.
- c) As long as the data subject's consent lasts, for cases where this is the legal basis.

6.2. We will retain your personal data in accordance with the available legal bases, given that due to the nature of the business in some cases it is not possible to specify in advance the periods for which your personal data will be retained in accordance with the existing relationship between the parties. In such cases, we will determine the retention period based on the following criteria, without prejudice to others:

- a) The existence of specific law or regulation demanding a specific period for data retention.
- b) Allog Group's internal policies.
- c) The existence of legal, administrative, or arbitral proceedings.
- d) Information requests made by government authorities.

7. YOUR RIGHTS

Allog Group respects the rights of the data subjects provided for in the LGPD (GLPD). Of these, we highlight:

- a) The right of access.
- b) The right of correction.
- c) The right to object to processing.

- d) The right to data portability.
- e) The right to sue before the competent authorities.
- f) The right to withdraw consent.
- g) The right not to be subjected to automated decisions and profiling.

You have the right to confirm whether or not we process your personal data and where we do, as well as the right to access such personal data. If the rights and freedoms of third parties are not affected, we will provide you with a copy of your personal data.

In certain circumstances, you have the right to have your personal data erased without undue delay. These circumstances include:

- a) Personal data is no longer necessary in relation to the purposes for which it was collected or processed.
- b) You withdraw consent to consent-based processing.
- c) Processing is for marketing purposes.
- d) Personal data was processed illegally.

However, there are exclusions to your right to object to processing, such as when it is necessary to exercise the right to freedom of expression and information, to comply with legal and/or regulatory obligations, to exercise rights in proceedings, or even for Allog Group's legitimate interest.

If you make such an objection, we will stop processing your personal data unless we can demonstrate compelling legitimate grounds for the processing that may override your interests, rights and freedoms, or the processing is for the establishment, exercise or defense of administrative, legal claims or arbitration.

If you consider that the processing of your personal information violates data protection legislation, you have the right to file a complaint with the competent authority and request that Allog Group immediately stop the processing in question.

To the extent that the legal basis for the processing of your personal data is consent, you have the right to withdraw this consent at any time. Withdrawal will not affect the legality of the processing prior to such withdrawal.

You can exercise any of your rights in relation to your personal data by means of a written notification to the Allog Group address, addressed to the Personal Data Processing Officer ("DPO – Data Protection Officer") or through an electronic procedure available on the website or by email at privacidade@allog.com.br

8. COOKIES, IDENTIFIERS, TRACKERS AND THIRD-PARTY INFORMATION

We use cookies on our website. To the extent that these cookies are not strictly necessary for browsing our website and/or providing our services, we will ask you to consent to the use of cookies when you visit our website.

Cookies do not normally contain any information that personally identifies a user, but the personal information we store about you may be linked to information stored in and obtained from cookies. We use cookies for the following purposes:

- a) Authentication – to identify you when you use our websites and electronic applications.
- b) Status - to help us determine whether you are logged into our websites and electronic applications.
- c) Customization – to store information about your preferences and customize services

for you.

d) Security - as an element of the security measures used to protect user accounts, including the prevention of fraudulent use of login credentials and to protect our portals, electronic applications, and services in general.

e) Advertising - to help us display advertisements that will be relevant to you.

f) Analysis - to help us analyze the use and performance of our website and services.

g) Cookies consent – to store your preferences regarding the use of cookies more generally.

Our service providers use cookies, and these cookies may be stored on your computer when you use our websites and electronic applications. Most browsers allow you to refuse to accept cookies and to delete cookies. The methods for doing this vary from browser to browser and from browser-to-browser version. Blocking all cookies will have a negative impact on the usability of many websites. If you block cookies, some of the features available on our websites and electronic applications may have their functionality compromised.

In addition to identifiers, we also use Web beacons that help us better manage the content on our websites by letting you know what content is effective. Web beacons are embedded in or associated with certain emails or other communications that you receive from us or our offices. Web beacons help us track your responses and interests and provide content and services that are relevant to you. For example, they may let us know when you take action based on emails we send.

We may use third-party services, such as open search tools and social media, to obtain information about you (such as your name or company) and enrich your personal data by obtaining publicly available information about you, such as your title, employment history and contact information.

9. INCIDENTS

Allog Group promptly assesses and responds to incidents that could compromise your Personal Data. If Allog Group becomes aware of any incident involving the Personal Data of data subjects under which it acts as controller, Allog Group will notify you and the responsible authorities.

10. DATA SECURITY AND GOOD PRACTICES

We take organizational security precautions, whether physical or technical, to promote good governance of personal data controlled by the organization. Protocols, controls, and related policies were developed, as well as procedures and guidelines to maintain these measures based on the performed risk mapping.

Training, qualification actions and specific dissemination campaigns for Data Privacy issues were included in our preventive actions, aimed at disseminating good practices and training our employees.

The Information Security and Privacy Committee is constantly proposing improvements, changes and adjustments related to the personal data privacy policy, information security and other regulations related to good practices applied by the organization.

11. DATA PROCESSING OFFICER (“DPO”)

Allog Group has a Data Processing Officer (“DPO”) duly appointed to act as a communication channel between the controller, the data subjects, and the National Data Protection Authority (NDPA). The identity and contact information are available on our website available at www.allog.com.br.

In case you need help, clarifications, or have questions about this Privacy Policy, please contact us by email at privacidade@allog.com.br (Mrs. Graciele Milan).

12. CHANGES TO THE DATA PRIVACY POLICY

Allog Group may change this policy at any time, and such updates are published on our website and other related platforms, which can be checked at any time. We recommend that you periodically check our communication tools to check for any changes to this Privacy Policy.

In the event of significant changes to this privacy policy, we may notify you of such changes via email or through specific messages on our communication platforms.

13. OUR INFORMATION

Allog Group is headquartered in the City of Itajaí, State of Santa Catarina, Brazil, at 333, Dr. Pedro Ferreira Street, Centro, CEP (zip code) 88301-030. In addition, we have branches in the cities of Campinas / SP, Curitiba / PR, Manaus / AM, Porto Alegre / RS, Rio de Janeiro / RJ, Santos / SP and São Paulo / SP.