GDPR Statement

This policy describes how **TAGME TECNOLOGIA LTDA** collects and processes personal data with respect to data subjects covered by the EU General Data Protection Regulation (GDPR). Depending on your geographic location, some parts of this statement may not apply to you. Except as described below, we are the processors of the personal data collected on our website. Our physical address is Avenida João Naves de Ávila, 1331 L6 - Room 654 and you can contact us by email at contato@tag.express. **Our EU representative is Osano International Compliance Services Limited and can be contacted by writing to North Wall Quay, Dublin 1D01C4E0.**

GDPR Principles

The GDPR principles exist to help businesses remain within the limits of the regulation and also help to understand its main objectives. Therefore, we comply with the contours and principles expressed as the core of compliance with the GDPR, which are:

Legality, fairness, and transparency. These first principles express the need to comply with the GDPR as required by this regulation due to our activities, as expressed in this Statement. We should keep you as informed as possible about our compliance with the GDPR.
Purpose limitation. As determined in the text of the GDPR, all purposes of data processing and collection must remain specific, explicit, and legitimate. The processor must use these personal data collected for the specific purposes for which consent was given for their collection and processing.
Data minimization. We only collect the data necessary and relevant to our activities. The fewer personal data we collect or process, the better for all parties involved.
Integrity and confidentiality. We protect and safeguard all personal data that we store and process and have methods to anonymize personal data.
Accountability. We remain committed to recording our activities and strategies, proving compliance with the GDPR and constantly reviewing and improving the management of personal data.

Data Collection Sources

In accordance with Decree No. 7,381 of December 2, 2010, which regulates the Tourism Law No. 11,771/2008, the daily movement of guests must be declared through the National Guest Registration Form. Therefore, the application of the NGRF is mandatory for all lodging facilities in Brazil. Thus, the data collected and/or received by TAG are the data listed in the NGRF.
By using our service through our website, our application, and the integration of our system with the hotel systems, we may ask you to provide us with certain personally identifiable information that can be used to contact or identify you ("Personal Data").

Categories of Personal Data

We collect the following categories of personal data:

- Full name;
- Date of birth;
- Age, Profession, and Gender;
- Cell phone, telephone, and email;
- Identification Document (Travel Document), Type, Issuing Authority (Issuing Country), ID, CPF (Brazilian individual taxpayer registry);
- Nationality, Permanent Address, City, State, Country;
- Vehicle plate, last origin, next destination, reason for travel, means of transportation;
- Guest signature;
- Cookies and usage data;
- Responses to satisfaction surveys (NPS).

Please remember that you have the right, at all times, not to disclose any personal information to us. However, this may impact and possibly limit your use of the website, and we may not be able to provide you with any Services to the extent that your personal data is necessary to allow us to provide such services.

Special Categories of Personal Data

We may collect personal data that is considered sensitive and classified as a "special category" under the GDPR. This may include:

Biometric data – Guest's facial photo (Selfie);

How we use your personal information

The data collected through our website, our application, and the integration of our system with hotel systems serve the following PURPOSES:

- Online check-in, with confirmation by the hotel, offering convenience and practicality to guests.
- Online check-out, with the application of satisfaction surveys in which the guest evaluates the services provided by the hotel.
- Offering the hotel the possibility to strengthen its relationship with guests through marketing campaigns, promotions, and loyalty programs, coordinating its operations more intelligently.

We follow GDPR guidelines in informing you about our uses, bases, and purposes for the collection and processing of your personal data. If any of these purposes change, we will be sure to inform you of any changes to the purposes, why we collect and process your data, and for what purpose.

Sharing of Your Personal Information

Upon collection, personal data is transferred to our system's databases, through online transmission via the Internet to the Amazon Web Services cloud, where it is stored and archived. TAG does not store or archive data on paper.

Only control data such as full address, CPF and email are shared with third-party platforms (for example, the IUGU sub-acquirer for check-out processing). The guest's credit card data goes directly from the browser to the IUGU, it is not stored in the TAG. It is worth remembering that IUGU is a PCI DSS compliant company.

Data sharing is only done with the hotel where the reservation was made. No personal data is shared with other hotels.

Under no circumstances will we transfer the data collected for advertising on third party websites. The information collected is kept exclusively with TAG and the hotels chosen by the user.

In accordance with Law 11,771/2008 and Decree 7,381/2010, check-ins and check-outs must be kept indefinitely by the hotel and entered into SNRHos, the National Guest Registration System of the Ministry of Tourism. Therefore, for the hotel's convenience, personal data is archived indefinitely.
The transmission of the content of personal data may occur on a mandatory basis for law enforcement, in rare circumstances, in accordance with a valid request from the authorities. However, the request will only be granted if it is made in accordance with applicable laws and regulations.

Legal Basis for Processing

The General Data Protection Law, or simply LGPD, is the Brazilian regulation related to the General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, published on April 27, 2016. It shares the same principles as the European regulation. Law 13.709/2018 aims to create an environment of legal security and standardization of rules related to the protection of citizens' data.

With the aim of clearly and transparently explaining our commitment to privacy and personal data protection, we have prepared this PRIVACY POLICY.
AVISO DE PRIVACIDADE TAG

This document represents a legal statement to demonstrate TAG's commitment to GDPR compliance. The Privacy Policy clarifies our procedures and practices regarding the collection and use of your personal data, details your rights as a data subject, and makes clear how we ensure the integrity and security of the information we store, demonstrating compliance with the principle of transparency.

The Policy covers all personal data of guests who use our system to automate hotel processes. Therefore, it details how and why we may collect, use, process, share, and retain the personal information you provide to us. Additionally, we clarify who has access to your data, the purposes for which they are processed, and how you can control the sharing of your information.

International Data Transfer Mechanisms

Many companies in the United States have commercial interests and operations within the European Union, which involves the processing of personal data of EU citizens protected by the GDPR. In light of this, Brazilian authorities, in accordance with the General Data Protection Law (LGPD), have recognized the need to establish valid mechanisms for the transfer of such data without compromising its security. Below are the main mechanisms:

Standard Contractual Clauses (SCCs): Also known as SCCs, these clauses are part of contracts between data controllers and processors to ensure secure and responsible transfers between EU countries and third countries.

Adequacy Decision: This decision is made when the Brazilian authority concludes that the destination country for the data offers a level of protection equivalent to that provided for in the LGPD. This allows data to be legally processed by the country or territory of destination as if it were under Brazilian jurisdiction.

Explicit Consent of the Data Subject: When not falling under other legal bases, international data transfers can be carried out with the explicit consent of the data subject.

International Contracts: Contracts containing specific clauses to ensure adequate data protection during international transfer.

Data Processing Agreement

DPA — TAGME TECNOLOGIA LTDA

Your Data Subject Rights

Right to **knowledge or confirmation**. You have the right to obtain confirmation if your personal data is being processed.

Right of **access**. The system allows you to access your information and processed data and for what purpose they are being used. The use of personal data and data produced by TAG aims to automate check-in and check-out. The system also uses the CRM tool, which allows the hotel to use personal data for sending personalized communications and marketing campaigns, and the NPS tool for satisfaction surveys.

Right to **copy**. Upon formal request by the data subject, we guarantee the provision of a copy of your personal data within 7 business days.

Right to **rectification**. To rectify your record, you may request the hotel to modify it accordingly if you believe your personal data is incomplete or incorrect.

Right to **erasure** (deletion). No personal data is deleted in accordance with state regulations. According to Law 11.771/2008 and Decree 7.381/2010, check-ins and check-outs must be kept indefinitely by the hotel and entered into the SNRHos, National Guest Registration System of the Ministry of Tourism. TAG also allows, upon request made by the data controller via email, the viewing, deletion, and anonymization of data entered into our platforms. Anonymized data, i.e., data that can no longer be associated with you as an individual, may be used for research and statistical purposes, in which case we may use this information indefinitely without prior notice.

Right to **restriction of processing**. You have the right to request restriction of the processing of your personal data when:

- The accuracy of personal data is contested;
- The processing of personal information is illegal and you do not require its deletion;
- The data controller no longer needs the personal data, but is required to keep it to comply with a legal obligation or to proceed or defend a legal action;
- You have objected to the processing of your personal data during the verification period by the controller.

Right to **object and withdraw consent**. The consent consists of free expression (the data subject must have the option to consent or not consent), informed (the data subject must be well informed about the processing to which they are consenting), and unequivocal (the data subject must have no doubts about their expression of

consent). Also, the customer can revoke consent at any time, which does not render illegal any processing carried out while consent is in force.

Right to **anonymization**. TAG also enables, upon request made by the data controller via email, the viewing, deletion, and anonymization of data entered into our platforms. Anonymized data, i.e., data that can no longer be associated with you as an individual, may be used for research and statistical purposes, and in this case, we may use this information indefinitely without prior notice.
The customer may exercise this right, upon request, through TAG channels.

Data Protection

Our priority is to protect the data you entrust to us. We employ a variety of technical and organizational measures to ensure the security of your personal data. This includes physical, administrative, and technological precautions to reduce the risk of loss, misuse, unauthorized access, disclosure, or alteration of your personal information. Access to your data is limited only to those who need it to perform their specific functions.

Furthermore, all employees of our company undergo information security training, undergo background checks, and are required to sign a binding confidentiality agreement.

In the event of a data breach and exposure of personal data, supervisory authorities in our jurisdiction will be notified within 72 hours.

For your security, whenever you submit a request to exercise your rights, TAG may request some additional information and/or documents to verify your identity, aiming to prevent fraud. We do this to ensure the security and privacy of everyone.

In some cases, TAG may have legitimate reasons to refuse to comply with a request to exercise rights. These situations include, for example, cases where disclosure of specific information could violate intellectual property rights or business secrets, whether ours or third parties'. Other examples are cases where requests for data deletion cannot be fulfilled due to TAG's obligation to retain data, either to comply with legal or regulatory obligations or to enable its own defense or that of third parties in disputes of any nature.

Furthermore, some requests may not be immediately answered, but TAG is committed to responding to all requests within a reasonable timeframe and always in accordance with applicable legislation.

Data Protection Officer

We have appointed a Data Protection Officer. You may contact him at:

DPO: Lucas Boaventura Menezes

Telefone / WhatsApp: (34) 99979-9099

E-mail: lucas@tag.express