

Trust Center

Privacy Policy

How personal data is processed on the website, at signup and on the platform.

Version · September 4, 2026

SHA-256 of source text 539c6b40f94ee1e3eda6b219027b32086af02d378afd413cb0acaa6d58fd6a18
<https://skyller.ai/en/privacy/2026-09-04>

1. Provider and scope

Skyller is provided by **SKILLS IT SOLUCOES EM TECNOLOGIA LTDA**, trading as **Skills IT**, CNPJ **05.699.856/0001-10**, at Quadra ACSE 1, Rua SE 1, No. 38, suite 10, 2nd floor, Plano Diretor Sul, Palmas, Tocantins, postal code 77020-014, Brazil. Privacy contact: contato@skillsit.com.br.

This is Skyller's single Privacy Policy: it covers website browsing, signup and use of the platform and its features. Skyller acts as controller when it determines its own purposes, such as business relationships, security, billing and account management. It acts as processor when handling personal data under a business customer's instructions; the DPA governs that relationship.

An organization administrator role does not authorize access to other people's private conversations. Shared access requires authorization from the conversation owner. The organization manages users, integrations and sharing according to the applicable permissions. The customer's privacy policy is also relevant to processing under its responsibility.

2. Data and sources

We may receive data directly from individuals, organization administrators and members, identity providers and authorized integrations:

- identification, professional contact details, organization and account information;
- federated identity, permissions, sessions, IP addresses and access events;

- tax and billing details needed for the contract;
- prompts, conversations, outputs, documents, images, audio and settings;
- information retrieved or transmitted by connected tools;
- consumption, failures, performance, technical records and support interactions.

The service is intended for adults in a professional setting, not children. Content about children or sensitive data requires specific necessity, legal grounds and safeguards; feature availability does not itself authorize such processing.

3. Purposes and legal grounds

For processing controlled by Skyller, the legal basis depends on the purpose and applicable law. Accepting this Policy is not blanket consent.

Purpose	Main data	Legal grounds, where applicable
Registration, contracting and support	Identity, contact details, account and requests	Contract performance or pre-contractual steps; legitimate interests in managing relationships with business representatives
Billing and tax obligations	Tax, billing and transaction details	Contract performance; legal or regulatory obligations
Security and abuse prevention	Access, IP addresses, events and technical records	Legitimate interests in protecting the service; legal obligations where applicable
Legal claims	Contractual evidence and relevant records	Establishment, exercise or defense of legal rights
Optional usage and performance metrics	Browsing data, interactions and interface metrics	Category-specific consent under the Cookie Policy
Business communications	Contact details and interaction history	Requested pre-contractual steps, legitimate interests where permitted, or consent where required

Legitimate interests require necessity, proportionality and respect for individual rights. Content processed on a customer's behalf follows its instructions and the legal grounds it must establish. Sensitive data requires a specific legal condition.

4. AI and integrations

Content may be sent to external models and tools to execute a feature. Model selection, configuration, availability and fallback may change the route. See [integrated services](#).

Skyller and the model API providers selected and contracted by Skyller do not use customer inputs — including prompts, messages and documents — or generated outputs to train artificial intelligence models. Content is processed to perform requested features, including generating responses. Operational retention and processing location vary by service, account and feature; information may be requested through the privacy contact. This no-training policy does not alter the conditions of independent services connected and contracted directly by the customer.

Outputs may contain errors. Customers must establish human review and controls for decisions affecting individuals, as required by applicable law.

5. Sharing

Data is processed by providers necessary to deliver the service and the integrations used, within the relevant purposes and permissions. Sharing between users follows applicable choices and authorizations. Processing or disclosure may also occur for legal requirements, protection of rights or a corporate reorganization with appropriate safeguards.

To execute requested features, Skyller automatically processes content and may record inputs and outputs for operation and diagnosis. Support assistance does not grant general authorization to access private conversations. Where necessary to resolve a problem or meet a legal obligation, technical processing of content must be limited to the relevant purpose and comply with the contractual duties of confidentiality and protection.

Skyller does not commercialize customer content or sell personal data as a product. The legal classification of particular operations, including sharing subject to local rights, depends on applicable law; this description does not remove those rights.

6. International processing

Data may be processed in Brazil and other countries according to infrastructure, accounts and routes used. Transfers require valid legal grounds and mechanisms, such as an adequacy decision or applicable contractual clauses where required. Translation or acceptance does not replace that mechanism.

Information about relevant recipients and safeguards may be requested through the privacy contact. Requirements for residence in a specific country or region must be included in the contracted conditions and corresponding service configuration.

7. Retention and deletion

Category	Retention criterion
Account and relationship	Duration of the relationship and time needed for relevant purposes and obligations
Content under customer instructions	Service term, return or deletion instructions and DPA procedures
Billing and contractual evidence	Legal obligations and legal claims for a justified period
Security and support records	Investigation, protection and support needs, limited to relevant scope
Backups and derivatives	Applicable technical cycle and coordinated deletion across covered components

Documents and conversations may produce extracted text, indexes, embeddings, caches and processing records. Deletion accounts for these derivatives. Retention periods depend on category, purpose and applicable obligations; account-specific processing information may be requested through the privacy contact.

Exceptional retention requires justification and restricted access for a period appropriate to its purpose. Account deletion, cancellation and data erasure are different operations. Support explains request scope, handling stages and applicable retention.

8. Cookies, preferences and metrics

The [Cookie Policy](#) applies across browsing, signup and the platform. It explains necessary technologies and optional usage analytics and performance categories, including events that do not depend on cookies.

Optional metrics remain off until you authorize them. You may accept, reject or customize categories and change your decision using footer, signup and account preference controls. In the same browser, a valid choice is shared between `skyller.ai` and its subdomains, without asking again simply because you navigate, change language or sign up.

Depending on the page and feature, metrics may use Skyller's own tools, Vercel Web Analytics, Vercel Speed Insights or Google Analytics when enabled. The Cookie Policy identifies each technology's scope. Hosting pages on Vercel involves web requests and technical data needed for delivery, independently of optional metrics.

Metrics consent is separate from contractual acceptance. Rejecting metrics does not prevent the requested service or disable necessary authentication, security, operational auditing, billing and AI processing.

9. Security and incidents

The architecture uses authentication, authorization and organization-based separation in covered components, alongside operational logging and monitoring. Questions about data protection and specific requirements may be sent to the privacy contact. The DPA sets out security and processing cooperation obligations.

Incidents will be assessed and addressed according to Skyller's role. Where required, communications to customers, authorities and affected individuals will follow legal requirements; initial information may be supplemented during investigation.

10. Rights, languages and changes

Rights and deadlines depend on applicable law, not the page's language. See [Data protection and your rights](#) for access, correction, deletion, objections and other requests. You may complain to the competent authority without giving up other legal remedies.

Material changes will be communicated through appropriate means. Fresh consent will be requested when necessary for processing that relies on it. Portuguese, English and Spanish versions provide the same information while preserving mandatory rights applicable to each person.