Lumez Data Processing Agreement

Agreement governing personal data processed by the Lumez provider on a customer's instructions, as incorporated into the service contract and supplemented by the customer-specific processing, security, subprocessor and transfer annexes.

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. Parties and contractual incorporation

This Data Processing Agreement, or DPA, concerns the provider identified in this document, operating under the trade name Digital Directive, and the customer identified in the service contract. Its subject is the processing of personal data through Lumez, available at lumez.digital-directive.com, on the customer's behalf. It forms part of the parties' contract when validly incorporated into that relationship.

Privacy and support contact: arthurgfcardozo@gmail.com. The parties must identify their legal entities, contacts and roles and document valid acceptance. Customer-specific annexes form part of the agreement and must specify the actual processing, security measures, authorized subprocessors and applicable transfer arrangements. Required information must be completed and verified before the corresponding processing starts; publication alone does not establish technical implementation or replace those annexes.

2. Roles and applicable data protection law

For operations governed by this DPA, the customer acts as controller and the provider as processor, unless the completed processing annex establishes a lawful processor-to-subprocessor relationship. In that case, the customer must hold the necessary authority and pass on its controller's applicable instructions. Roles depend on actual activities, not only the label used in a contract.

Each party must comply with the data protection law applicable to its role and operations. This can include Brazil's LGPD, the EU or UK GDPR, or the California CCPA as amended by the CPRA where their requirements for application are met. Processing by the provider for its own independently determined purposes must be identified separately and cannot be silently included in customer instructions.

3. Documented instructions and purpose restrictions

The provider must process covered data only on documented, lawful instructions and only for the agreed service purposes, including for transfers. The contract, completed annexes and authorized configurations may record instructions. A material change in purpose or scope requires a recorded agreement; broad technical access does not authorize unrelated use.

The provider must inform the customer immediately if, in its opinion, an instruction infringes applicable data protection law, seek clarification and refrain from carrying out the unlawful instruction. Where law requires processing beyond instructions, the provider must identify the legal requirement and notify the customer before processing unless that law prohibits notification.

Where the provider acts as a CCPA service provider or contractor, it must not sell or share covered personal information, retain, use or disclose it outside the specified purposes or direct business relationship, or combine it with other data except as expressly permitted by applicable law. It must provide the required level of protection, notify inability to comply and enable the customer's lawful steps to monitor, stop and remedy unauthorized use.

4. Required processing annex

The parties must complete an annex describing the actual processing before the corresponding operations start. The categories below identify matters to assess; they do not authorize every category, establish a universal retention period or assert that a particular integration is active in production.

- Subject, nature and purposes: the contracted contact and conversation functions, storage, organization, access, transmission, export, deletion and any expressly authorized automation or AI processing.
- Data categories: relevant identifiers, contact details, messages and attachments, interaction metadata and any contracted order or scheduling data. Sensitive data, children's data and other restricted categories require explicit assessment and safeguards before inclusion.
- Data subjects: the customer's users, staff, representatives, leads, contacts, customers and other persons whose data is lawfully included in the defined service.

- Duration and retention: the service period, category-specific retention instructions, return or deletion procedure, backup cycle and any specific legal retention. Also identify the customer's rights and obligations and the authorized instruction and incident contacts.

5. Customer responsibilities and cooperative review

The customer must establish lawful purposes and grounds, provide required notices and obtain authorizations where required, define proportionate access and retention, and submit instructions consistent with applicable law and the rights of data subjects. It must evaluate whether the contracted service is appropriate for the types of data and activities it intends to process.

The provider must supply the information reasonably needed for that assessment and raise identified material limitations. The customer is not required to assume the provider's own legal duties. Neither party may treat a general assurance from the other as a substitute for resolving a known unlawful or unsafe processing arrangement.

6. Confidentiality and security annex

The provider must restrict access to authorized personnel who need the data for the service and are bound by confidentiality or an appropriate statutory duty. It must implement and maintain technical and organizational measures appropriate to the nature, context and risk of the agreed processing. The security annex must identify measures actually implemented, their scope and the responsible roles.

The security annex must be verified before the corresponding processing starts and reviewed when material risks or processing change. The provider must not materially reduce agreed protection without addressing the risk and fulfilling applicable notice and agreement requirements. Each listed control must accurately describe its implementation and scope.

- Access management, least privilege, authentication, credential protection and removal of unnecessary access.
- Protection of data in transit and storage, separation of customer environments and secure handling of secrets, as appropriate to the risk.
- Logging, vulnerability correction, change control, incident detection and personnel awareness.
- Backup protection, restoration, resilience, secure disposal and periodic assessment of the effectiveness of the measures.

7. Subprocessors and changes to the list

The provider may engage a subprocessor only under the customer's prior written authorization in the form required by applicable law. Lumez infrastructure includes AWS, Google Cloud, Vercel and the provider's own infrastructure. The annex must identify the legal entities, contracted functions, processing locations and transfer arrangements actually involved in each operation. The provider must impose equivalent data protection duties by contract and remains responsible for its subprocessor's performance as required by law.

If general authorization is chosen, the agreed operational channel must provide advance notice of intended additions or replacements and a meaningful opportunity to object on data protection grounds before the affected processing starts. The parties must record the notice and objection process in the annex, examine alternatives and resolve the objection. Unresolved lawful objections must not be treated as automatic authorization; any suspension or termination must preserve the customer's mandatory rights and data return options.

8. International transfers

The transfer annex must map the exporting and receiving legal entities, processing countries, remote access and onward transfers. For each restricted flow, the parties must identify a valid mechanism and any required assessment or supplementary measures. An adequacy decision applies only within its actual territorial and material scope; a decision under one legal system does not automatically satisfy another.

Where official standard clauses are required, the correct instrument, module, parties and annexes must be completed and validly incorporated without rewriting or contradicting mandatory text. EU clauses, the UK IDTA or Addendum, and ANPD clauses are distinct instruments. This DPA does not reproduce, execute or replace them, and a link or blank annex is not a completed transfer arrangement.

9. Rights requests and regulatory assistance

Taking account of the processing and information available, the provider must assist the customer with access, correction, deletion, restriction, portability, objection and other applicable rights through appropriate technical and organizational measures. It must promptly forward requests relating to covered data to the designated customer contact and respond directly only when authorized or legally required.

Assistance must enable compliance with applicable legal deadlines, including where existing export or deletion tools do not cover all relevant data. The parties must maintain a working escalation and completion process for covered processing. The provider must also assist with security obligations, impact assessments, prior consultations and regulatory inquiries as required, without disclosing unrelated customers' data.

10. Personal data incidents

The provider must notify the designated customer contact without undue delay after becoming aware of a personal data breach affecting covered data and meet any shorter applicable legal requirement. It must take appropriate steps to contain, investigate, mitigate and remedy the incident, preserve relevant evidence and cooperate with the customer's assessment and required notifications.

The notice must provide the information then available on the nature of the incident, affected data and persons, likely consequences, measures taken or proposed and a contact for follow-up. Missing information must be supplied progressively without delaying the initial notice. The controller's notification duties do not excuse delay by the processor; the provider must not make admissions or communications on the customer's behalf without authority, except where law requires them.

11. Information, verification and audits

The provider must make available the information necessary to demonstrate compliance with this DPA and applicable processor duties and allow and contribute to audits, including inspections by the customer or an authorized auditor. Relevant existing evidence may support the review but cannot replace a legally required audit or conceal a material gap.

The parties may coordinate scope, timing and confidentiality to protect security and other customers' information, without making review ineffective or preventing urgent action or lawful authority access. Identified deficiencies must be investigated and corrected with documented follow-up. Statements about certifications, completed audits or compliance must be supported by applicable, verifiable evidence.

12. Return, deletion and necessary retention

At the end of the relevant processing service, the provider must, at the customer's choice, return or delete covered personal data and delete existing copies unless applicable law requires retention. The annex must define the practical method, export scope, completion steps and backup treatment. The provider must give an accurate completion record identifying any lawful retention, its basis and duration or determining criteria.

Retention cannot be justified solely by technical convenience. Data that must remain must be isolated, protected and used only for the required purpose until deletion is lawful. The parties must validate a defined backup deletion cycle and controls against reintroducing deleted data. Limited automated tools require complementary assistance; workspace deletion, account deletion and deletion of copies held by independent recipients are distinct operations.

13. Meta, AI and customer-selected destinations

The role of Meta, WhatsApp and each other integration must be determined from the actual data flow and applicable contract. A recipient independently selected by the customer, such as an automation webhook destination, is not automatically a subprocessor engaged by the provider. The annex must identify the relevant recipient, instructions and responsibility without transferring the provider's own duties to the customer.

Production AI processing requires prior documentation of the actual provider, purpose, transmitted data, retention, access and transfer mechanism where applicable. Covered data must not be used to train a general-purpose model or for the provider's unrelated purposes under this DPA. Simulations do not establish a production supplier relationship; any additional processing requires a separate lawful assessment, appropriate notice and valid instructions or agreement.

14. Priority, changes and continuing duties

For covered processing, this DPA prevails over conflicting general service provisions, while mandatory law and validly incorporated transfer instruments prevail to the extent required. It does not reduce data subjects' rights, regulatory powers or remedies that cannot be limited by contract. No commercial liability provision may defeat a protection that applicable law makes mandatory.

Changes must be recorded, communicated and validly agreed where required. The parties must review the annexes when processing materially changes and stop any affected operation that lacks a lawful basis or required safeguard until resolved. Confidentiality, security, assistance and deletion duties continue for data still held after termination. The customer-specific annexes and acceptance record remain essential to a complete agreement.