# Privacy Policy

How personal data is used in Lumez, who is responsible for each use, and the current limits of retention, sharing and rights procedures.

Version: 2026-09-18.1
Last updated: 2026-09-18

## Responsible provider

64.117.651 ARTHUR GOMES DE FREITAS CARDOZO

CNPJ 64.117.651/0001-49

10A RUA DOUTOR MONTEIRO, 864, CASA, CENTRO, ARROIO GRANDE/RS, CEP 96330-000 - Brasil

Official domain: https://lumez.digital-directive.com

Privacy and support: arthurgfcardozo@gmail.com

Initial market: South America

Infrastructure: AWS, Google Cloud, Vercel and infrastructure operated by Digital Directive

Digital Directive is the trade name declared by the owner. Lumez is the product covered by these documents; other products are not automatically included.

## 1. Scope and responsibility

This policy concerns Lumez, offered at lumez.digital-directive.com by the business identified in this document under the trade name Digital Directive. Lumez is not a separate legal entity. The initial market is South America. Other Digital Directive products may use other subdomains of digital-directive.com; sharing that domain does not extend this policy or its processing purposes to those products.

The provider determines the purposes of its own account administration, website enquiries, commercial relationships, support and service security, acting as controller for those activities. A business customer normally determines why its contacts and conversations are processed; the provider processes that operational content on the customer's documented instructions. Roles depend on the actual activity, and a data processing agreement must define the relevant instructions and responsibilities.

As a common protective standard, rights should be facilitated free of charge, with proportionate identity checks, no unnecessary account creation or document demands, and no retaliation. Any permitted fee or refusal requires an individual legal justification and a challenge route. More favourable mandatory local rights remain available; a business-to-business relationship does not exclude personal data rights.

## 2. Data categories and sources

Information may come directly from a user or prospective customer, from the business administering a workspace, from people communicating with that business, or from an enabled integration. Available fields do not mean every customer uses them. The current data model can contain the following categories.

- Account and team data: name, email, profile image, authentication and verification records, role, invitations and workspace membership. Session records can include IP address, browser information and access times.
- Business data: organisation and unit names, registration details, address, time zone, language, settings and authorised integration identifiers.
- Contact and conversation data: names, phone numbers, email addresses, documents, date of birth, notes, tags and custom fields; message content, attachments, location or contact information when sent, delivery and read status, assignments and internal notes.
- Records associated with enabled features: orders, delivery addresses, appointments, automation instructions and execution records. Their presence in the software does not establish that they are included in a particular subscription.
- Website enquiry data: name, email, WhatsApp number, business segment, team size, objective, preferred contact channel and consent choices. Campaign parameters and a reduced referring page address may accompany the enquiry; query strings and fragments are removed from the referrer.

## 3. Purposes and grounds for processing

A legal basis must be linked to a specific purpose and the relationship with the individual. Acceptance of a privacy policy is not blanket consent. The following mapping describes the purposes and grounds to be applied according to the actual processing and the governing law.

- Creating an account and delivering a service requested by an individual may rely on contractual necessity or requested pre-contractual steps. For employees or representatives of a business customer who are not parties to that contract, the appropriate basis must be assessed separately, including proportionate legitimate interests where permitted.
- Authentication, access controls, abuse prevention, troubleshooting and service security may rely on legitimate interests, subject to necessity, proportionality and the rights of individuals. A legal obligation is used only where an applicable rule actually requires the processing.
- Responding to a demonstration enquiry serves the person's request. The current form records permission to contact them about that enquiry separately from optional marketing consent, together with the version and date of those choices.
- Optional marketing must use the basis and communication permissions required in the recipient’s jurisdiction. A person may withdraw consent or object to direct marketing by writing to arthurgfcardozo@gmail.com, indicating Digital Directive - Privacy/Lumez, or by post to the address

identified in this document. For marketing controlled by a business customer, the request may be sent to that business.

- For customer-controlled content, the customer must establish the applicable grounds, provide notices and issue lawful instructions. The provider's access to that content to deliver the contracted service does not give it an independent right to reuse the content for unrelated advertising or other products.

## 4. Recipients, WhatsApp and customer integrations

When a customer enables WhatsApp, messages, recipients, media, delivery information and business asset identifiers pass through the relevant Meta or WhatsApp services. The provider stores operational records needed for the configured functions. Meta or WhatsApp may have their own legal responsibilities and notices; this document does not replace them or promise deletion from their systems.

The infrastructure used for Lumez includes AWS, Google Cloud, Vercel and the provider’s own infrastructure. This identification does not imply that every supplier receives every data category. The subprocessor and transfer register distinguishes this infrastructure from Meta/WhatsApp and customer-selected integrations. Specific services, contracting entities, processing regions and contractual safeguards must be assessed for each actual data flow; no unverified country or contract is attributed to a supplier here.

- Authorised workspace members can access data according to their permissions. Infrastructure, storage, email and support suppliers may receive only the data relevant to their assigned service, under arrangements appropriate to their role.

- An automation may send a JSON payload to a public HTTPS endpoint selected by the customer. The customer must assess that recipient and its instructions; a customer-selected destination is not automatically a supplier appointed by the provider.

- Disclosure to authorities or other third parties must have a valid legal basis and be limited to the relevant request or obligation. This policy does not authorise unrestricted disclosure merely because a request is received.

## 5. Cookies, browser storage and language

The reviewed application uses browser storage for authentication, language preference and continuation of registration. Its current code review did not identify an active advertising pixel or an external audience analytics integration. This is an implementation finding, not a statement about unreviewed hosting services or future integrations.

The browser storage notice details these functions. New optional technologies require an updated inventory and the notices, consent or other controls required by local law before activation. Blocking essential session storage can prevent sign-in; clearing language storage can reset the selected language.

- Authentication is configured with sessions lasting up to 14 days, a five-minute encrypted session cache, a ten-minute two-factor step and, when selected, a trusted-device period of up to 30 days. Individual sessions may end earlier.
- The lumez_locale cookie stores the selected language for up to one year. Without a saved choice, the application considers browser language preferences and then an available country header from the hosting layer; otherwise it uses English. This flow does not request precise GPS location.
- The lumez:pending-onboarding local storage entry contains the company name and team size entered during registration. It is removed when onboarding is completed or the stored record cannot be parsed; no automatic time-based expiry was identified.
- Where local table persistence is active, lumez:grid:{workspace}:{user}:{screen} stores sorting, search text, filters, column choices, density and pagination. Search text and filters may contain personal data. Later choices can overwrite the record and resetting the view can remove it; this does not automatically erase a view saved on the server.

## 6. Sensitive information, children and automated features

Free-text messages, notes and attachments can contain information that the service did not specifically request, including sensitive data. Customers should restrict collection to what their activity requires and establish the specific legal basis, protections and instructions needed for sensitive data or information about children. The current product is a business tool and is not presented as a child-facing service. The reviewed implementation does not provide an age-verification system or parental-consent controls.

The reviewed AI playground uses a local simulation, and external AI runtimes are not enabled. There is therefore no basis in this implementation for naming a particular AI model provider as a current recipient. Rule-based automations can execute configured actions; customers must assess their effects and provide appropriate human review. Before introducing external AI, profiling or decisions with legal or similarly significant effects, the actual data flows, legal requirements and review procedures must be assessed and the documents updated.

## 7. Security and incident handling

Implemented controls include workspace access permissions and database isolation, server-side protection of Meta credentials with authenticated encryption, checks on webhook signatures, request limits and removal of recognised secrets from certain error records. Authentication supports email verification and two-factor authentication. These measures describe specific controls and do not amount to a certification or a guarantee against every security incident.

The effectiveness and coverage of encryption, hosting and backup protections depend on the configurations and services actually used; this policy does not assert encryption of all stored information or a fixed availability or incident-notification service level. Applicable legal notification duties remain relevant. The responsible controller must assess incidents, document decisions and notify affected persons or authorities when the governing rules require it, with processor assistance where applicable.

## 8. Retention and disposal

Retention depends on purpose, the customer's authorised settings, applicable obligations and the actual category of data. The current implementation does not support a statement that all personal data disappears after a single period. The following limits must be considered when handling a request.

- A daily workspace routine uses a default period of 90 days, subject to the configured entitlement. It removes eligible media, clears message content and provider payloads, webhook payloads and audit details, and anonymises qualifying inactive contact fields.
- That routine does not cover every contact identity, internal note, related order or appointment field, automation payload or other associated record. Those categories require a documented retention decision and complementary action when relevant to a request. Completion of the routine is not proof of comprehensive deletion.
- Demonstration enquiries have a 90-day expiry in the database, renewed when a repeated enquiry updates the record. A worker deletes expired records. Notification emails and copies held elsewhere are not removed by that database routine.
- Generated export files become eligible for removal 30 days after completion. Removal is asynchronous; the current implementation does not establish an exact expiry instant for every copy or download.
- A recorded legal hold can suspend the workspace purge. Any continued preservation must be justified, limited and reviewed. This policy does not state a verified uniform retention period for production backups or promise immediate removal from every backup. Relevant backup copies must be considered when assessing retention and deletion, including access restrictions and the effect of any restoration.

## 9. International processing and transfers

The initial focus on South America does not mean that all processing takes place there. AWS, Google Cloud, Vercel, the provider’s own infrastructure, WhatsApp and customer-selected integrations can involve different parties and locations. The actual configuration determines each flow; no exclusive storage country or unverified processing region is stated here.

Before each relevant international flow is activated, its parties, countries, roles and applicable transfer rules must be identified. A valid adequacy decision may cover a particular flow; otherwise an available lawful safeguard or other permitted mechanism must be assessed. An EU mechanism does not automatically satisfy Brazilian or UK requirements, and onward transfers need their own assessment. Signing or publishing this policy does not itself create standard contractual clauses or validate a transfer.

## 10. Rights under Brazilian law

Where the LGPD applies, individuals may exercise the rights relevant to their circumstances, including confirmation and access, correction, information about sharing, and the remedies described below. Identity and authority must be checked proportionately. The data rights and deletion document explains the existing functions and their limitations.

- Request anonymisation, blocking or deletion of unnecessary, excessive or unlawfully processed data, and deletion of data processed on consent where applicable, subject to lawful preservation grounds.
- Withdraw consent and obtain information about the possibility and consequences of refusing it; request portability under the applicable regulatory conditions; object to processing in the cases provided by law.
- Request review of decisions made solely through automated processing that affect the person's interests and the information required by law about the relevant criteria and procedures.
- Address the business customer for content it controls, or the provider for its own activities, and use the competent authority's complaint procedures where applicable. A complete confirmation or access response and other rights may have different statutory deadlines; the technical queue's target date does not replace them.

## 11. EEA and United Kingdom

The GDPR and UK data protection rules apply according to their territorial and material scope, including relevant establishment, targeted offering or monitoring. The mere availability of translated pages does not establish that every rule applies to every activity. Where applicable, the responsible controller must provide the required notice and lawful basis, and the parties must implement the processor arrangements and other safeguards their activities require.

Subject to applicable conditions, rights include access, rectification, erasure, restriction, portability, objection and withdrawal of consent without affecting earlier lawful processing. Individuals can complain to the competent supervisory authority. Requirements for representatives, a data protection officer or impact assessments depend on the actual activity; this policy does not itself appoint those persons or establish that an assessment has been completed.

- Objection to direct marketing must be respected, including related profiling where covered by law.
- Where rules on solely automated decisions with legal or similarly significant effects apply, the required protections and intervention or review routes must be available.
- The responsible party must observe the applicable response periods and any lawful extension procedure. The current export and deletion functions do not, by themselves, implement every right or every notification requirement.

## 12. California, contact arrangements and updates

California requirements must be evaluated by the activity, legal role and statutory thresholds. If the CCPA applies, relevant rights can include knowing and accessing information, correction, deletion, opting out of sale, and opting out of sharing for cross-context behavioural advertising as defined by the CCPA, limiting certain uses of sensitive information and protection against unlawful discrimination for exercising rights. Customer contracts may also impose service-provider or contractor duties.

Identifying the infrastructure suppliers does not establish the legal classification of every data flow as sale, sharing or use of sensitive information. This policy makes no blanket no-sale claim and does not assert that an automated opt-out or Global Privacy Control mechanism is implemented. Any activity covered by those rules must respect the applicable rights and provide the required notices and controls; requests can be directed to the provider through the contact route below.

For the provider’s own processing, send rights requests or requests for reconsideration to arthurgfcardozo@gmail.com, indicating Digital Directive - Privacy/Lumez, or by post to the address identified in this document. The authenticated export and deletion controls are additional routes for authorised users; a person need not create an account solely to exercise rights. For customer-controlled conversations, contact the business you interacted with. The official domain for consulting this policy and its material updates is lumez.digital-directive.com. Mandatory local rights that are more favourable, including those applicable in South American countries, prevail; neither the geographic focus nor the available translations establishes universal compliance.