

Legal documents

Complete documents from this version, collected in an A4 PDF with defined margins. Download the file or open the PDF to print.

Version · 2026-10-20

1. [Terms of Use](#)
2. [Privacy Policy](#)
3. [Data Processing Agreement \(DPA\)](#)
4. [Subprocessors](#)
5. [Data protection and your rights](#)
6. [Trust Center](#)
7. [Cookie Policy](#)

Terms of Use

Version · 2026-10-20

SHA-256 of source text 2194c9e5facaae5bd880edbe63be09b0b25522427df7c3671ead04885cfee6fc

<https://skyller.ai/en/terms/2026-10-20>

1. Contracting parties and scope

Skyller is provided by **SKILLS IT SOLUCOES EM TECNOLOGIA LTDA**, trading as **Skills IT**, Brazilian corporate taxpayer number (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. In these Terms, “Skyller” means the service or its provider, as the context requires.

These Terms govern the business platform for artificial intelligence, agents, search, documents, integrations, automation and collaboration. You must have legal capacity to contract. Anyone accepting for an organization represents that they have authority to bind it. The service is intended for professional use by adults.

A specific proposal or contract takes precedence for expressly negotiated terms. The DPA takes precedence in conflicts concerning personal data processed on the customer's behalf. The Privacy Policy explains other processing.

2. Accounts and administration

Customers must maintain accurate information, protect credentials and devices, and manage members, permissions and sharing. They must revoke unnecessary access and report suspected misuse to security@skyller.ai.

Administrators manage members, permissions and business environment settings. An administrator role does not authorize access to other people's private conversations. Shared access requires authorization from the conversation owner. Control of an email address or domain does not replace evidence of legal authority. Skyller may request proportionate verification to resolve account disputes or prevent fraud.

Optional usage analytics and performance choices follow the Cookie Policy. Permission is independent of signup and contractual acceptance.

3. Content and intellectual property

Customers retain their rights in submitted materials. They authorize processing, storage, transmission and creation of technical derivatives only as necessary to provide, maintain, protect and support the contracted service and meet applicable obligations.

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. This authorization also does not grant a general license to commercialize content. Processing needed to generate responses and operational retention follow authorized purposes, the Privacy Policy and DPA. Independent services connected and contracted directly by the customer are governed by their own conditions.

As between the parties, customers may use the outputs they receive to the extent permitted by law and applicable rights. Outputs may resemble those received by others, contain third-party material or lack copyright protection. Exclusivity and freedom from third-party rights are not guaranteed.

The platform, its brand and proprietary components remain with their respective owners. Access does not transfer those rights.

4. AI, agents and external actions

AI responses may contain errors, omissions or outdated information. They and their sources must be checked before consequential use. Skyller does not replace qualified professionals or guarantee legal, medical, financial or business outcomes.

Customers must configure permissions and supervision appropriate to agents' actions. Integrations may retrieve, transmit, create, modify or delete information and perform operations in other services. Granting an integration access authorizes operations within the configured scope; not every action requires an additional on-screen confirmation.

Regulated uses, sensitive data and decisions affecting people require legal assessment and appropriate controls. A feature's availability does not certify its suitability for those uses.

5. Acceptable use

You must not use the service to:

- violate laws, privacy, intellectual property or confidentiality duties;

- engage in fraud, exploitation, harassment, unlawful discrimination or illegal surveillance;
- distribute malware, gain unauthorized access or bypass controls and limits;
- conduct intrusive testing without written authorization;
- send spam or deceptively impersonate others;
- automate decisions about people contrary to review requirements or other legal safeguards;
- resell or reproduce the platform beyond what the contract permits.

6. Plans, billing and cancellation

Prices, currency, taxes, billing intervals, allowances, credits and trial conditions are those presented at purchase or in the proposal. Customers must review them before confirming. A free trial is not presumed to convert automatically into a paid plan without the relevant disclosure and authorization.

Payment methods and providers depend on billing country, currency, plan and the conditions presented at purchase or checkout, where the applicable provider will be identified. Not all methods or markets are available. Confirmation, dispute and refund processing times depend on the transaction and applicable rules, without displacing statutory deadlines or rights.

Billing follows the contracted cycle. Commercial changes will be communicated as required by the contract and applicable law. Nonpayment may restrict or suspend features, with notice and an opportunity to resolve the issue where appropriate.

Cancellation may be requested through available account options or support@skyller.ai. Confirmation identifies the effective date; when scheduled for the end of the cycle, the plan remains active until then and does not renew. Usage incurred and amounts validly due remain payable. Mandatory refund, withdrawal and other rights are preserved where applicable.

Where a transaction is subject to the Brazilian Consumer Protection Code and is concluded away from business premises, the seven-day withdrawal right under Article 49 applies, including legally required reimbursement. Whether a business transaction falls within that protection depends on its circumstances.

7. Third parties, availability and support

Models and integrations depend on third parties, their conditions and customer configuration. Routes may change for availability or fallback. No particular provider or model is guaranteed to remain available. See [integrated services](#).

Skyller will provide the service with professional care, take proportionate measures to protect its operation and communicate material disruptions through support channels. Service levels, support windows and any availability credits will be those expressly agreed at purchase. Maintenance and external dependencies may affect access; support will coordinate diagnosis and service recovery.

8. Suspension and termination

Skyller may suspend or terminate access for material breach, nonpayment, legal requirements or security risk. Measures will be proportionate; where urgency permits, reasonable notice and an opportunity to remedy will be given.

Before termination, customers should request return of needed data through available features or support. Deletion, justified retention and backups are governed by the DPA and Privacy Policy. Cancelling a subscription does not immediately delete every record.

9. Liability

Each party is responsible for breaches of its obligations and damage legally attributable to it. Assessment considers causation, the parties' conduct and applicable law. Customer conduct or third-party failures do not remove Skyller's own liability where it exists.

Nothing excludes rights or liabilities that cannot lawfully be excluded by contract.

10. Versions, languages and governing law

Material changes will be published and communicated through appropriate means; express acceptance will be requested where necessary. Publication does not retroactively replace earlier acceptance evidence. Continued use alone does not constitute consent to new data-processing purposes.

Portuguese, English and Spanish present the same contractual basis. If interpretations differ, the [Portuguese version](#) guides interpretation unless a specific agreement or mandatory law provides otherwise. The selected language does not determine residence or applicable law.

Brazilian law governs, subject to mandatory rules of other jurisdictions that actually apply. Disputes will be heard by the legally competent court. Specific conditions for markets or regulated uses may be set out in a supplementary agreement.

Contract contact: contact@skyller.ai. Support: support@skyller.ai. Privacy: privacy@skyller.ai.

Privacy Policy

Version · 2026-10-20

SHA-256 of source text f680677a2e1c55a95eead0c369d41fece03328dac3dd0195200d60df995f0200

<https://skyller.ai/en/privacy/2026-10-20>

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: privacy@skyller.ai. Data protection officer (encarregado under the LGPD): **Adriano Fante**, through the same channel.

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
Marketing and remarketing	Browser and advertising identifiers, pages visited and conversion events	Consent to the Marketing category 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. Google Calendar in Skyller Meetings

Google Calendar integration is optional and only works if you connect your own calendar in Skyller Meetings. With your permission, we read only your events and calendar names, to recognize meetings and fill in the title and participants; we do not change anything in your calendar.

We do not use this data for advertising, we do not sell it, and we do not use it to train artificial intelligence models. Skyller's use of information received from Google APIs will adhere to the [Google API Services User Data Policy](#), including the Limited Use requirements. You can disconnect your calendar at any time in the app settings or in your Google Account.

6. 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.

With permission for the Marketing category, browser and advertising identifiers, pages visited and conversion events may be shared with advertising platforms such as Meta and Google to show ads, run remarketing and measure campaigns. These platforms also process the data under their own policies. Without that permission, this sharing does not occur; permission can be withdrawn at any time in cookie preferences.

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.

7. 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. When authorized under the Marketing category, advertising platforms such as Meta and Google may process the corresponding data outside Brazil, according to their infrastructure.

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.

8. 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

Category	Retention criterion
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.

9. Cookies, preferences and metrics

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

Optional categories 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. With marketing permission, Google advertising features and the Meta Pixel may be used. On public forms of customer companies, the company publishing the form may configure tools such as Google Analytics 4, Plausible and the Meta Pixel, loaded only after permission for the corresponding category; in that case, it is the controller of the data collected by those tools. 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.

Authorizing optional categories is separate from contractual acceptance. Rejecting them does not prevent the requested service or disable necessary authentication, security, operational auditing, billing and AI processing.

10. 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.

11. 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.

Data Processing Agreement (DPA)

Version · 2026-10-20

SHA-256of source text aa79806b6f939ed4604ad69cf921fe68076c04f86465a461e5227ca01bf2d462

<https://skyller.ai/en/dpa/2026-10-20>

1. Parties, roles and subject matter

This Agreement forms part of the contract between the customer and **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, the provider of Skyller.

It applies to personal data Skyller processes as processor on behalf of the customer as controller. If the customer acts as processor for another controller, it must be authorized to engage Skyller as a subprocessor and convey valid instructions.

Skyller's own processing for accounts, billing, security and legal claims follows the [Privacy Policy](#), within the corresponding lawful purposes.

2. Processing description

Element	Scope
Purpose	Provide contracted AI, document, search, collaboration, integration and automation features
Operations	Receipt, storage, organization, retrieval, transmission, inference, creation of derivatives and deletion
Individuals	Users, employees, contractors, customers, suppliers and other people in authorized content
Data	Identification and contact details, message and file content, images, voice, settings and associated records

Element	Scope
Duration	Service term and time necessary for return, deletion or legally required retention

Customers determine content and must minimize data. Sensitive categories or children's data require a specific assessment, legal grounds and appropriate controls. The parties must agree additional requirements needed for regulated uses before the relevant processing.

3. Documented instructions

Skyller will process data only on documented instructions, including the contract, settings and authorized requests, also regarding transfers. If the law requires different processing, it will inform the customer beforehand unless legally prohibited.

Skyller will inform the customer if it considers an instruction inconsistent with applicable law and may suspend the affected workflow pending clarification. Customers are responsible for lawful instructions, notices to individuals and access permissions.

4. Authorized people and security

Skyller will ensure that people authorized to process data are bound by contractual or statutory confidentiality duties and have access appropriate to their role.

Skyller will maintain technical and organizational measures proportionate to risk, considering the nature and context of processing, and review their suitability throughout service delivery. These measures must address access management, confidentiality, integrity, availability and data recovery within the contracted scope. Customers may request control information and evidence to assess suitability for their processing.

Customers manage members, credentials, integrations and sharing and must keep this access consistent with their instructions.

5. Subprocessors and changes

Customers give general authorization for subprocessors necessary for the features used, described in [integrated services](#). Internal software components and services acting as independent controllers are not automatically subprocessors.

Before adding or replacing a subprocessor for covered processing, Skyller will inform the customer through appropriate means, including the registered contact, and provide a reasonable opportunity for a substantiated objection. The public list supplements that communication. Requests and objections should be sent to privacy@skyller.ai.

The parties will seek a viable alternative. While an objection remains unresolved, the affected workflow may remain unavailable; if no solution is found, it may be terminated under the contract, preserving mandatory rights.

Skyller will require protection obligations consistent with this Agreement and remain responsible to the customer for performance of the processing obligations entrusted to subprocessors, to the extent required by applicable law.

6. AI and connected services

Prompts, context, files and outputs may be transmitted to providers needed for execution. Routing and fallback do not authorize purposes incompatible with instructions.

Skyller and the model API providers it selects and contracts do not use customer inputs, including prompts, messages and documents, or generated outputs to train artificial intelligence models. Skyller will maintain this condition when selecting and contracting those providers, including fallback routes. Inference processing and operational retention remain limited to authorized purposes. Retention and location must be compatible with instructions and contracted conditions. Independent services contracted and controlled directly by the customer are governed by their own agreements.

7. Assistance to customers

Taking account of the processing and information available, Skyller will assist customers with individual rights requests, security, impact assessments and consultations with authorities where required.

Requests received directly about customer data will be forwarded to the responsible party where possible; responses will not exceed its instructions unless legally required. The parties may coordinate scope and resources for extraordinary assistance without preventing compliance with legal obligations.

8. Personal data incidents

Skyller will notify the customer without undue delay after becoming aware of an incident involving personal data processed on its behalf. Initial information may be supplemented; completing the entire investigation is not a condition for notification.

Where available, notification will include the event's nature, affected data and individuals, likely consequences, containment measures and a contact point. Skyller will cooperate in investigation and mitigation. The controller assesses communications for which it is responsible and observes applicable deadlines.

9. Return and deletion

On termination, customers may choose return or deletion of covered data through available features or support. Skyller will coordinate the available format, stages and deletion of remaining copies unless retention is required by law.

The procedure covers relevant derivatives, such as extracted text, indexes, embeddings, caches and records containing content. Backups will remain protected until their removal cycle; if restored, deletion instructions must be reapplied.

Skyller will carry out or coordinate deletion of covered data, including with subprocessors, and provide confirmation describing the scope completed and legally justified retention. Steps requiring further processing will be tracked to completion, with updates to the customer. Records Skyller retains as controller will have their own legal basis, defined purpose and restricted access.

10. International transfers

Skyller will adopt a valid mechanism for covered transfers where required by law, considering the parties, destination and workflow. Applicable standard clauses will be incorporated in full into the relevant instrument, together with required information and annexes.

Customers may request information about the workflow and safeguards. Specific territorial restrictions must be agreed and verified before the relevant processing.

11. Evidence and audits

Skyller will make available information needed to demonstrate compliance with this Agreement and allow and contribute to audits by the customer or an authorized auditor. The parties will agree scope, notice and protection of third-party information without frustrating statutory audit rights.

Intrusive testing requires written authorization. Requests from competent authorities and justified urgent cases will be handled under applicable law.

12. Precedence, languages and survival

This DPA takes precedence in conflicts concerning covered processing. Mandatory legal duties remain applicable regardless of language. The Portuguese version guides interpretation of translation differences unless contract or law provides otherwise.

Protection duties survive while covered data remains. Earlier acceptance evidence stays linked to its respective version; publication does not change it retroactively.

Contact: privacy@skyller.ai.

Subprocessors

Version · 2026-10-20

SHA-256 of source text 91f959f4ad66ee6110c22d7ac46124722d83e7ccf2fd3017f3a30adcced08b26

<https://skyller.ai/en/subprocessors/2026-10-20>

1. How to read this list

Skyller is provided by **SKILLS IT SOLUCOES EM TECNOLOGIA LTDA**, trading as **Skills IT**, CNPJ **05.699.856/0001-10**. This page presents services that may participate in data processing, grouped by purpose. The recipients for each operation depend on the features the customer uses.

Use depends on the feature, configuration, model and route, including fallback. For a specific assessment, ask support about the recipients and conditions for your intended processing before enabling it.

2. Services that may process content on a customer's behalf

Integrated service	Purpose	Potential data and conditions of use
Anthropic	AI inference	Prompts, context, supported files and outputs, according to model and route
OpenAI	AI inference	Prompts, context, supported files and outputs, according to model and route
Google	AI inference	Content submitted to the model, according to model and route
xAI	AI inference	Prompts, context and outputs, according to model and route
DeepInfra	Hosting and inference	Prompts, context and outputs, according to model and route

Integrated service	Purpose	Potential data and conditions of use
OpenRouter	Model routing	Prompts, context, parameters and outputs, according to route
DeepSeek	AI inference	Prompts, context and outputs, according to model and route
Z.AI	AI inference	Prompts, context and outputs, according to model and route
Alibaba Cloud / DashScope	AI inference	Prompts, context and outputs, according to model and route
Xiaomi	AI inference	Prompts, context and outputs, according to model and route
Firecrawl	Web reading and extraction	Queries, URLs and returned content when the tool is used
Exa	Semantic web search	Queries, URLs and results when the tool is used
Serper	Web search	Queries and results when the tool is used

Queries and URLs may contain personal data provided by users; publicly accessible content is not necessarily free of rights or restrictions. Additional tools connected by customers depend on their permissions and contracts.

3. Identity, billing and website services

The following services support account management and website operation. Each provider's responsibilities depend on its processing role and applicable contract.

Service	Purpose	Potential data and conditions of use
Google	Social login	Identity, email and authorized attributes when selected
Microsoft	Social or business login	Identity and authorized organizational attributes when selected
Asaas	Billing and payment	Tax, billing and transaction data when used
Cloudflare Turnstile	Abuse protection	Technical browser and challenge data when configured and used
Vercel	Marketing website hosting and delivery	Web requests, IP addresses and technical access data when visiting the website
Vercel Web Analytics	Website access metrics	Technical browsing data on pages with the integration
Vercel Speed Insights	Website performance	Technical loading and browsing metrics on pages with the integration
Google Analytics	Browsing and usage analytics	Browsing data on pages and interfaces where configured, enabled and authorized

Payment providers used depend on billing country, currency and methods available at purchase. Newly used providers will be identified before the relevant processing; availability is not determined by website language.

Preferences under the [Cookie Policy](#) apply across the website, signup and platform. Vercel Web Analytics and Speed Insights operate on Vercel-hosted pages with permission for their respective category. Google Analytics requires configuration and permission. Optional first-party platform usage and performance metrics follow the same categories; records necessary for operation, security and billing have their own purposes.

4. Internal components

PostgreSQL, Redis, Weaviate, Keycloak, Langfuse, LiteLLM, OCR/Docling and local models form part of the architecture operated by Skyller. These software components are presented separately from external providers receiving data.

5. Countries, retention and safeguards

Skyller and the model API providers it selects and contracts do not use customer inputs, including prompts, messages and documents, or generated outputs to train artificial intelligence models. This condition applies to model routes offered by Skyller, including fallback. Location and operational retention vary according to the service, account, endpoint and contract used. Independent tools and services connected and contracted directly by the customer are governed by their own conditions.

The DPA sets out subprocessor selection, contracting and oversight obligations. The Privacy Policy describes processing and the channel for information about recipients, retention and transfer mechanisms.

6. Changes and contact

For DPA-covered processing, Skyller will communicate additions or replacements of subprocessors before use, allowing substantiated objections under the Agreement. Processing will remain limited to authorized purposes and the scope of features used.

Contact: privacy@skyller.ai. The three language versions describe the same scope of services.

Data protection and your rights

Version · 2026-10-20

SHA-256 of source text 0fc5373706beee3d09e4a63e83d1f4f5cc65a710ff9041e91ef6c737295d9e38

<https://skyller.ai/en/data-subject-rights/2026-10-20>

1. Contact for requests

Skyller privacy requests are received by **SKILLS IT SOLUCOES EM TECNOLOGIA LTDA**, trading as **Skills IT**, CNPJ **05.699.856/0001-10**, at privacy@skyller.ai. The data protection officer (encarregado under the LGPD) is **Adriano Fante**, who answers data subjects and the ANPD through that channel.

Address: Quadra ACSE 1, Rua SE 1, No. 38, suite 10, 2nd floor, Plano Diretor Sul, Palmas, Tocantins, postal code 77020-014, Brazil.

Describe your request, the email associated with your account and the relevant organization, if any. Do not send passwords, tokens or complete identity documents without guidance on an appropriate channel. Representatives may provide the relevant authorization.

2. Who is responsible for processing

Skyller responds for processing it performs as controller. When a customer organization determines the purpose of content, it is responsible as controller; Skyller assists as processor and may forward the request to an authorized contact.

Consulting administrators does not authorize disclosure of other people's data. Identity and authority checks must be proportionate to the request. Further information appears in the [Privacy Policy](#) and [DPA](#).

3. Rights you may exercise

Depending on the law and circumstances, you may request:

- confirmation of processing and access to your data;
- correction of inaccurate, incomplete or outdated information;
- information about purposes, recipients and sharing;

- deletion, anonymization or blocking where provided by law;
- portability under applicable legal and technical conditions;
- withdrawal of consent, without invalidating earlier lawful processing;
- objection to or restriction of processing where applicable;
- review and information concerning solely automated decisions affecting your interests, within legal limits;
- reasons for a refusal or inability to fulfill a request and available ways to challenge it.

Professional use and interface language do not remove mandatory rights. European, US or other Latin American rules apply only when their conditions for application are met; one regime is not presumed to govern every user.

4. Deadlines and follow-up

We will record requests, verify identity and scope, and explain the action taken or relevant reasons.

In Brazil, the LGPD provides for confirmation or access immediately in simplified form, or a complete statement within 15 days of the request. This specific deadline is not a single rule for all rights.

Where the European Union GDPR applies, a response is due without undue delay and generally within one month. An extension of up to two further months depends on request complexity or volume, with notice and reasons within the first month. Other regimes have their own requirements and deadlines.

5. Limits and retention

Records subject to legal retention or another valid exception will be kept only within a justified scope and period. The response will identify the relevant grounds and measures taken to protect retained data.

Request handling will cover the relevant data and necessary coordination concerning derivatives, integrations and backups under applicable law. You will receive information about action taken and follow-up on additional steps. To request erasure, state that objective expressly, including when also cancelling a plan.

6. Complaints and official sources

You may contact the competent authority and exercise other legal remedies. In Brazil, consult the ANPD. Where applicable, complaint, appeal and non-discrimination rights for exercising your rights remain available.

Portuguese, English and Spanish versions describe the same procedures; language does not change territorial criteria.

Sources: LGPD, particularly Articles 18–20 and GDPR, particularly Articles 12–22.

Trust Center

Version · 2026-10-20

SHA-256 of source text 76b62edd7984d7f3f5d9b6dd2bb4038c68170331b86a31d9802842fb956ae73a

<https://skyller.ai/en/trust-center/2026-10-20>

1. Our responsibility

Skyller is provided by **SKILLS IT SOLUCOES EM TECNOLOGIA LTDA**, trading as **Skills IT**, CNPJ **05.699.856/0001-10**, with its registered office at Quadra ACSE 1, Rua SE 1, No. 38, suite 10, 2nd floor, Plano Diretor Sul, Palmas, Tocantins, postal code 77020-014, Brazil.

This center brings together the data protection, security and support commitments governing Skyller's customer relationships. The documents below define rights, responsibilities and channels for assessing your organization's requirements.

2. Documents in this version

- Terms of Use: contracting, acceptable use, AI, billing and liability.
- Privacy Policy: data, purposes, sharing and retention.
- Cookie Policy: common privacy choices across website, signup and platform.
- Data Processing Agreement: instructions, subprocessors, assistance and deletion.
- Integrated services: potential recipients according to the workflow used.
- Data protection and your rights: requests, criteria and applicable deadlines.

Each document has an identified version and integrity hash. Skyller will preserve the reference to the text associated with each acceptance, allowing consultation during the contractual relationship and afterwards where needed to exercise legal rights.

3. Protection commitments

Area	Contractual commitment
Access	Restrict processing to authorized people and services, with permissions appropriate to their roles

Area	Contractual commitment
Data protection	Adopt technical and organizational measures proportionate to risk and contracted scope
Confidentiality	Require confidentiality duties for people authorized to process data
Incidents	Notify customers and cooperate in investigation and mitigation under the DPA
Providers	Establish protection obligations, oversee processing and communicate subprocessor changes
Rights and deletion	Provide assistance and coordinate return or deletion under instructions and applicable law

Customers must manage users, credentials and sharing, restrict agent permissions and review consequential actions and outputs. These duties complement, rather than replace, Skyller's obligations.

Skyller and the model API providers it selects and contracts do not use customer inputs — including prompts, messages and documents — or generated outputs to train artificial intelligence models. This commitment covers Skyller model routes, including fallback. Processing needed to respond and operational retention follow the Privacy Policy and DPA. Independent services contracted directly by the customer are governed by their own conditions.

4. Service conditions and specific requirements

Service levels, support hours, data residency and specific retention periods will be defined in expressly contracted conditions. Support will assist in assessing these requirements and identifying the features and providers involved.

For regulated uses or sensitive data processing, the parties must assess purposes, data categories, instructions and additional safeguards before starting the relevant workflow.

Skyller will provide information about measures applicable to processing and cooperate in assessments and audits under the DPA. Return and deletion will cover data within its responsibility and coordination with subprocessors, subject to legal retention and protected backup cycles.

5. International use

Portuguese, English and Spanish versions provide a common contractual basis while preserving mandatory rules applicable to the circumstances. Additional territorial or sector-specific requirements may be addressed in the service's specific conditions.

Each version provides the full content in its language. Contract interpretation rules appear in the Terms and DPA, subject to applicable mandatory law.

6. Privacy, security and support

Send contractual questions to contact@skyller.ai, privacy requests to privacy@skyller.ai, and vulnerability reports or suspected incidents to security@skyller.ai. Describe the context without sending passwords or secrets. The team may verify identity and authorization before sharing restricted information.

Intrusive testing requires prior authorization. Business assessments may request additional information about controls, processing contracts and suitability for their needs through the same channel.

Cookie Policy

Version · 2026-10-20

SHA-256of source text 55b0534dc83c30a24bf2d85612c4d80930613d5f7d90369e1706f80a49aa836f

<https://skyller.ai/en/cookies/2026-10-20>

1. One policy across Skyller

This Policy supplements the [Privacy Policy](#) and covers browsing, signup and use of the Skyller platform. The responsible company is **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. Contact: privacy@skyller.ai.

Privacy choices apply across the service. Technologies used depend on the page and feature: the same choice applies to the authorized category even when a particular tool operates only in part of Skyller.

2. Technologies and categories

We use cookies, local storage, pixels and similar technologies, including measurement events that do not rely on cookies.

Category	Purpose	Your choice
Necessary	Authentication, sessions, security, recording privacy choices and requested preferences such as language and theme	Remain active to provide the requested service
Usage analytics	Browsing and usage statistics, including interactions and signup steps, to understand and improve the experience	Optional; off until authorized
Performance	Interface loading and response-time metrics to assess the experience	Optional; off until authorized

Category	Purpose	Your choice
Marketing	Advertising, remarketing and campaign measurement, including on advertising platforms such as Meta and Google	Optional; off until authorized

The three optional categories may be allowed or rejected separately. Rejecting them does not prevent signup or use of contracted features.

3. Inventory and duration

Technology	Category and purpose	Where used	Duration or condition
skyller_privacy_cons ent	Necessary: records version, analytics, performance and marketing choices and decision date	Browsing, signup and platform	Up to 180 days after the choice is saved
Authentication and session cookies	Necessary: maintain access and protect the session	Flows requiring identification	According to the session lifecycle and security controls
NEXT_LOCALE and theme storage	Necessary for requested preferences	Pages and interfaces offering these choices	Language: up to one year; theme: until changed or storage is cleared
Vercel Web Analytics	Usage analytics: pages, referral sources and technical browsing information	Website pages hosted on Vercel	Runs only with analytics permission
Vercel Speed Insights	Performance: technical loading metrics	Website pages hosted on Vercel	Runs only with performance permission

Technology	Category and purpose	Where used	Duration or condition
Google Analytics, including _ga and _ga_<id>	Usage and browsing analytics	Pages and interfaces where enabled and authorized	Cookies configured for up to 180 days, without automatic renewal on each visit
Google advertising features (consent mode and _gcl_* cookies)	Marketing: advertising, remarketing and campaign conversion measurement	Pages and interfaces where enabled and authorized	Active only with marketing permission; without it, Google receives the signal that advertising use was refused. Cookie duration set by Google, generally up to 90 days; removed when permission is withdrawn
Meta Pixel, including _fbp and _fbx	Marketing: advertising, remarketing and campaign measurement on Meta	Pages, interfaces and forms where enabled and authorized	Loads only with marketing permission; cookie duration set by Meta, generally up to 90 days
Measurement tools configured by customer companies on public forms they publish on Skyller	Google Analytics 4 and Plausible: usage analytics; Meta Pixel: marketing	Public forms of customer companies that enable these tools	Loaded only after permission for the corresponding category; durations set by each tool and by the customer company's configuration
First-party experience events	Usage analytics: interactions, form filling and signup steps; performance: interface response times	Corresponding platform features	Each event requires permission for its category

Google Analytics, Google advertising features and the Meta Pixel require configuration and activation; inclusion in this Policy does not mean collection on every page. First-party events may be processed by Skyller's observability infrastructure, including Langfuse. They are not necessarily sent to Google, Meta or Vercel.

On public forms published by customer companies, the company publishing the form chooses and configures the measurement tools and determines their purposes; it is the controller of the data collected by those tools, and Skyller loads them according to that configuration and only after the person's permission. Questions about that processing should be addressed to the company responsible for the form.

Browser cookie and storage durations differ from processed-data retention periods, described in the Privacy Policy. You may remove local data in browser settings.

4. Accepting, rejecting and changing

The preference panel lets you accept optional categories, reject them or customize each one. Accept and reject options are equally easy to access. In the initial notice, closing the notice or pressing Escape continues with necessary features only and saves that choice where possible. When preferences are reopened, closing without saving preserves the previous choice. Ignoring the notice does not authorize any optional category. Legal document pages can be read before making any choice.

You may reopen preferences using controls in the footer, signup and account preferences. Changes apply to future collection; withdrawing permission does not invalidate earlier processing with a valid basis. Requests about previously processed data follow the privacy contact and individual rights process.

5. Keeping your choice

In the same browser, choices are shared between `skyller.ai` and its subdomains. Browsing, changing language, signing in or completing signup does not require a new choice while the record remains valid for the presented purposes. Authentication cookies remain tied to their respective host; sharing preferences does not share session credentials.

On other domains, choices remain tied to the corresponding host. Another device, browser, private browsing or cleared storage may require a new choice. The notice may also reappear when the record is missing, invalid or expired, or a material change to purposes or scope requires a new decision. An editorial revision alone does not require renewed consent.

Adding the Marketing category in this version is a change of purpose: choices recorded before it are requested again, and the Marketing category stays off until newly authorized.

6. Preferences and service operation

Rejecting optional categories does not disable processing necessary for authentication, security, operational auditing, billing and requested features, including AI responses. It also does not automatically erase previous records. These activities follow their own purposes and legal grounds under the Privacy Policy and DPA.

Cookie choices are independent of accepting the [Terms of Use](#), acknowledging the Privacy Policy and entering into the [DPA](#). Signing up or accepting contractual documents does not authorize optional categories.

7. Rights and contact

Skyller provides these common choices in Portuguese, English and Spanish while preserving applicable legal requirements. For questions, withdrawal or requests concerning your data, use preferences or privacy@skyller.ai.