Data rights, export and deletion

How to request access, correction, export or deletion from Lumez, using the available contact routes and understanding the scope of its current functions.

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. Identify the responsible party

For messages or customer records held by a business using Lumez, start with that business: it normally determines the purpose of the processing and can identify the relevant workspace. The provider assists it as appropriate to its role. For a Lumez account, a demonstration enquiry or the provider's own relationship with you, the provider identified in this document is the relevant point of contact.

The common protective standard is free facilitation of rights, proportionate identity checks and no retaliation for making a request. A fee or refusal may be considered only where applicable law permits an exception, with a specific explanation and an available challenge route. A business-to-business service does not remove the rights of the individuals whose data it processes.

- A workspace is the business's shared environment; deleting it is different from deleting one contact or a personal account.
- Being a contact of a business does not require you to create a Lumez account solely to exercise your rights.
- For the provider’s own processing or assistance with a request, write to arthurgfcardozo@gmail.com, indicating Digital Directive - Privacy/Lumez, or send correspondence to the postal address identified

in this document. Authorised users may also use the authenticated functions described below. The official Lumez domain is lumez.digital-directive.com.

2. What to include

Describe the result you want, such as access, correction, an export, objection, restriction, consent withdrawal or deletion. Give enough context to locate the records without sending unnecessary information about yourself or other people. A request does not need a particular legal formula to be considered.

- Identify the business or workspace involved and, if relevant, the approximate dates and the contact address or phone number used in the interaction.
- Explain whether the request concerns one contact, selected information, your own account or an entire workspace. A person requesting their own data should not receive another person's information merely because it appears in the same record.
- Provide a secure way to receive a reply. An authorised representative may act for you, subject to a proportionate check of authority.
- Do not send passwords, access tokens, app secrets, full payment details or identity documents unless a specific, necessary verification step has been explained through a secure channel.

3. Verification and access permissions

Requests involving disclosure or destructive changes require checks proportionate to the risk. Where possible, the existing authenticated session or a known contact channel should be used before asking for additional documents. Any further information should be limited to resolving a specific doubt about identity or authority, with the reason explained and protected handling arranged.

The current application requires an authenticated workspace member with the relevant permission to export data or request contact deletion. Only the authenticated owner may initiate deletion of the whole workspace. These controls protect other users’ data; they do not justify rejecting a person’s statutory request solely because the person is not an administrator. Use the provider’s email or postal contact for requests outside those controls; identity and scope must be assessed without demanding unnecessary account creation.

4. Use the current export function

An authorised user can sign in, confirm the active workspace, open the Privacy page at /privacy and use its export panel to request an export. The request list can then be refreshed; when processing has completed successfully, the authenticated JSON download is available. Request registration alone does not mean the file is ready.

The current export is a structured snapshot of the selected contact scope or workspace contact records and their associated conversations. It can assist an access or portability request, but it is not automatically a complete response to every right or a universal migration package.

- The implemented JSON includes contacts, channel identities, conversations, messages, orders and appointments within the applicable scope.
- Binary attachments, internal notes, all account records and every other associated category are not automatically included. Additional retrieval, explanation and protection of third-party information may be necessary.
- Export files become eligible for asynchronous removal 30 days after completion. Store any downloaded copy securely and delete it when it is no longer needed; the application cannot erase copies you download to another system.

5. Delete or correct a contact's information

A person whose information is held in a customer's workspace should ask that business to locate and review the relevant records. The current service supports an authorised contact deletion request, but this document does not assert a public self-service form for an unauthenticated contact. Correction of a record and withdrawal of marketing consent should be addressed to the responsible business without requiring deletion of the entire workspace.

The implemented contact deletion removes associated media, internal notes, contact tags and channel identities, clears message content and anonymises specified contact fields. It does not comprehensively remove all related order or appointment fields, webhook records, automation payloads or other associated copies. Those remaining categories require a specific assessment and complementary action; a successful automated contact task must not be represented as proof that all personal data was erased.

6. Delete an entire workspace

The workspace owner can sign in, verify that the correct workspace is active and open /data-deletion. The first click opens a confirmation step; the request is submitted only after the second, explicit confirmation. Export any needed records beforehand, subject to your authority and lawful retention duties. Deletion affects the shared business environment and is not an appropriate substitute for a request concerning one person.

Once processed successfully, the workspace deletion routine removes its operational records, integration credentials and configuration, business organisation links and private stored objects within its scope. It retains a minimal structural record and completion evidence so the action can be accounted for. Review the actual request status and outcome rather than treating a confirmation click as completion.

- An existing preservation measure can suspend processing. The basis, affected scope and further handling must be reviewed; a hold is not a general licence to retain everything indefinitely.
- The global personal login is not deleted merely because a workspace is removed, since that account may belong to other workspaces. Removing a workspace also does not cancel an external Meta account or erase recipients' WhatsApp copies.

- Do not assume a submitted deletion can be reversed. Where cancellation is still available before processing, it is subject to the request status and the owner's permissions; completed removal is not a guaranteed recovery point.

7. Personal accounts and website enquiries

Deletion of a personal account, withdrawal of a demonstration enquiry, correction of its details and marketing choices concern different records from a workspace deletion. The current public workspace buttons do not provide a complete account-erasure or lead-rights service. They should not be used to imply that these requests have been fully carried out.

Send these requests to arthurgfcardozo@gmail.com, indicating Digital Directive - Privacy/Lumez, or to the postal address identified in this document. The provider must assess the relevant account, enquiry, notification emails and other copies, explain any lawful preservation and communicate the result. Additional action is necessary when the automated workspace functions do not cover the request; receiving a request does not itself mean deletion has been completed.

8. Requests received from Meta

The application includes a callback for deletion requests sent by Meta. It verifies the signed request and its association with the relevant configuration, then supplies a confirmation code and a status address. An invalid or unmatched request is not authority to remove an unrelated workspace or another person's information.

The implemented Meta-related handling addresses the matched actor and connection data in its scope, including disconnection and removal of associated credentials where applicable. It is not the same as deleting every customer contact or the person's global Lumez account, and it does not erase Meta's own records. The status page reports the outcome of that defined task, including cases with no matching data; broader rights requests need their own assessment.

9. Related copies, backups and retention

A right must be assessed across the relevant processing, not only the record visible on screen. Automatic routines have defined scopes. Where they omit a relevant category, the responsible party needs complementary action and a truthful explanation of what was removed, restricted, anonymised or lawfully retained.

The current technical functions do not establish immediate erasure from every production backup or a verified uniform backup retention period. Relevant backup copies need to be assessed separately, including restricted access, retention expiry and how a valid deletion decision remains effective if a backup is restored. Removing an active record alone must not be treated as proof that every backup copy was erased.

- The daily 90-day default workspace routine is partial and may be changed by authorised settings; it is not a universal retention limit for every personal data category.

- Deleting an expired demonstration record from the database does not also remove its notification emails. Downloaded exports, customer-selected integrations and recipients' copies need to be considered separately according to the responsible party's control and legal duties.
- Anonymisation must actually prevent identification under the applicable standard. A retained identifier or linked record may still be personal data; labelling a task as anonymisation does not by itself settle that question.

10. Responses, exceptions and review

The request-handling process must identify the governing rules, explain its decision in clear language and respect the applicable time limits. A technical queue's target date is not a universal legal deadline or a promised operational service level. A need for clarification, lawful extension or justified partial refusal should be explained, with the relevant grounds and available next steps.

These common protections do not reduce more favourable mandatory rights under the LGPD, the GDPR, UK rules, the CCPA or another applicable law. South America is the initial market, and more favourable mandatory rules of the relevant country prevail. Application depends on the actual activity and legal conditions; the geographic focus and available translations do not establish worldwide compliance.

- Requests should be facilitated free of charge and without retaliation. Excessive document demands, unnecessary account creation or loss of unrelated service access should not be used to discourage the exercise of rights.
- Any permitted fee, refusal or preservation exception must be individually justified and limited. The existence of a legal hold or a technical limitation does not remove the duty to assess the request and explain the outcome.
- Where applicable, the response should explain how to request reconsideration, act through an authorised representative or complain to the competent data protection authority. Requests for reconsideration can be sent to arthurgfcardozo@gmail.com or to the identified postal address, indicating the original request and the reason for the challenge.
- Do not send confidential credentials through a rights request. If the current functions cannot achieve the requested result, that limitation must be disclosed and addressed through a real complementary process before the request is treated as completed.