

Prestataires d'Infrastructure et Sous-traitants Ultérieurs

Prestataires déclarés pour Lumez, infrastructure exploitée par Digital Directive et distinctions entre ces relations, les composants logiciels et les intégrations des clients.

Version: 2026-09-18.1

Mis à jour le: 2026-09-18

Prestataire responsable

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

Domaine officiel: <https://lumez.digital-directive.com>

Confidentialité et assistance: arthurgfcardozo@gmail.com

Marché initial: Amérique du Sud

Infrastructure: AWS, Google Cloud, Vercel et infrastructure exploitée par Digital Directive

Digital Directive est le nom commercial déclaré par le titulaire. Lumez est le produit couvert par ces documents ; les autres produits ne sont pas automatiquement inclus.

1. Périmètre et prestataires déclarés

Cet inventaire concerne Lumez, proposé par Digital Directive à l'adresse lumez.digital-directive.com, avec des marchés initiaux en Amérique du Sud. Digital Directive déclare utiliser Amazon Web Services (AWS), Google Cloud et Vercel, ainsi qu'une infrastructure qu'elle exploite elle-même. Les entrées suivantes distinguent ces prestataires des composants logiciels et des destinataires choisis par les clients.

Digital Directive a confirmé les noms des prestataires. Pour chaque entrée, les services précis, les entités juridiques contractantes, la répartition des données, les lieux de traitement et de sauvegarde et les instruments contractuels applicables ne sont pas encore confirmés. Identifier un prestataire ne signifie pas que toutes les catégories de données de Lumez lui sont transmises, que tous ses services sont utilisés ou qu'un accord de traitement particulier a été accepté.

2. Les rôles dépendent du traitement

Lorsque Digital Directive traite les informations d'un espace de travail sur instruction d'un client professionnel, un prestataire engagé par Digital Directive pour réaliser une partie de ce traitement peut être un sous-traitant ultérieur. La même entreprise peut avoir un rôle différent pour une autre activité. L'analyse doit suivre les décisions, instructions et contrats réels, plutôt qu'une qualification générale appliquée à tous les services.

- Les prestataires utilisés pour la gestion propre des comptes, les relations commerciales ou les obligations légales de Digital Directive peuvent être ses sous-traitants ou des responsables de traitement indépendants, selon l'activité. Les informations correspondantes doivent également figurer dans la Politique de confidentialité.
- Un destinataire choisi et engagé directement par le client n'est pas automatiquement un sous-traitant ultérieur de Digital Directive. Les intégrations gérées par le client nécessitent leur propre analyse des responsabilités et instructions.

3. Composants logiciels et environnement local

La configuration locale examinée utilise les composants suivants. Installer ou exécuter un logiciel ne démontre pas, à lui seul, que son éditeur reçoit des données personnelles ou fournit un service hébergé à Lumez. Les composants logiciels et les entreprises engagées pour exploiter leur infrastructure sont des éléments distincts de l'inventaire des traitements.

- PostgreSQL : logiciel de base de données pour les enregistrements de l'application. Sa présence n'identifie pas un prestataire contractuel d'hébergement de la base.
- Redis : logiciel utilisé dans l'infrastructure de traitement et de files d'attente. Sa présence ne prouve pas l'existence d'un contrat de service cloud géré.
- MinIO : stockage local d'objets compatible avec l'interface S3. Cette compatibilité n'identifie pas les services utilisés auprès d'AWS et n'établit pas le pays où les données de production sont stockées.
- Mailpit et Better Auth : respectivement, outil local de test des courriels et bibliothèque d'authentification utilisée par l'application. Ils ne démontrent pas l'existence d'un prestataire d'envoi de courriels en production ni d'un fournisseur externe d'identité hébergée.

4. Prestataires déclarés et infrastructure propre

Les noms suivants sont les prestataires d'infrastructure déclarés par Digital Directive. Le rôle et la portée de l'accès de chacun dépendent du service et du contrat réels. Leur présence ne signifie pas que chacun traite le contenu des messages, les identifiants d'accès ou toutes les autres catégories de données.

- Amazon Web Services (AWS) : prestataire cloud déclaré. Les services AWS utilisés, l'entité juridique contractante, les catégories pertinentes de données et les régions de production ou de sauvegarde ne sont pas encore confirmés dans cet inventaire.

- Google Cloud : prestataire cloud déclaré. Les services utilisés, l'entité juridique contractante, les catégories pertinentes de données et les lieux de traitement ne sont pas encore confirmés dans cet inventaire. Cette entrée n'établit pas l'utilisation de modèles d'IA de Google.
- Vercel : prestataire déclaré utilisé dans l'exploitation de Lumez. Les services précis, l'entité juridique contractante, les catégories pertinentes de données et les lieux de traitement ne sont pas encore confirmés dans cet inventaire.
- Infrastructure propre : exploitée par Digital Directive et ne constituant donc pas un tiers sous-traitant ultérieur distinct. Tout prestataire externe participant à cette infrastructure doit être évalué séparément selon son accès et son rôle réels ; le lieu et le périmètre de l'infrastructure propre ne sont pas confirmés ici.

5. Détails du traitement par service

Pour chaque prestataire, le registre de traitement doit préciser les informations ci-dessous concernant les services effectivement utilisés. Cette cartographie couvre tout hébergement, base de données, stockage, sauvegarde, courriel, surveillance, assistance ou facturation recevant des données personnelles ou pouvant y accéder ; citer une catégorie ne prouve pas qu'un prestataire donné la fournit.

- Entité juridique et nom du service ; partie qui le contracte ; rôle de sous-traitant, de sous-traitant ultérieur ou de responsable indépendant ; et finalités réellement autorisées.
- Catégories pertinentes de données et de personnes concernées ; accès au contenu, aux métadonnées ou aux identifiants ; pays de stockage, de sauvegarde et d'accès par l'assistance ; et modalités de conservation ou de suppression.
- Accord de traitement, engagements de sécurité et mécanisme de transfert applicables ; caractère obligatoire ou lié à une fonctionnalité activée par le client ; et date de vérification de l'entrée.

6. Intégration avec Meta et WhatsApp

Lumez comprend une intégration à WhatsApp Business Platform et aux API Meta. Lorsqu'une connexion réelle est utilisée, le fonctionnement peut impliquer des identifiants d'entreprise et de compte, des numéros de téléphone, des identifiants d'accès au canal, le contenu et les médias des messages, des informations de livraison et des événements webhook, selon les fonctions activées. Une simulation locale ne démontre pas que ces données ont été transmises à Meta.

Meta/WhatsApp est identifié ici comme une intégration. L'entité contractante concernée et son rôle juridique dépendent du modèle réel de connexion et de l'activité de traitement. Il faut identifier dans cette relation l'entité pertinente, les contrats acceptés par Digital Directive et par le client, et les responsabilités par catégorie. Les conditions de messagerie professionnelle et de traitement doivent être examinées ensemble ; une activité de responsable indépendant ne doit pas être présentée comme une sous-traitance ultérieure.

7. Fonctionnalités d'intelligence artificielle

La fonction examinée des agents d'IA permet actuellement une publication uniquement avec son environnement local simulé. Cela n'établit aucune transmission à un fournisseur externe de modèles. L'utilisation déclarée de l'infrastructure Google Cloud ne signifie pas qu'un service d'IA de Google est activé, et les noms de fonctions ou bibliothèques installées ne prouvent pas l'engagement d'un autre fournisseur externe de modèles.

Avant l'activation d'un fournisseur externe d'IA, l'inventaire et l'examen contractuel doivent préciser les données transmises, les finalités, la conservation, l'accès par le personnel, l'utilisation ou non pour l'entraînement, les lieux de traitement et les contrôles du client. Le simulateur actuel ne permet de déduire ni une garantie générale d'absence d'entraînement ni une autorisation d'entraîner des modèles sur les conversations.

8. Destinations configurées par le client

Les automatisations peuvent transmettre des données à un webhook HTTPS choisi par le client. La destination et les informations comprises dans l'action doivent être évaluées avant l'activation de l'automatisation. L'acceptation technique d'une URL ne vérifie pas le contrat, les pratiques de confidentialité ou les garanties de transfert international du destinataire.

Lorsque le client choisit et engage directement cette destination, son exploitant ne devient pas automatiquement un sous-traitant ultérieur de Digital Directive. Les instructions du client et les responsabilités respectives doivent être documentées, notamment les données pouvant être transmises et les moyens d'interrompre l'accès ou les transmissions futures. Si Digital Directive engage elle-même la destination pour fournir son service, cette relation doit être évaluée en vue de son inclusion dans son propre inventaire de prestataires.

9. Pays et transferts internationaux

Le siège d'un prestataire, une marque de logiciel, le domaine officiel ou les marchés initiaux en Amérique du Sud ne déterminent pas où les données personnelles sont traitées. Le stockage, les répliques, les sauvegardes et l'accès à distance par l'assistance doivent être cartographiés séparément. Les régions utilisées par AWS, Google Cloud, Vercel et l'infrastructure propre ne sont pas précisées ici ; cet inventaire n'établit pas d'engagement de résidence exclusive des données.

Pour les transferts soumis à la LGPD brésilienne, le flux réel doit reposer sur un mécanisme juridique applicable et respecter les exigences de transparence. Les clauses contractuelles types de l'ANPD, lorsqu'elles sont utilisées, doivent respecter le texte et les conditions officiels ; ce document ne les reproduit pas et n'affirme pas qu'elles ont déjà été signées.

Lorsque le RGPD ou les règles britanniques s'appliquent, les transferts exigent une analyse distincte au regard de ces règles. Les décisions d'adéquation de 2026 entre le Brésil et l'Union européenne peuvent être pertinentes dans leur champ d'application, mais ne couvrent pas automatiquement les transferts ultérieurs et n'établissent pas une adéquation britannique. Les obligations californiennes, notamment les éventuelles restrictions applicables aux prestataires de services ou contractants, dépendent également

de l'applicabilité de la loi et de la relation réelle. La mise à disposition de traductions ne détermine pas, à elle seule, lequel de ces régimes s'applique.

10. Approbation, modifications et demandes des clients

L'évaluation d'un sous-traitant ultérieur doit porter sur la nécessité et la portée de l'accès, la confidentialité, les mesures de sécurité, l'assistance concernant les droits et incidents, la conservation et la suppression, ainsi que toute nouvelle délégation. Les contrats applicables doivent définir des instructions et responsabilités cohérentes avec le rôle exercé. Cet inventaire ne certifie aucun prestataire, audit achevé ou engagement de niveau de service.

Les ajouts ou remplacements pertinents doivent respecter l'accord de traitement et les exigences légales applicables, notamment les éventuels droits d'autorisation ou d'opposition du client. Le délai précis et le mode de notification doivent être établis dans la relation concernée ; ce document n'affirme pas l'existence d'un mécanisme automatique d'abonnement aux avis.

Les demandes de confidentialité, d'assistance et d'information sur les prestataires peuvent être envoyées à arthurgfcardozo@gmail.com ou à Digital Directive à l'adresse postale indiquée dans ces documents. Identifiez l'espace de travail et le service concernés sans transmettre de jetons d'accès ou de contenu de conversation inutile. Les demandes des personnes concernées suivent la Politique de confidentialité et le document Droits et suppression, y compris les commandes authentifiées existantes. Retirer une intégration ne prouve pas, à lui seul, la suppression de toutes les copies détenues par ses destinataires.