Privacy Policy

Last updated: November 1, 2026 · Version 1.2

1. Who we are and who this policy applies to

Guvik (GUVIK TECNOLOGIA E INTELIGENCIA ARTIFICIAL LTDA, registered under CNPJ (Brazilian company tax ID) 67.712.906/0001-00, headquartered at AV BRIG FARIA LIMA, 1811, Conj. 1119, Jardim Paulistano, São Paulo/SP, CEP 01452-001, Brazil) is a Brazilian company that develops and operates an orchestration platform for **AI agents for SAP**, focused on support (AMS), projects, documentation and the evolution of SAP solutions (ECC and S/4HANA).

This Privacy Policy describes how we process personal data in connection with:

- Visitors and users of the corporate website (`guvik.ai`);
- Registered users of the application/product (`dashboard.guvik.ai` / `app.guvik.ai`) and of the agent API (`agent.guvik.ai`), including individuals who purchase the **personal plans**, which are also governed by the **Personal Plan Terms**;
- Business partners and users of the Partner Portal (`parceiros.guvik.ai`);
- People who submit an **access dispute** concerning an SAP environment;
- Business contacts, leads and subscribers to Guvik communications.

This policy does **not** cover the processing of data of job applicants at Guvik — for them, please see the **Privacy Notice for Applicants**. It also does not replace the **Data Processing Agreement (DPA)**, which governs the processing of customer data when Guvik acts as operator/processor, as explained in Section 3.

Our primary regime is the **Lei Geral de Proteção de Dados** (LGPD, Brazilian General Data Protection Law, Law No. 13,709/2018), under the supervision of the **Autoridade Nacional de Proteção de Dados** (ANPD, Brazilian National Data Protection Authority). For data subjects located in the European Economic Area (EEA), we also comply with the **GDPR** (Regulation (EU) 2016/679) and, in the United Kingdom, with the **UK GDPR** and the Data Protection Act 2018. For consumers residing in the United States, we comply with the **CCPA/CPRA** in California and with other state privacy laws, when applicable. These regimes are addressed in a coordinated manner in this policy.

This policy is a single text, valid in every country where Guvik offers its services. The language in which you read it does not change the applicable law or your rights. The rules specific to each region (Brazil; European Economic Area and United Kingdom; United States; other countries) are in Section 16.

2. Personal data we collect

Category	Examples	Source
Account data	Name, email, job title and company (when provided), password (hash), language and preferences	Provided by the data subject at sign-up
Purchase and payment data	Name, CPF (Brazilian individual tax ID, in Brazil) or, outside Brazil, country of residence and address, plan and term purchased, billing history, withdrawal and cancellation requests, tax documents. Card or payment account data stays with the payment institution (in Brazil, Asaas; outside Brazil, the payment method shown in the purchase summary); Guvik keeps only identifiers and the results of charges	Provided by the data subject at purchase and generated by billing
Referrals and coupons	Referral code, link between referrer and referred person, coupon used	Generated by use of the programs
Contact/business data	Name, email, phone, company, messages in forms	Provided by the data subject (website, leads, support)
Platform usage content	Prompts and messages exchanged with the AI agents, generated artifacts (documents, code, answers), conversation history, files and workspace memory	Generated by use of the product
SAP object metadata	Names and identifiers of ABAP/SAP objects queried, search results, source code snippets read during debugging	Generated by use of the product, from the connected SAP environment
SAP connection credentials	Username and password provided to connect to the SAP environment	Provided by the data subject. For a personal connection, they are kept in memory only, for up to 12 hours; if the data subject chooses to save them in the vault, they are stored encrypted in Guvik's storage until removed or until the connection is deleted. They are never sent to AI providers
Acceptances and declarations	Document accepted, version, language and hash of the text displayed, date and time, verified IP address and browser. For SAP connection declarations, also the environment, the responsible company and the CNPJ or the country's tax identification provided, the relationship, the type of environment and the form of authorization	Generated when the data subject accepts a document or declares a connection
Access logs	Account identification, date and time of access, verified IP address and technical session data	Generated automatically at login and session renewal

Category	Examples	Source
Access disputes	Name, company, email, description of the case and IP address of the person submitting the dispute	Provided by the disputing party
Telemetry and usage	Tokens consumed, estimated cost, latency, errors, technical logs, IP address, device/session identifiers	Generated automatically by the platform
Partner data	Partner company registration, sales opportunities, interactions on the Partner Portal	Provided by the partner
Cookies and browsing data	Session identifiers and preferences (such as language)	Collected automatically (see Section 8)

We do not deliberately collect sensitive categories of personal data (for example, health data, biometrics, racial or ethnic origin). If conversation content or source code entered by a customer incidentally contains personal data of third parties (e.g., names in test data or SAP code comments), Guvik processes such data **on behalf of the customer**, as operator/processor, under the DPA.

3. Guvik's role: controller vs. operator/processor

Guvik acts in two distinct roles, depending on the type of data:

Type of data	Guvik's role	Applicable instrument
Account, purchase and payment, referral and coupon, acceptance and declaration, access log, dispute, contact, business, website browsing and partner data	**Controladora** (LGPD) / **Controller** (GDPR and UK GDPR) / **Business** (CCPA/CPRA) — decides purposes and means	This Privacy Policy
Conversation content, SAP metadata and other data processed on the platform on behalf of the customer while providing the service	**Operadora** (LGPD) / **Processor** (GDPR and UK GDPR) / **Service provider** (CCPA/CPRA) — processes according to the customer's instructions	Data Processing Agreement (DPA)
Data from a company's SAP environment that a personal plan holder connects to their account	**Operator/processor**, following the instructions of the data subject, who acts on behalf of the company responsible for the environment; that company is the controller	Personal Plan Terms (Section 11) and this Policy

When Guvik acts as operator/processor, the contracting customer is the controller of that data and is responsible for ensuring a legal basis for entering it into the platform. Guvik's obligations in that role — documented instructions, confidentiality, security measures, subprocessors, incident assistance — are detailed in the **Data Processing Agreement (DPA)**.

In the personal plan, for each connection, the data subject declares in the **SAP connection authorization declaration** that they have authorization from the company responsible for the environment to have that data processed by Guvik and sent to AI providers, including providers abroad. The responsible company may dispute the access through the page `app.guvik.ai/contestar-acesso`, which requires no account or login.

4. Purposes and legal bases

Purpose	Data involved	LGPD legal basis	GDPR / UK GDPR legal basis
Create and manage user accounts	Account data	Performance of contract (Art. 7, V)	Performance of contract (Art. 6(1)(b))
Provide the service (chat with agents, SAP object search, AI Debug, workflows, jobs, scheduling)	Account, usage content, SAP metadata, SAP credentials	Performance of contract (Art. 7, V)	Performance of contract (Art. 6(1)(b))
Sell and bill the personal plan, process withdrawals, cancellations and plan changes	Purchase and payment, account	Performance of contract (Art. 7, V)	Performance of contract (Art. 6(1)(b))
Issue tax documents and meet accounting obligations	Purchase and payment	Legal obligation (Art. 7, II)	Legal obligation (Art. 6(1)(c))
Prevent fraud and ensure single use of Guvik Start, referrals and coupons	CPF (in Brazil), email, payment method, referrals and coupons	Legitimate interest (Art. 7, IX)	Legitimate interest (Art. 6(1)(f))
Prove acceptance of documents and connection declarations	Acceptances and declarations	Regular exercise of rights (Art. 7, VI)	Legitimate interest (Art. 6(1)(f))
Keep the access logs required by the Marco Civil da Internet (Brazilian Internet Civil Rights Framework, Law No. 12,965/2014, Art. 15)	Access logs	Legal obligation (Art. 7, II)	Legal obligation (Art. 6(1)(c))
Review access disputes and suspend connections when necessary	Disputes, declarations, access logs	Legitimate interest and regular exercise of rights (Art. 7, IX and VI)	Legitimate interest (Art. 6(1)(f))
Send notices about renewal, billing, closure and deletion of the account	Account, purchase	Performance of contract (Art. 7, V)	Performance of contract (Art. 6(1)(b))
Technical support and AI-assisted triage	Account, usage content, telemetry	Performance of contract / legitimate interest (Art. 7, V/IX)	Performance of contract / legitimate interest (Art. 6(1)(b)/(f))

Purpose	Data involved	LGPD legal basis	GDPR / UK GDPR legal basis
Invoicing and commercial management	Account data, business data	Performance of contract / legal obligation (Art. 7, V/II)	Performance of contract / legal obligation (Art. 6(1)(b)/(c))
Information security, fraud prevention and auditing	Telemetry, logs, account data	Legitimate interest (Art. 7, IX)	Legitimate interest (Art. 6(1)(f))
Product improvement and aggregate metrics	Telemetry (usage, cost, errors)	Legitimate interest (Art. 7, IX)	Legitimate interest (Art. 6(1)(f))
Commercial communications and marketing	Contact/lead data	Consent / legitimate interest (Art. 7, I/IX)	Consent / legitimate interest (Art. 6(1)(a)/(f))
Compliance with legal and regulatory obligations	As required	Legal obligation (Art. 7, II)	Legal obligation (Art. 6(1)(c))
Partner Portal management	Partner data, opportunities	Performance of contract (Art. 7, V)	Performance of contract (Art. 6(1)(b))

For data subjects in the EEA and the United Kingdom, when the legal obligation indicated above arises only from Brazilian law (for example, the Marco Civil da Internet or tax legislation), the GDPR / UK GDPR legal basis is Guvik's legitimate interest in complying with the law to which it is subject (Art. 6(1)(f)); legal obligation (Art. 6(1)(c)) applies when the obligation arises from the law of the European Union, of a Member State or of the United Kingdom.

We do not process sensitive categories of data (Art. 11 of the LGPD / Art. 9 of the GDPR and the UK GDPR) as a normal part of the product. If, exceptionally, such processing becomes necessary, we will seek a specific legal basis (e.g., explicit consent) before proceeding.

5. Use of AI and language model providers

The platform's intelligence is provided by **third-party language models** (LLMs). With the Guvik key, models are accessed through **OpenRouter**, configured to use only providers that do not use the data to train models and do not keep it, except when the provider requires **limited retention for safety and abuse monitoring** (currently Google models and some open models). Conversation history stays in the data subject's Guvik account, for the periods in Section 9.

Enterprise customers may use **their own key (BYOK)**; personal plans do not allow it. With their own key, content goes to the provider chosen by the customer, data retention and use follow the policies and settings of the customer's account with that provider, and that provider is outside Guvik's chain of subprocessors.

The platform keeps a **human in the loop**: the AI agents assist in analyzing and carrying out tasks, but critical decisions (for example, transports and changes in an SAP production environment) remain under the customer's control. AI-generated output may contain inaccuracies ("hallucinations") and must be reviewed by a qualified professional before operational use.

6. Who we share personal data with

We share personal data only when necessary to provide the service, to comply with a legal obligation, or on the basis of legitimate interest or consent, with the following categories of recipients:

- **Subprocessors/technology vendors** — LLM/AI providers (through OpenRouter), hosting, authentication, transactional email, web search (Brave Search, for queries triggered by the platform) and optional integrations (e.g., Microsoft Teams). The current list is in the **List of Subprocessors**, published together with the **Data Processing Agreement (DPA)**.
- **Payment institution** — in Brazil, **Asaas** processes charges, subscriptions and refunds for the personal plans and receives the data needed for that. Outside Brazil, the payment method, the currency, the taxes and, if any, the reseller or "merchant of record" are shown in the purchase summary and receive the data needed for billing; if a reseller is the seller of record, its processing of payment data follows its own privacy policy.
- **Service providers** acting on Guvik's behalf (e.g., support, invoicing, accounting), under contractual confidentiality and security obligations.
- **Public authorities** when required by law, court order or regulatory request (e.g., ANPD, tax authorities).
- **Third parties in corporate transactions** (merger, acquisition, reorganization), with the protections in this policy continuing to apply.

Guvik **does not sell** personal data and does not share it for third-party advertising purposes.

7. International transfers

Guvik is headquartered in Brazil. The platform is hosted by **Vultr** (The Constant Company, LLC) in the **United States (New Jersey)**, and AI models are accessed through **OpenRouter** (United States), which routes the content to model providers (for example, Anthropic, OpenAI and Google), which may process it in the United States or in other countries. The other infrastructure providers (authentication, transactional email, web search and optional integrations) are also mostly based in the US, as shown in the **List of Subprocessors**. As a result, personal data may be transferred internationally, for example:

- from Brazil to the United States and other countries where the providers operate;
- from the data subject's country (including the EEA, the United Kingdom or the United States) to Brazil, where Guvik is headquartered and operates the service, and from there to the United States and other countries where the providers operate.

We adopt safeguards compatible with the LGPD (Art. 33), the GDPR and the UK GDPR (Chapter V), including, as applicable: the **standard contractual clauses approved by the ANPD** (Resolution CD/ANPD No. 19/2024), the European Commission's Standard Contractual Clauses (SCCs), an assessment of the adequacy of the destination country, and contractual security and confidentiality requirements imposed on subprocessors. Contractual details of these safeguards are in the **Data Processing Agreement (DPA)**.

For data of data subjects in the **EEA and the United Kingdom**:

- **Adequacy of Brazil:** the European Commission has recognised that Brazil ensures an adequate level of protection (Commission Implementing Decision (EU) 2026/179). Transfers of personal data of data subjects in the EEA to Guvik in Brazil are based on that decision. The United Kingdom does not recognise Brazil as adequate; for personal data of data subjects in the United Kingdom, the safeguards below apply.
- **Standard clauses:** transfers to countries without an adequacy decision, including to providers in the United States, follow the **Standard Contractual Clauses (SCCs)** approved by the European Commission and, for UK data, the **UK Addendum to the SCCs** or the **International Data Transfer Agreement** (IDTA) issued by the Information Commissioner's Office (ICO), together with the contractual security and confidentiality requirements described above.
- **Copy of the safeguards:** data subjects may request information about the safeguards applied to a transfer, and a copy of them, through the Data Protection Officer (DPO) channel (Section 15).

8. Cookies and similar technologies

Today, the `guvik.ai` website and the platform use only essential cookies and similar technologies: session and authentication, security and user preferences, such as language. We do not use usage analytics or advertising cookies. You can manage cookies in your browser settings; blocking essential cookies may prevent sign-in and other features.

If we start using non-essential cookies, we will update this Policy before doing so and, where required by law (e.g., the GDPR and the ePrivacy Directive in the EEA; the UK GDPR and the Privacy and Electronic Communications Regulations — PECR in the United Kingdom), we will ask for your prior consent through a specific banner.

9. Data retention

We keep personal data for as long as necessary for the purposes described in this policy, as follows:

Category	Retention period
Account data and usage content of the personal plan (conversations, files, memory, connections)	While the account is active and for **90 days** after it is closed or suspended; before deletion, the data subject is notified by email and may export their data
Usage content and SAP metadata of enterprise customers	According to the contractual period agreed with the customer (controller); see the DPA

Category	Retention period
SAP credentials	In memory only, for up to 12 hours; if saved in the vault, until removed or until the connection is deleted
Access logs	**6 months**, under the Marco Civil da Internet (Art. 15)
Acceptances and declarations	**5 years** after the end of the relationship with the data subject, for evidence and defense of rights
Tax and payment data	**5 years**, under tax legislation
Access disputes	**5 years** after they are closed
Telemetry and technical logs	Period defined in a technical retention policy, for security and auditing purposes
Business data/leads	Until consent is withdrawn or the business relationship ends
Partner data	For the duration of the partnership, plus the legal retention period

At the end of the applicable period, data is deleted, anonymized or retained only when required by a legal or regulatory obligation or for the regular exercise of rights. Deleting the personal account does not delete access logs, acceptances and declarations or tax data, which follow their own periods above.

10. Information security

We adopt technical and organizational measures to protect personal data against unauthorized access, loss, alteration or destruction, including isolation of SAP environments per customer ("tenant"), authentication via Firebase (JWT), the principle of least privilege in permissions, usage audit trails and protection of SAP credentials: by default they are kept in memory only, and the optional vault stores them encrypted. Additional details are in Guvik's **Security Policy**.

11. Data subject rights

We recognize and facilitate the exercise of the rights provided for in the LGPD, the GDPR, the UK GDPR, the CCPA/CPRA and, when applicable, other US state privacy laws. The table below compares the main rights:

Right	LGPD (Art. 18)	GDPR / UK GDPR (Arts. 15-22)	CCPA/CPRA (California)
Confirmation of and access to data	Yes	Yes (right of access)	Yes (right to know)
Correction of incomplete/inaccurate data	Yes	Yes (rectification)	Yes (correction)

Right	LGPD (Art. 18)	GDPR / UK GDPR (Arts. 15-22)	CCPA/CPRA (California)
Deletion/anonymization	Yes	Yes (erasure, "right to be forgotten")	Yes (deletion)
Restriction of processing	Yes (blocking)	Yes (Art. 18)	Not expressly provided
Portability	Yes	Yes	Partial (through the right to know)
Objection to processing	Yes	Yes	Yes (opt-out of sale/sharing)
Withdrawal of consent	Yes	Yes	Yes
Information about sharing with third parties	Yes	Yes	Yes
Review of automated decisions	Yes	Yes	Not expressly provided
Non-discrimination for exercising rights	Implied	Implied	Yes (express)
Complaint to an authority	Yes (ANPD)	Yes (local supervisory authority; see Section 13)	As provided by state law

Personal account holders can, through the platform itself, **download a copy of their data** and **request deletion of the account**. The other rights can be exercised through the channel indicated in Section 15. We may request additional information to verify your identity before fulfilling the request, and we will respond within the applicable legal deadlines (as a rule, up to 15 days under the LGPD, Art. 19, and one month under the GDPR and the UK GDPR, extendable where permitted). California consumers may consult the **CCPA/CPRA Privacy Notice** for specific details on how to exercise their rights; residents of other US states, see Section 16.3.

12. Minors' data

Our products and website are not directed to persons under 18, and we do not knowingly collect personal data of children or adolescents. Sign-up on the platform requires the data subject to declare that they are at least 18 years old. If we identify that a minor's data was collected without a proper legal basis or the consent of their parents or guardians, we will take steps to delete it.

13. Data Protection Officer (DPO), representatives and supervisory authorities

Guvik has a **Data Protection Officer (DPO)** (in Portuguese, *Encarregado*) responsible for handling data subject requests and communicating with the ANPD and other data protection authorities. Contact: **dpo@guvik.com.br**. Data subjects who believe their rights have not been properly addressed may file a complaint with the **Autoridade Nacional de Proteção de Dados (ANPD)**, without prejudice to other administrative or judicial remedies.

Representative in the EEA and the United Kingdom. Under Article 27 of the GDPR and Article 27 of the UK GDPR, Guvik will designate a representative when the law requires it and will disclose their details in this Policy. Once designated, the representative may be contacted, in addition to Guvik, on any matter relating to the processing of personal data of data subjects in those territories.

Local supervisory authority. Data subjects in the EEA may file a complaint with the data protection supervisory authority of the Member State of their habitual residence, place of work or place of the alleged infringement (Art. 77 of the GDPR). Data subjects in the United Kingdom may file a complaint with the **Information Commissioner's Office (ICO)**. This right does not depend on a prior complaint to Guvik and does not exclude other administrative or judicial remedies.

14. Changes to this policy

We may update this Privacy Policy from time to time to reflect changes in the product, in the law or in our practices. The current version is always the one published at `guvik.ai`, showing the date of update and version number. Material changes will be communicated by reasonable means (e.g., an in-product notice or email) and, when required, will ask for new acceptance at the next access.

15. Contact

For questions, requests concerning personal data or the exercise of rights, please contact:

- Privacy: **privacidade@guvik.com.br**
- Data Protection Officer (DPO): **dpo@guvik.com.br**
- Representative in the EEA and the United Kingdom (Art. 27 of the GDPR and of the UK GDPR): to be designated when the law requires it
- Security: **seguranca@guvik.com.br**
- Legal/commercial: **contato@guvik.com.br**
- Support: **suporte@guvik.com.br**

The current version of this Privacy Policy is the one published at `guvik.ai`.

16. Rules by region

Sections 1 to 15 apply to all data subjects. This section summarizes the rules specific to each region; in case of doubt, the mandatory data protection rules applicable to the data subject prevail.

16.1 Brazil

The LGPD is the primary regime, under ANPD supervision. The rights under Art. 18 of the LGPD are, as a rule, fulfilled within 15 days (Art. 19). International transfers follow Art. 33 of the LGPD, as described in Section 7. Payments for the personal plans are processed by Asaas.

16.2 European Economic Area and United Kingdom

For data subjects in the EEA, the GDPR applies; in the United Kingdom, the UK GDPR and the Data Protection Act 2018. Guvik acts as controller of the data indicated in Section 3 and as processor of the data processed on behalf of the customer, under the DPA. Data subjects have the rights of access, rectification, erasure, restriction of processing, portability, objection (including to direct marketing, at any time) and withdrawal of consent, without affecting the lawfulness of prior processing, and the right not to be subject to a decision based solely on automated processing that produces legal or similarly significant effects (Arts. 15 to 22). Responses are given within one month, extendable as provided by law. Transfers to Brazil and the United States follow Section 7, non-essential cookies require prior consent (Section 8), and the representative and the supervisory authorities are in Section 13. Further details are in the **GDPR Compliance** document.

16.3 United States

Platform data is hosted in the United States (New Jersey) and processed by Guvik, which is headquartered in Brazil (Section 7). **California** residents have the rights described in the **CCPA/CPRA Privacy Notice**, which supplements this policy. Residents of other states have the rights provided by their state's privacy law, when applicable, under the terms and limits of that law — as a rule, access, correction, deletion, portability and the right to opt out of the sale of data, targeted advertising and profiling — and, where the state law so provides, may appeal Guvik's response through the same channel (Section 15). Guvik does not sell personal data and does not share it for third-party advertising purposes (Section 6), and does not discriminate against anyone who exercises their rights.

16.4 Other countries

This policy applies in full, with the LGPD as the primary regime, without prejudice to the mandatory data protection rules of the data subject's country of residence, when applicable. Requests may be sent through the channels in Section 15.

17. Language

This policy is published in Portuguese (pt-BR), English (en-US) and Spanish (es-ES), with the same content. In case of discrepancy between the versions, the version in the language the user accepted prevails when consumer protection law so requires; in all other cases, the Portuguese (pt-BR) version prevails.