

Politique de confidentialité

Comment les données personnelles sont utilisées dans Lumez, qui répond de chaque usage et quelles sont les limites actuelles de conservation, de communication et d'exercice des droits.

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 responsabilités

Cette politique concerne Lumez, proposé sur lumez.digital-directive.com par le fournisseur identifié dans ce document sous le nom commercial Digital Directive. Lumez n'est pas une personne morale distincte. Le marché initial est l'Amérique du Sud. D'autres produits de Digital Directive peuvent utiliser d'autres sous-domaines de digital-directive.com ; ce domaine partagé n'étend ni cette politique ni ses finalités de traitement à ces produits.

Le fournisseur détermine les finalités de sa propre gestion des comptes, des demandes du site, des relations commerciales, de l'assistance et de la sécurité du service, en qualité de responsable du traitement pour ces activités. Le client professionnel décide normalement pourquoi ses contacts et conversations sont traités ; le fournisseur traite ce contenu opérationnel sur ses instructions documentées. Les rôles dépendent de l'activité réelle et un accord de traitement des données doit définir les instructions et responsabilités pertinentes.

Comme socle commun de protection, les droits doivent être facilités gratuitement, avec vérification proportionnée de l'identité, sans création inutile de compte, exigences documentaires excessives ni représailles. Tous frais ou refus permis nécessitent une justification juridique individuelle et une voie de

contestation. Les droits locaux impératifs plus favorables demeurent applicables ; une relation entre entreprises n'exclut pas les droits sur les données personnelles.

2. Catégories de données et sources

Les informations peuvent provenir directement d'un utilisateur ou prospect, de l'entreprise administrant un espace de travail, des personnes échangeant avec elle ou d'une intégration activée. La présence de champs ne signifie pas que chaque client les utilise. Le modèle actuel peut contenir les catégories suivantes.

- Données de compte et d'équipe : nom, courriel, image de profil, enregistrements d'authentification et de vérification, rôle, invitations et appartenance à l'espace de travail. Les sessions peuvent comprendre adresse IP, informations du navigateur et horaires d'accès.
- Données professionnelles : noms de l'organisation et de ses unités, informations d'immatriculation, adresse, fuseau horaire, langue, paramètres et identifiants des intégrations autorisées.
- Données de contacts et conversations : noms, téléphones, courriels, documents, date de naissance, notes, étiquettes et champs personnalisés ; messages, pièces jointes, localisation ou contacts lorsqu'ils sont envoyés, états de livraison et de lecture, affectations et notes internes.
- Enregistrements associés aux fonctions activées : commandes, adresses de livraison, rendez-vous, instructions d'automatisation et journaux d'exécution. Leur présence dans le logiciel n'établit pas leur inclusion dans un abonnement particulier.
- Données des demandes du site : nom, courriel, WhatsApp, secteur, taille d'équipe, objectif, canal préféré et choix de consentement. Des paramètres de campagne et une adresse réduite de la page d'origine peuvent accompagner la demande ; les paramètres de requête et fragments sont retirés de l'adresse référente.

3. Finalités et bases du traitement

Une base légale doit correspondre à une finalité précise et à la relation avec la personne. Accepter une politique de confidentialité ne constitue pas un consentement général. La correspondance ci-dessous décrit les finalités et bases à appliquer selon le traitement réel et la législation pertinente.

- Créer un compte et fournir un service demandé par une personne peut relever de la nécessité contractuelle ou de mesures précontractuelles demandées. Pour les salariés ou représentants d'un client professionnel qui ne sont pas parties au contrat, une base appropriée doit être évaluée séparément, notamment des intérêts légitimes proportionnés lorsqu'ils sont admis.
- L'authentification, les contrôles d'accès, la prévention des abus, le diagnostic et la sécurité peuvent reposer sur des intérêts légitimes, sous réserve de nécessité, de proportionnalité et des droits des personnes. Une obligation légale n'est invoquée que si une règle applicable exige réellement le traitement.

- Répondre à une demande de démonstration donne suite à la sollicitation de la personne. Le formulaire actuel enregistre l'autorisation de la contacter à ce sujet séparément du consentement facultatif au marketing, avec la version et la date de ces choix.
- Le marketing facultatif doit utiliser la base et les autorisations de communication exigées dans la juridiction du destinataire. La personne peut retirer son consentement ou s'opposer à la prospection en écrivant à arthurgcardozo@gmail.com, en indiquant Digital Directive - Confidentialité/Lumez, ou par courrier à l'adresse identifiée dans ce document. Pour la prospection contrôlée par un client professionnel, la demande peut être adressée à cette entreprise.
- Pour le contenu contrôlé par le client, celui-ci doit établir les bases applicables, informer les personnes et donner des instructions licites. L'accès du fournisseur pour exécuter le service convenu ne lui confère aucun droit indépendant de réutiliser ce contenu pour une publicité étrangère au service ou d'autres produits.

4. Destinataires, WhatsApp et intégrations du client

Lorsque le client active WhatsApp, les messages, destinataires, médias, informations de livraison et identifiants d'actifs professionnels passent par les services concernés de Meta ou WhatsApp. Le fournisseur conserve les enregistrements opérationnels nécessaires aux fonctions configurées. Meta ou WhatsApp peuvent avoir leurs propres responsabilités juridiques et notices ; ce document ne les remplace pas et ne promet pas d'effacement dans leurs systèmes.

L'infrastructure utilisée par Lumez comprend AWS, Google Cloud, Vercel et l'infrastructure propre du fournisseur. Cette identification ne signifie pas que chaque prestataire reçoit toutes les catégories de données. Le registre des sous-traitants ultérieurs et transferts distingue cette infrastructure de Meta/WhatsApp et des intégrations choisies par le client. Les services précis, entités contractantes, régions de traitement et garanties contractuelles doivent être évalués pour chaque flux réel ; aucun pays ou contrat non vérifié n'est attribué ici à un prestataire.

- Les membres autorisés de l'espace accèdent aux données selon leurs permissions. Les fournisseurs d'infrastructure, de stockage, de courriel et d'assistance peuvent recevoir uniquement les données pertinentes pour leur mission, selon des accords adaptés à leur rôle.
- Une automatisation peut envoyer un contenu JSON vers une adresse HTTPS publique choisie par le client. Celui-ci doit évaluer le destinataire et ses instructions ; une destination choisie par le client n'est pas automatiquement un fournisseur engagé par le prestataire de Lumez.
- Une communication à des autorités ou à d'autres tiers doit avoir un fondement juridique valide et se limiter à la demande ou à l'obligation pertinente. Cette politique n'autorise pas une divulgation sans limite au seul motif qu'une demande a été reçue.

5. Cookies, stockage du navigateur et langue

L'application examinée utilise le stockage du navigateur pour l'authentification, la langue et la poursuite de l'inscription. La revue actuelle n'a identifié ni pixel publicitaire actif ni intégration externe de mesure d'audience. Il s'agit d'un constat sur l'implémentation, non d'une affirmation sur des services d'hébergement non examinés ou de futures intégrations.

La notice sur le stockage du navigateur détaille ces fonctions. De nouvelles technologies facultatives nécessitent un inventaire actualisé et les informations, consentements ou autres contrôles requis localement avant activation. Bloquer le stockage essentiel des sessions peut empêcher la connexion ; effacer celui de la langue peut réinitialiser la préférence.

- L'authentification prévoit des sessions de 14 jours maximum, un cache de session chiffré de cinq minutes, une étape de double authentification de dix minutes et, si elle est choisie, une confiance accordée à l'appareil jusqu'à 30 jours. Une session donnée peut se terminer plus tôt.
- Le cookie `lumez_locale` conserve la langue choisie pendant un an maximum. En l'absence de choix enregistré, l'application considère les préférences du navigateur, puis un en-tête de pays disponible dans l'infrastructure ; sinon elle utilise l'anglais. Ce parcours ne demande pas de localisation GPS précise.
- L'entrée `lumez:pending-onboarding` du stockage local contient le nom de l'entreprise et la taille de l'équipe saisis à l'inscription. Elle est supprimée à la fin de l'intégration ou lorsque l'enregistrement stocké ne peut pas être interprété ; aucune expiration automatique fondée sur le temps n'a été identifiée.
- Lorsque la mémorisation locale des tableaux est active, `lumez:grid:{workspace}:{user}:{screen}` conserve tri, recherches, filtres, colonnes, densité et pagination. Recherches et filtres peuvent contenir des données personnelles. De nouveaux choix peuvent remplacer l'enregistrement et réinitialiser la vue peut le supprimer ; cela n'efface pas automatiquement une vue enregistrée sur le serveur.

6. Données sensibles, enfants et fonctions automatisées

Les messages libres, notes et pièces jointes peuvent contenir des informations que le service n'a pas expressément demandées, notamment des données sensibles. Les clients doivent limiter la collecte au nécessaire et établir la base spécifique, les protections et les instructions requises pour les données sensibles ou concernant des enfants. Le produit actuel est un outil professionnel et n'est pas présenté comme un service destiné aux enfants. L'implémentation examinée ne propose ni vérification d'âge ni contrôle du consentement parental.

L'environnement de test d'IA examiné utilise une simulation locale et les moteurs d'IA externes ne sont pas activés. Cette implémentation ne permet donc pas de désigner un fournisseur particulier de modèles comme destinataire actuel. Les automatisations par règles peuvent exécuter des actions configurées ; le client doit en évaluer les effets et prévoir une revue humaine appropriée. Avant d'introduire une IA externe, du profilage ou des décisions produisant des effets juridiques ou

comparables, les flux réels, les exigences légales et les procédures de réexamen doivent être évalués et les documents actualisés.

7. Sécurité et gestion des incidents

Les contrôles mis en œuvre comprennent des permissions par espace et l'isolation en base, la protection des identifiants Meta sur le serveur par chiffrement authentifié, la vérification des signatures de webhooks, des limites de requêtes et le retrait de secrets reconnus de certains journaux d'erreur. L'authentification propose la vérification du courriel et le double facteur. Ces mesures décrivent des contrôles précis et ne constituent ni certification ni garantie contre tout incident de sécurité.

L'efficacité et la couverture du chiffrement, de l'hébergement et de la protection des sauvegardes dépendent des configurations et services réellement utilisés ; cette politique n'affirme pas le chiffrement de toutes les informations stockées et ne fixe pas de niveau de service de disponibilité ou de notification d'incident. Les obligations légales applicables demeurent pertinentes. Le responsable doit évaluer les incidents, documenter ses décisions et informer les personnes ou autorités lorsque les règles l'exigent, avec l'assistance du sous-traitant le cas échéant.

8. Conservation et suppression

La conservation dépend de la finalité, des paramètres autorisés du client, des obligations applicables et de la catégorie réelle de données. L'implémentation actuelle ne permet pas d'affirmer que toutes les données personnelles disparaissent après un délai unique. Les limites suivantes doivent être prises en compte lors du traitement d'une demande.

- Une routine quotidienne de l'espace utilise une durée par défaut de 90 jours, selon la limite configurée. Elle supprime les médias admissibles, efface contenu et charges des messages, charges de webhooks et détails d'audit, et anonymise les champs des contacts inactifs répondant aux critères.
- Cette routine ne couvre pas toute identité de contact, note interne, champ de commande ou rendez-vous associé, charge d'automatisation ou autre enregistrement connexe. Ces catégories nécessitent une décision documentée de conservation et une action complémentaire lorsqu'elles concernent une demande. L'achèvement de la routine ne prouve pas un effacement intégral.
- Les demandes de démonstration expirent après 90 jours dans la base, délai renouvelé lorsqu'une demande répétée actualise l'enregistrement. Un processus supprime les enregistrements expirés. Les courriels de notification et les copies conservées ailleurs ne sont pas supprimés par cette routine.
- Les fichiers d'export deviennent admissibles à la suppression 30 jours après leur achèvement. La suppression est asynchrone ; l'implémentation actuelle ne fixe pas un instant d'expiration exact pour chaque copie ou téléchargement.
- Une mesure de conservation enregistrée peut suspendre la purge de l'espace. Toute conservation supplémentaire doit être justifiée, limitée et réexaminée. Cette politique n'indique pas de durée uniforme vérifiée de conservation des sauvegardes de production et ne promet pas l'effacement immédiat de chaque copie. Les copies pertinentes doivent être prises en compte lors de l'évaluation

de la conservation et de l'effacement, notamment les restrictions d'accès et les effets d'une restauration.

9. Traitement et transferts internationaux

La priorité initiale à l'Amérique du Sud ne signifie pas que tous les traitements y ont lieu. AWS, Google Cloud, Vercel, l'infrastructure propre du fournisseur, WhatsApp et les intégrations choisies par le client peuvent impliquer différentes parties et localisations. La configuration réelle détermine chaque flux ; aucun pays exclusif de stockage ni aucune région de traitement non vérifiée n'est affirmé ici.

Avant l'activation de chaque flux international pertinent, ses parties, pays, rôles et règles de transfert doivent être identifiés. Une décision d'adéquation valide peut couvrir un flux donné ; sinon, une garantie licite disponible ou un autre mécanisme autorisé doit être évalué. Un mécanisme européen ne satisfait pas automatiquement les exigences brésiliennes ou britanniques, et les transferts ultérieurs nécessitent leur propre analyse. Signer ou publier cette politique ne crée pas à lui seul des clauses contractuelles types et ne valide pas un transfert.

10. Droits prévus par la législation brésilienne

Lorsque la LGPD s'applique, les personnes peuvent exercer les droits pertinents à leur situation, notamment confirmation et accès, correction, information sur les communications et mesures ci-dessous. L'identité et le pouvoir de représentation doivent être vérifiés de manière proportionnée. Le document sur les droits et l'effacement explique les fonctions existantes et leurs limites.

- Demander l'anonymisation, le blocage ou l'effacement de données inutiles, excessives ou traitées illicitement, et l'effacement des données traitées sur consentement lorsque cela s'applique, sous réserve des motifs légaux de conservation.
- Retirer son consentement et obtenir des informations sur la possibilité et les conséquences de le refuser ; demander la portabilité dans les conditions réglementaires applicables ; s'opposer au traitement dans les cas prévus par la loi.
- Demander le réexamen de décisions prises exclusivement par traitement automatisé affectant ses intérêts et les informations légalement requises sur les critères et procédures pertinents.
- S'adresser au client professionnel pour le contenu qu'il contrôle ou au fournisseur pour ses activités propres, et utiliser les voies de réclamation de l'autorité compétente lorsque cela s'applique. Une réponse complète de confirmation ou d'accès et les autres droits peuvent avoir des délais légaux différents ; la date cible de la file technique ne les remplace pas.

11. EEE et Royaume-Uni

Le RGPD et les règles britanniques de protection des données s'appliquent selon leur champ territorial et matériel, notamment l'établissement, l'offre ciblée ou le suivi pertinents. La disponibilité de pages traduites ne signifie pas que chaque règle s'applique à chaque activité. Lorsqu'elles s'appliquent, le responsable doit fournir les informations et la base exigées, et les parties doivent mettre en place les accords de sous-traitance et autres garanties requis par leurs activités.

Sous réserve des conditions applicables, les droits comprennent l'accès, la rectification, l'effacement, la limitation, la portabilité, l'opposition et le retrait du consentement sans remettre en cause les traitements antérieurs licites. Les personnes peuvent saisir l'autorité de contrôle compétente. Les exigences concernant des représentants, un délégué à la protection des données ou des analyses d'impact dépendent de l'activité réelle ; cette politique ne désigne pas à elle seule ces personnes et ne prouve pas la réalisation d'une analyse.

- L'opposition à la prospection directe doit être respectée, y compris le profilage associé lorsqu'il est couvert par la loi.
- Lorsque les règles relatives aux décisions exclusivement automatisées produisant des effets juridiques ou comparables s'appliquent, les protections et voies d'intervention ou de réexamen exigées doivent être disponibles.
- La partie responsable doit respecter les délais de réponse applicables et toute procédure de prolongation licite. Les fonctions actuelles d'export et d'effacement ne mettent pas en œuvre, à elles seules, tous les droits ni toutes les obligations d'information.

12. Californie, contacts et modifications

Les exigences californiennes doivent être évaluées selon l'activité, le rôle juridique et les seuils légaux. Si le CCPA s'applique, les droits pertinents peuvent comprendre la connaissance et l'accès aux informations, la correction, l'effacement, le refus de vente et le refus du partage à des fins de publicité comportementale intercontextuelle au sens du CCPA, la limitation de certains usages d'informations sensibles et la protection contre une discrimination illicite liée à l'exercice des droits. Les contrats clients peuvent aussi imposer des obligations de prestataire de services ou de contractant.

Identifier les fournisseurs d'infrastructure ne détermine pas la qualification juridique de chaque flux comme vente, partage ou usage d'informations sensibles. Cette politique ne fait aucune déclaration générale d'absence de vente et n'affirme pas l'existence d'un mécanisme automatisé d'opposition ou de prise en compte de Global Privacy Control. Toute activité couverte par ces règles doit respecter les droits applicables et fournir les notices et contrôles exigés ; les demandes peuvent être adressées au fournisseur par la voie de contact ci-dessous.

Pour les traitements propres du fournisseur, envoyez vos demandes de droits ou de réexamen à arthurgfcardozo@gmail.com en indiquant Digital Directive - Confidentialité/Lumez, ou par courrier à l'adresse identifiée dans ce document. Les contrôles authentifiés d'export et d'effacement sont des voies supplémentaires pour les utilisateurs autorisés ; créer un compte n'est pas nécessaire uniquement pour exercer ses droits. Pour les conversations contrôlées par le client, contactez l'entreprise avec laquelle vous avez échangé. Le domaine officiel de consultation de cette politique et de ses modifications importantes est lumez.digital-directive.com. Les droits locaux impératifs plus favorables prévalent, notamment ceux applicables dans les pays d'Amérique du Sud ; ni la priorité géographique ni les traductions disponibles n'établissent une conformité universelle.