

Privacy Policy

Version 2, effective as of 15/09/2026. Replaces version 1, of 08/06/2026.

This Privacy Policy explains how RELEVANTI TECNOLOGIA E SERVICOS LTDA, enrolled with the CNPJ under No. 53.178.015/0001-00, with its head office at Alameda Rio Negro, 500, salas 2213 e 2214, Alphaville Centro Industrial e Empresarial, Barueri, SP, CEP 06454-000 (“RELEVANTI”), processes personal data on the RELEVANTI Website and Platform, under Lei nº 13.709/2018 (the Brazilian General Data Protection Law, or “LGPD”).

RELEVANTI’s role changes depending on where the data comes from. So start with this table:

If you are	Relevanti’s role	Who is accountable for decisions about your data
A Website visitor or business contact (demonstration, proposal, content)	Controller	RELEVANTI, under this Policy.
A Platform User, as regards your account data and your Platform usage	Controller	RELEVANTI, under this Policy.
A person whose data was entered into the Platform by a Customer (for example, an employee, candidate, supplier or partner contact)	Processor	The Customer, the company that contracted the Platform. Refer to its privacy policy. RELEVANTI processes such data solely in accordance with the Customer’s instructions.

1. Definitions

1.1. Capitalized terms not defined here have the meaning given to them by RELEVANTI’s General Terms and Conditions of Contract or by the LGPD. For the purposes of this Policy:

- (i) **Customer:** a company that contracts the RELEVANTI Platform.
- (ii) **User:** an individual who accesses the Platform on behalf of a Customer.
- (iii) **Platform:** RELEVANTI’s SaaS solution, including applications, public forms, integrations and AI Agents.
- (iv) **Website:** RELEVANTI’s corporate website and its content pages.
- (v) **Customer Content:** data, documents, messages and records entered into the Platform by the Customer or by its Users.
- (vi) **Personal Data, Sensitive Personal Data, Anonymized Data, Data Subject, Processing, Controller, Processor and Data Protection Officer (Encarregado):** as defined in the LGPD.
- (vii) **Subprocessor:** a third party engaged by RELEVANTI that processes Personal Data on its behalf, such as hosting providers and artificial intelligence model providers.

2. What data we process

2.1. We process the groups of data below, according to how you interact with RELEVANTI:

Data group	How we collect it	Data
Business contact	Demonstration, contact and materials forms on the Website, and conversations with the sales team.	Name, corporate e-mail, company, job title, country, team size, areas of interest, phone number (optional), message, Website language and the page the request originated from.
Website browsing	Automatic collection, as described in Clause 10 (Cookies).	Language preference, pages visited and source of access.

Contracting and billing	Service Order, electronic signature and invoicing.	Name, CPF, job title, phone number and e-mail of the legal representative; finance department e-mail; name and e-mail of the person responsible for implementation; electronic signature records.
User account	Provided by the Customer or by the User at account creation, or received from the Customer's single sign-on (SSO) provider.	Name, corporate e-mail, job title, phone number, photo (optional), permission profile and access credentials.
Access logs	Automatic collection during Platform usage.	IP address, date and time of access, device type, operating system, browser and approximate location derived from the IP address.
Platform usage	Automatic collection during Platform usage.	Features used, settings, audit trail (who did what and when), errors and support interactions.
Customer Content (RELEVANTI as Processor)	Entered, imported or integrated by the Customer and by its Users, including through public forms and connectors.	According to the features the Customer uses: employee data (identification, contact details, job title, position, department, manager, hiring, movements, compensation, performance and development); partner data and their contacts; contracts, assets and custom records; tasks, projects and processes; documents; messages, notes and meetings; and data processed by AI Agents and apps.

2.2. Sensitive Personal Data in Customer Content. The Customer may enter Sensitive Personal Data into the Platform, such as health information in medical certificates and occupational health examinations, or diversity data. In such cases, it is up to the Customer, as Controller, to determine the applicable legal basis under article 11 of the LGPD and to restrict access through the Platform's permissions.

2.3. Data quality. Whoever provides the data is responsible for its accuracy and for keeping it up to date. RELEVANTI does not verify the truthfulness of the information it receives, but will correct or update data when requested to do so by a person entitled to make such a request.

3. What we use the data for and on what legal basis

3.1. When acting as Controller, RELEVANTI processes Personal Data for the purposes below, based on article 7 of the LGPD:

Purpose	Data involved	Legal basis
Responding to requests, scheduling demonstrations and preparing proposals	Business contact	Pre-contractual procedures (item V)
Sending relevant commercial communications to those who have expressed interest, with an opt-out option in every message	Business contact	Legitimate interest (item IX)
Sending newsletters and content to those who have subscribed	Business contact	Consent (item I)
Entering into and managing the contract, billing and issuing invoices	Contracting and billing	Performance of a contract (item V) and legal obligation (item II)
Creating accounts, authenticating Users and providing, maintaining and supporting the Platform	User account, access logs, Platform usage	Legitimate interest (item IX), in the context of the performance of the contract entered into with the Customer (item V)
Protecting the Platform, preventing fraud and investigating security incidents	Access logs, Platform usage	Legitimate interest (item IX)

Retaining access logs required by the Marco Civil da Internet (Lei nº 12.965/2014, the Brazilian Internet Civil Rights Framework)	Access logs	Legal obligation (item II)
Improving the Platform and the Website through aggregated usage analytics	Platform usage, Website browsing	Legitimate interest (item IX)
Exercising and defending rights in judicial, administrative or arbitration proceedings	Those necessary in each case	Regular exercise of rights (item VI)

3.2. **Customer Content.** When acting as Processor, RELEVANTI processes Customer Content solely to provide the contracted services and in accordance with the Customer's instructions, under Clause 9 of the General Terms and Conditions of Contract.

3.3. **Anonymized Data and benchmarks.** As authorized by the Customer in the General Terms and Conditions of Contract, RELEVANTI may anonymize and aggregate data to produce statistics, comparative indicators and market intelligence, including for the benefit of other Customers. Only effectively anonymized data is used, with no reasonable possibility of re-identification, which ceases to be Personal Data under article 12 of the LGPD.

4. AI Agents

4.1. The Platform's AI Agents process Customer Content within the scope and permissions defined by the Customer, and all actions are recorded in the audit trail.

4.2. **Models contracted by RELEVANTI.** Some features, such as the Ask Relevanti assistant, operate with models from providers contracted by RELEVANTI, which act as Subprocessors and may be located outside Brazil, as described in Clause 7. These providers are listed in the list of Subprocessors published on the website.

4.3. **Models and services connected by the Customer.** The Customer may connect its own access credentials for artificial intelligence model providers and third-party services to the Platform. In that case, the provider is contracted directly by the Customer, which decides what data to send and is responsible for assessing the terms of use, the policy on the use of data for model training and any international transfer. Such providers are not RELEVANTI's Subprocessors, and RELEVANTI does not control the processing they carry out.

4.4. RELEVANTI does not use, and does not authorize the providers it contracts to use, Customer Content to train artificial intelligence models.

4.5. Outputs generated by AI Agents must be reviewed by people before they are used as the basis for decisions affecting Data Subjects. The Data Subject may request a review of decisions made solely on the basis of automated processing, under article 20 of the LGPD.

5. Who we share data with

5.1. RELEVANTI does not sell Personal Data. Data may be shared only in the following cases:

- (i) **Processors and Subprocessors** engaged to operate the Website and the Platform, such as cloud hosting and database providers, e-mail delivery, artificial intelligence models, billing and invoice issuance, electronic signature, and customer service and business relationship tools. All of them are contractually required to process the data solely in accordance with RELEVANTI's instructions and with adequate security measures. The up-to-date list is permanently available on RELEVANTI's website.
- (ii) **Other Users of the same Customer**, according to the permission profiles configured by the Customer.
- (iii) **Third-party services connected by the Customer**, such as systems integrated through connectors and artificial intelligence model providers accessed with the Customer's own credentials, as described in Clause 4.3. The processing carried out by such services is also governed by their own privacy policies, over which RELEVANTI has no control.
- (iv) **Public authorities**, to comply with a legal or regulatory obligation or a court order.
- (v) **Advisors** such as law and accounting firms, for the regular exercise of RELEVANTI's rights.

(vi) **Corporate transactions**, such as a merger, acquisition or reorganization, in which case the successor is bound by this Policy and Data Subjects will be informed of any material changes.

6. Storage and security

6.1. Data is stored in cloud infrastructure provided by market-recognized providers, subject to contractual security and confidentiality obligations.

6.2. RELEVANTI adopts technical and administrative measures appropriate to the nature of the data, including profile-based access control, single sign-on (SSO), encryption in transit, an audit trail and backups.

6.3. No system is entirely immune to incidents. Should a security incident occur that may result in relevant risk or damage to Data Subjects, RELEVANTI will notify the ANPD (the Brazilian Data Protection Authority) and the affected Data Subjects under article 48 of the LGPD and the ANPD's regulations. Where the incident involves Customer Content, RELEVANTI will notify the Customer within the period set out in the General Terms and Conditions of Contract.

6.4. Each User is responsible for keeping their credentials confidential and must immediately notify RELEVANTI of any suspected unauthorized access to their account.

7. International transfer

7.1. Some Subprocessors, such as artificial intelligence model providers, may process data outside Brazil. Such transfers follow the cases set out in article 33 of the LGPD and the ANPD's regulations, including through standard contractual clauses, ensuring a level of protection compatible with that required in Brazil.

8. How long we keep data

Data	Retention period
Business contact	For as long as the relationship lasts and for up to 24 months after the last contact.
User account and Platform usage	For as long as the account is active and for up to 6 months after termination of the Customer's contract.
Access logs	6 months, under article 15 of the Marco Civil da Internet.
Contracting and billing	For the periods required by tax and accounting legislation and for the applicable statutes of limitation.
Customer Content	For the term of the contract. After termination, the Customer has 30 days to request an export, after which the data is deleted, in accordance with the General Terms and Conditions of Contract.

8.1. Once these periods end, the data is deleted or anonymized, except in the retention cases set out in article 16 of the LGPD, such as compliance with a legal obligation or the regular exercise of rights.

9. Your rights

9.1. Under article 18 of the LGPD, you may request: (i) confirmation that processing exists; (ii) access to the data; (iii) correction of incomplete, inaccurate or outdated data; (iv) anonymization, blocking or deletion of unnecessary or excessive data, or data processed in breach of the law; (v) portability; (vi) deletion of data processed on the basis of consent; (vii) information about the entities with which we share your data; (viii) information about the possibility of withholding consent and the consequences of doing so; and (ix) withdrawal of consent. You may also request a review of automated decisions (article 20) and file a complaint with the ANPD.

9.2. **How to exercise these rights.** Send your request to the Data Protection Officer (Encarregado) at the e-mail address indicated in Clause 12. We may request additional information to confirm your identity. Confirmation that processing exists, or access to the data, will be provided in simplified format immediately or, in full format, within 15 days, under article 19 of the LGPD.

9.3. **Data entered by a Customer.** If your request involves Customer Content, such as HR data entered by your employer, RELEVANTI will forward the request to the Customer, which is the Controller, and will support it in responding.

9.4. Some deletion requests may prevent continued access to the Platform, and some data may be retained for the legal periods indicated in Clause 8.

10. Cookies and similar technologies

10.1. We use only cookies and similar technologies that are **necessary** for the operation of the Website and the Platform, which ensure authentication, security and preferences such as language. Because they are indispensable, they do not require consent.

10.2. We do not use audience measurement, advertising or third-party tracking cookies. Should we begin to use them, this Policy will be updated and such cookies will only be activated with your consent, which may be changed at any time in the Website's cookie preferences or in your browser settings.

11. Children and adolescents

11.1. The Website and the Platform are intended for companies and are not directed at persons under 18 years of age. Data of adolescents that may be entered by Customers, such as data of young apprentices, forms part of the Customer Content and must be processed by the Customer in the best interest of the Data Subject, under article 14 of the LGPD.

12. Data Protection Officer and contact

12.1. Questions, requests and complaints about this Policy or about the Processing of Personal Data may be sent to RELEVANTI's Data Protection Officer (Encarregado) for the Processing of Personal Data: **Marcelo Aguiar**, at the e-mail address **marcelo@relevanti.ai**.

13. Changes to this Policy

13.1. This Policy may be updated to reflect changes in the services or in the legislation. The version in force is permanently published and available for download on RELEVANTI's website, indicating its effective date, and previous versions remain accessible for consultation, so that you can check the content in force at any time. Material changes to the purposes or legal bases of Processing will be highlighted at the beginning of this Policy for a period of 30 (thirty) days from publication.

14. Language

14.1. This Policy is written in Portuguese. The English and Spanish versions are made available as a courtesy, to aid understanding. In the event of any divergence, doubt or conflict of interpretation between the versions, the Portuguese version shall prevail for all purposes.

Relevanti Tecnologia e Serviços Ltda., CNPJ 53.178.015/0001-00. Alameda Rio Negro, 500, salas 2213 e 2214, Alphaville Centro Industrial e Empresarial, Barueri, SP, CEP 06454-000.