

KLARA AI S.A.
PRIVACY POLICY

Klara AI application and platform — myklara.ai (Brazil)

Last updated: 31.08.2026 | Effective date: 31.08.2026

English version. The Portuguese-language version is the only legally binding version. In case of discrepancies between language versions, the Portuguese version shall prevail.

1. Introduction and scope

This Privacy Policy (the «Policy») describes the processing of personal data carried out by KLARA AI S.A. («KLARA») in connection with the use of the Klara AI mobile application and the services accessible through it (collectively, the «Services») in Brazil.

This Policy has been prepared in compliance with Law No. 13,709/2018 («LGPD»), the Brazilian Internet Civil Framework (Law No. 12,965/2014), the Consumer Defense Code (Law No. 8,078/1990) and the remaining applicable regulations on data protection and consumer protection in Brazil.

2. Data controller

Name	KLARA AI S.A.
CNPJ	57.651.484/0001-56
Address	Alameda Rio Negro, n.º 1030, sl. 2304, Alphaville Centro Industrial e Empresarial, Barueri/SP, CEP 06.454-000, Brasil
Legal representative	Sérgio Ossiliere Furtado de Campos, Company's Legal Representative, pursuant to Power of Attorney (CPF 979.802.426-53)
Privacy contact	compliance@theklara.com

For the purposes of art. 41 of the LGPD, KLARA has designated a data protection contact channel, reachable at compliance@theklara.com, responsible for receiving communications from data subjects and the Brazilian National Data Protection Authority (ANPD), providing clarifications and adopting measures in relation to the processing of personal data described in this Policy.

3. Nature of KLARA and provider of the Banking-as-a-Service solution

KLARA is a technology company acting as an application layer and digital interface. KLARA is not a financial institution, a payment institution or an electronic money institution and does not itself provide regulated financial services. The financial services available through the Application (payment account, card, execution of payments) are provided by CELCOIN INSTITUIÇÃO DE PAGAMENTO S.A., a payment institution authorised and supervised by the Central Bank of Brazil, engaged by KLARA to provide the Banking-as-a-Service technology solution. The User's financial relationship with such services is governed by the specific terms of CELCOIN.

3.1. The User acknowledges and agrees that the payment account held in their name will be opened directly with CELCOIN INSTITUIÇÃO DE PAGAMENTO S.A., enrolled under CNPJ No. 13.935.893/0001-09, a partner company engaged by KLARA AI S.A. to provide the Banking-as-a-Service technology solution (“Bank as a Service”/“BaaS”), which encompasses the procedures for opening and managing payment accounts, issuing electronic currency, and processing and settlement services.

3.2. The User acknowledges and agrees that all data provided for opening and maintaining the account will be used by CELCOIN solely to fulfil the contractual relationship entered into with KLARA AI S.A., and the duties arising from current regulations, always in compliance with data protection and information security legislation. CELCOIN may, at any time, request additional information for legal and regulatory purposes.

4. Categories of data processed

KLARA processes the following categories of personal data of the User:

- a) Identification and contact data: name, surnames, date of birth, postal address, e-mail address, phone number, and, where applicable, CPF (Brazilian individual taxpayer registry number).
- b) Account and profile data: access credentials, preferences, history of interactions with the Application.
- c) Technical and usage data: IP address, device identifiers, operating system, logs and telemetry data.
- d) Financial and transactional data: accessible through CELCOIN's API (balance, transaction history, card status). KLARA does not store full card data (PAN, CVV).
- e) Health data (WoMoon): only where the User expressly activates the WoMoon feature, subject to the WoMoon Consent.
- f) AI usage data: prompts, queries and messages entered by the User in the conversational assistant, which are stored by KLARA and are not used to train models.

5. Purposes and legal bases

KLARA processes personal data for the following purposes:

Purpose	Data	Legal basis
Management of the User's account and provision of the Services	Identification, account, technical data.	Performance of the contract (art. 7, V, LGPD)
Customer service and operational communications	Contact and usage data.	Performance of the contract (art. 7, V)
Compliance with legal and regulatory obligations (tax, accounting, AML)	Identification, financial, KYC data.	Legal/regulatory obligation (art. 7, II)
AI assistant features	Prompts, queries, usage data.	Performance of the contract (art. 7, V)
Processing of health data (WoMoon)	Data under art. 11 LGPD provided by the User.	Specific and highlighted consent (art. 11, I)
Commercial communications and marketing	Contact and usage data.	Consent (art. 7, I)
Analytics and product improvement	Pseudonymised usage data.	Consent, or legitimate interest where legally permitted (art. 7, I / IX)
Security and fraud prevention	Technical and usage data.	Legitimate interest (art. 7, IX) and legal obligation (art. 7, II)

6. Recipients

KLARA discloses personal data only where necessary for the provision of the Services, the fulfilment of legal obligations or the protection of legitimate interests. The main recipients are:

- CELCOIN INSTITUIÇÃO DE PAGAMENTO S.A. — payment institution providing the financial services and the KYC procedures, authorised and supervised by the Central Bank of Brazil. Acts as an independent data controller with respect to the financial data and the AML/KYC procedures.
- Infrastructure providers — Amazon Web Services (cloud hosting).
- Payment services provider — Stripe, Inc., for the processing of Subscription fees via Stripe Elements. Card data is entered in fields hosted by Stripe without passing through KLARA's servers.
- AI providers — the conversational assistant and AI-generated content features of the Application are provided by OpenAI, acting as a data operator on behalf of KLARA under art. 39 of the LGPD and a data processing agreement. KLARA may in the future integrate additional AI providers as its capabilities evolve; this Policy will be updated in advance of any such change. Where processing by KLARA's AI provider(s) takes place outside Brazil, KLARA applies the safeguards required by art. 33 of the LGPD for international data transfers.
- Communications and marketing automation provider — Customer.io, Inc. (United States), for transactional communications and, subject to the User's consent, commercial and lifecycle communications.

- Analytics and marketing providers — including AppsFlyer, Segment, PostHog, Firebase, Meta SDK, TikTok SDK, Google Ads and Smartlead. Their activation is subject to the User's consent through the cookie banner of the Website or the App Tracking Transparency mechanism on iOS.
- Authorities and advisors — public, judicial or supervisory authorities where a legal obligation exists (including the ANPD and the Central Bank of Brazil); legal and tax advisors subject to professional secrecy.

KLARA does not sell personal data to third parties and does not make it available to data brokers for monetisation purposes unrelated to the Services.

7. International transfers

Certain recipients identified in Section 6 above process personal data outside Brazil. In particular, Stripe processes data in the United States; and the analytics, attribution, marketing and communications providers (including AppsFlyer, Segment, PostHog, Firebase, Meta SDK, TikTok SDK, Google Ads, Smartlead and Customer.io) carry out or may carry out processing outside Brazil, including transfers to the United States and, as regards TikTok, transfers to the People's Republic of China. For all international transfers, KLARA adopts the safeguards required by art. 33 of the LGPD, including standard contractual clauses, specific consent of the User where applicable, and, where relevant, ANPD adequacy decisions regarding the recipient country. KLARA's main infrastructure hosting is performed via Amazon Web Services.

8. Retention periods

Personal data is retained only for the time necessary for the purposes of the processing and to respond to any liabilities arising therefrom. Indicative periods are as follows:

Category	Period
User account data	While the contractual relationship is maintained and until a deletion request.
AML/KYC and financial data	Five (5) years from the termination of the relationship, in accordance with Law No. 9,613/1998 and applicable Central Bank of Brazil regulations for payment institutions.
Accounting and tax documentation	Five (5) years, pursuant to the Brazilian National Tax Code (CTN).
Health data (WoMoon)	While the User keeps the Feature active and consent has been given. Erasure following withdrawal in accordance with the grace period set out in the WoMoon Consent.
Technical, usage and log data	Up to 24 months from generation.
Marketing and communications data	Until revocation of consent.

9. Security

KLARA applies appropriate technical and organisational security measures in accordance with art. 46 of the LGPD, proportionate to the nature, scope and risks of the processing. Such measures include, among others: encryption in transit and at rest, access control restricted to authorised personnel, activity logs, staff training and incident management procedures. In the event of a personal data security incident posing a relevant risk to data subjects, KLARA will comply with its notification obligations under art. 48 of the LGPD, including communication to the ANPD and to the affected data subjects, where applicable.

10. Automated decisions

KLARA's conversational assistant does not adopt automated decisions that define the User's personal, professional, consumer or credit profile, or aspects of their personality, within the meaning of art. 20 of the LGPD. The responses and «insights» generated are purely informative and do not entail any approval, denial or credit assessment. The User may request a review of decisions taken solely on the basis of automated processing that affect their interests, in accordance with art. 20 of the LGPD. The automated controls applicable to the provision of financial services (including fraud prevention and AML/KYC filters) are executed by CELCOIN in its capacity as a regulated payment institution.

11. Rights of the data subject

The User may exercise at any time the rights afforded under the LGPD (art. 18), including: confirmation of the existence of processing; access to data; correction of incomplete, inaccurate or outdated data; anonymisation, blocking or deletion of unnecessary or excessive data; data portability; deletion of personal data processed with consent; information about public and private entities with which KLARA has shared data; information about the possibility of not providing consent and the consequences thereof; and revocation of consent. For that purpose, the User may contact compliance@theklara.com.

KLARA will respond to requests for confirmation of processing or access to data immediately, in simplified format, or within fifteen (15) days, in complete format, in accordance with art. 19, §1 of the LGPD. The User may also lodge a complaint with the Brazilian National Data Protection Authority (ANPD), www.gov.br/anpd.

12. Minors

The Services are directed exclusively at persons who have reached eighteen (18) years of age. KLARA does not knowingly collect personal data of minors. Should KLARA become aware of the use of the Services by a minor, their data will be erased without undue delay, in accordance with the best-interest-of-the-child principle set out in art. 14 of the LGPD.

13. Cookies and App Tracking Transparency

The use of cookies and similar technologies is governed by the Brazilian Internet Civil Framework (Law No. 12,965/2014) and the LGPD. Non-essential cookies are used subject to the User's consent, collected through a preference mechanism that allows the User to accept, reject or manage preferences by category.

On iOS devices, the Application implements Apple's App Tracking Transparency («ATT») mechanism. Advertising identifiers and events are not shared with marketing providers prior to obtaining the User's consent.

14. Commercial communications and direct marketing

KLARA may send the User commercial communications, by electronic means or other channels, in relation to its Services, subject to the User's prior consent, in accordance with art. 7, I of the LGPD, offering in each communication a simple and free opt-out mechanism, in line with the Consumer Defense Code (Law No. 8,078/1990).

The User may object at any time to the sending of commercial communications by means of the unsubscribe mechanisms included in each communication, by managing preferences within the Application, or by contacting compliance@theklara.com. The objection will not prevent the sending of communications strictly necessary for the performance of the contract (service notices, operational notifications, legal communications).

15. WoMoon feature

The optional WoMoon feature allows the User to track menstrual cycle, fertility and reproductive wellness. Its activation entails the processing of health-related data within the meaning of art. 11 of the LGPD, on the basis of the User's specific and highlighted consent (art. 11, I LGPD). WoMoon data is kept isolated from any financial functionality and is not used for credit assessment, financial profiling, nor disclosed to insurers or advertisers. The detailed regime of WoMoon, including the mechanism for withdrawal of consent, is set out in the WoMoon Consent that the User must accept upon activating the Feature.

16. Amendments to the Policy

KLARA may amend this Policy to reflect regulatory, technical or operational changes. The updated version will be available in the Application. Where the changes are substantial and affect the User's rights, KLARA will notify the User reasonably in advance.

17. Contact

E-mail	compliance@theklara.com
--------	--

Postal mail	KLARA AI S.A. — Alameda Rio Negro, No. 1030, Suite 2304, Alphaville Centro Industrial e Empresarial, Barueri/SP, CEP 06454-000, Brazil. Ref.: «Privacy»
Supervisory authority	Brazilian National Data Protection Authority (ANPD) — www.gov.br/anpd