Accord de traitement des données de Lumez

Accord régissant les données personnelles traitées par le fournisseur de Lumez sur instruction d'un client, incorporé au contrat de service et complété par les annexes propres à la relation contractuelle concernant le traitement, la sécurité, les sous-traitants ultérieurs et les transferts.

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. Parties et incorporation contractuelle

Le présent Accord de traitement des données, ou DPA, concerne le fournisseur identifié dans ce document, exerçant sous le nom commercial Digital Directive, et le client identifié dans le contrat de service. Il porte sur le traitement de données personnelles par Lumez, disponible sur lumez.digital-directive.com, pour le compte du client. Il fait partie du contrat des parties lorsqu'il est valablement incorporé à cette relation.

Contact pour la confidentialité et l'assistance : arthurgfcardozo@gmail.com. Les parties doivent identifier leurs entités juridiques, contacts et rôles et documenter une acceptation valable. Les annexes propres à la relation contractuelle font partie de l'accord et doivent préciser le traitement réel, les mesures de sécurité, les sous-traitants ultérieurs autorisés et les mécanismes de transfert applicables. Les informations nécessaires doivent être complétées et vérifiées avant le début du traitement correspondant ; la publication seule ne démontre pas la mise en œuvre technique et ne remplace pas ces annexes.

2. Rôles et droit applicable à la protection des données

Pour les opérations régies par ce DPA, le client agit comme responsable du traitement et le fournisseur comme sous-traitant, sauf si l'annexe complétée établit une relation licite entre sous-traitant et sous-traitant ultérieur. Dans ce cas, le client doit disposer de l'autorisation nécessaire et transmettre les instructions applicables de son responsable du traitement. Les rôles dépendent des activités réelles, et pas seulement de la dénomination contractuelle.

Chaque partie doit respecter le droit de la protection des données applicable à son rôle et à ses opérations. Il peut notamment s'agir de la LGPD brésilienne, du RGPD de l'Union européenne ou du Royaume-Uni, ou du CCPA californien modifié par le CPRA lorsque leurs critères d'application sont remplis. Les traitements du fournisseur pour ses finalités propres, déterminées indépendamment, doivent être identifiés séparément et ne peuvent être inclus silencieusement dans les instructions du client.

3. Instructions documentées et limitation des finalités

Le fournisseur doit traiter les données couvertes uniquement sur instructions documentées et licites, pour les finalités convenues du service, y compris en matière de transferts. Le contrat, les annexes complétées et les configurations autorisées peuvent consigner des instructions. Un changement important de finalité ou de périmètre exige un accord enregistré ; un accès technique étendu n'autorise pas un usage étranger au service.

Le fournisseur doit informer immédiatement le client lorsqu'il estime qu'une instruction enfreint le droit applicable à la protection des données, demander des précisions et s'abstenir d'exécuter l'instruction illicite. Si la loi impose un traitement au-delà des instructions, il doit identifier cette obligation et en informer le client avant le traitement, sauf si cette loi interdit l'information.

Lorsqu'il agit comme prestataire de services ou contractant au sens du CCPA, le fournisseur ne doit ni vendre ni partager les informations personnelles couvertes, ni les conserver, utiliser ou divulguer hors des finalités définies ou de la relation commerciale directe, ni les combiner à d'autres données sauf autorisation expresse du droit applicable. Il doit assurer le niveau de protection requis, signaler son incapacité à respecter ses obligations et permettre les mesures licites du client visant à vérifier, arrêter et corriger les utilisations non autorisées.

4. Annexe de traitement obligatoire

Les parties doivent compléter une annexe décrivant le traitement réel avant le début des opérations correspondantes. Les catégories suivantes désignent des éléments à évaluer ; elles n'autorisent pas toutes les catégories, ne fixent aucune conservation universelle et n'affirment pas qu'une intégration donnée est active en production.

- Objet, nature et finalités : fonctions souscrites de contacts et conversations, stockage, organisation, accès, transmission, exportation, suppression et toute automatisation ou tout traitement par IA expressément autorisé.

- Catégories de données : identifiants pertinents, coordonnées, messages et pièces jointes, métadonnées d'interaction et données de commandes ou de rendez-vous prévues au contrat. Les données sensibles, celles des enfants et les autres catégories restreintes exigent une évaluation explicite et des garanties avant inclusion.
- Personnes concernées : utilisateurs, personnel, représentants, prospects, contacts, clients du cocontractant et autres personnes dont les données sont licitement incluses dans le service défini.
- Durée et conservation : période du service, instructions par catégorie, procédure de restitution ou suppression, cycle des sauvegardes et conservations légales spécifiques. Identifier également les droits et obligations du client et les contacts autorisés pour les instructions et incidents.

5. Responsabilités du client et évaluation conjointe

Le client doit établir des finalités et fondements juridiques licites, fournir les informations requises et obtenir les autorisations nécessaires, définir des accès et durées de conservation proportionnés et donner des instructions compatibles avec le droit applicable et les droits des personnes concernées. Il doit évaluer si le service souscrit convient aux types de données et aux activités qu'il prévoit de traiter.

Le fournisseur doit fournir les informations raisonnablement nécessaires à cette évaluation et signaler les limitations importantes identifiées. Le client n'a pas à assumer les obligations légales propres au fournisseur. Aucune partie ne peut considérer une assurance générale de l'autre comme un substitut à la résolution d'une situation de traitement connue comme illicite ou non sécurisée.

6. Confidentialité et annexe de sécurité

Le fournisseur doit limiter l'accès au personnel autorisé qui a besoin des données pour le service et est soumis à la confidentialité ou à une obligation légale appropriée. Il doit mettre en œuvre et maintenir des mesures techniques et organisationnelles adaptées à la nature, au contexte et aux risques du traitement convenu. L'annexe de sécurité doit identifier les mesures effectivement mises en œuvre, leur portée et les fonctions responsables.

L'annexe de sécurité doit être vérifiée avant le début du traitement correspondant et revue lorsque les risques ou le traitement changent sensiblement. Le fournisseur ne doit pas réduire substantiellement la protection convenue sans traiter le risque et respecter les exigences applicables d'information et d'accord. Chaque contrôle énuméré doit décrire fidèlement sa mise en œuvre et sa portée.

- Gestion des accès, moindre privilège, authentification, protection des identifiants et retrait des accès inutiles.
- Protection des données en transit et stockées, séparation des environnements clients et gestion sécurisée des secrets, selon les risques.
- Journalisation, correction des vulnérabilités, contrôle des changements, détection des incidents et sensibilisation du personnel.
- Protection des sauvegardes, restauration, résilience, destruction sécurisée et évaluation périodique de l'efficacité des mesures.

7. Sous-traitants ultérieurs et modification de la liste

Le fournisseur ne peut faire appel à un sous-traitant ultérieur qu'avec l'autorisation écrite préalable du client, dans la forme requise par le droit applicable. L'infrastructure de Lumez comprend AWS, Google Cloud, Vercel et l'infrastructure propre du fournisseur. L'annexe doit identifier les entités juridiques, fonctions souscrites, lieux de traitement et mécanismes de transfert effectivement impliqués dans chaque opération. Le fournisseur doit imposer contractuellement des obligations équivalentes de protection des données et reste responsable de l'exécution par son sous-traitant ultérieur selon les exigences légales.

Si une autorisation générale est retenue, le canal opérationnel convenu doit informer à l'avance des ajouts ou remplacements envisagés et offrir une possibilité effective d'opposition pour des motifs de protection des données avant le début du traitement concerné. Les parties doivent consigner dans l'annexe la procédure d'information et d'opposition, examiner les solutions alternatives et résoudre l'objection. Une objection licite non résolue ne vaut pas autorisation automatique ; toute suspension ou résiliation doit préserver les droits impératifs du client et ses possibilités de restitution des données.

8. Transferts internationaux

L'annexe de transferts doit identifier les entités exportatrices et destinataires, les pays de traitement, les accès à distance et les transferts ultérieurs. Pour chaque flux soumis à restrictions, les parties doivent identifier un mécanisme valable et les évaluations ou mesures complémentaires requises. Une décision d'adéquation ne s'applique que dans son champ territorial et matériel réel ; une décision d'un système juridique ne satisfait pas automatiquement un autre.

Lorsque des clauses types officielles sont nécessaires, l'instrument, le module, les parties et les annexes appropriés doivent être complétés et valablement incorporés, sans réécrire ni contredire le texte obligatoire. Les clauses de l'Union européenne, l'IDTA ou Addendum britannique et les clauses de l'ANPD sont des instruments distincts. Ce DPA ne les reproduit, ne les conclut et ne les remplace pas ; un lien ou une annexe vide ne constitue pas un mécanisme de transfert complet.

9. Demandes d'exercice des droits et assistance réglementaire

Compte tenu du traitement et des informations disponibles, le fournisseur doit aider le client pour l'accès, la rectification, l'effacement, la limitation, la portabilité, l'opposition et les autres droits applicables, par des mesures techniques et organisationnelles appropriées. Il doit transmettre rapidement les demandes relatives aux données couvertes au contact désigné du client et ne répondre directement que sur autorisation ou obligation légale.

L'assistance doit permettre de respecter les délais légaux applicables, y compris lorsque les outils actuels d'exportation ou de suppression ne couvrent pas toutes les données pertinentes. Les parties doivent maintenir une procédure opérationnelle d'escalade et de réalisation pour le traitement couvert. Le fournisseur doit également contribuer aux obligations de sécurité, analyses d'impact, consultations préalables et demandes des autorités lorsque cela est requis, sans divulguer les données étrangères au dossier d'autres clients.

10. Incidents relatifs aux données personnelles

Le fournisseur doit notifier au contact désigné du client, sans retard injustifié, toute violation de données personnelles couvertes dont il prend connaissance, et respecter toute exigence légale applicable plus courte. Il doit prendre des mesures appropriées pour contenir, examiner, atténuer et corriger l'incident, préserver les preuves pertinentes et coopérer à l'évaluation et aux notifications requises du client.

La notification doit fournir les informations alors disponibles sur la nature de l'incident, les données et personnes touchées, les conséquences probables, les mesures prises ou proposées et un contact de suivi. Les informations manquantes doivent être fournies progressivement, sans retarder la notification initiale. Les obligations de notification du responsable du traitement ne justifient pas un retard du sous-traitant ; le fournisseur ne doit faire aucune reconnaissance ni communication au nom du client sans autorisation, sauf obligation légale.

11. Informations, vérification et audits

Le fournisseur doit mettre à disposition les informations nécessaires pour démontrer le respect de ce DPA et des obligations applicables au sous-traitant, et permettre les audits et y contribuer, y compris les inspections du client ou d'un auditeur autorisé. Les preuves existantes pertinentes peuvent soutenir l'examen, mais ne peuvent remplacer un audit légalement requis ni dissimuler une lacune importante.

Les parties peuvent coordonner la portée, le calendrier et la confidentialité pour protéger la sécurité et les informations d'autres clients, sans rendre l'examen inefficace ni empêcher une action urgente ou l'accès licite des autorités. Les lacunes identifiées doivent être examinées et corrigées avec un suivi documenté. Les affirmations relatives aux certifications, aux audits achevés ou à la conformité doivent être étayées par des preuves pertinentes et vérifiables.

12. Restitution, suppression et conservation nécessaire

À la fin du service de traitement concerné, le fournisseur doit, au choix du client, restituer ou supprimer les données personnelles couvertes et supprimer les copies existantes, sauf conservation exigée par le droit applicable. L'annexe doit définir la méthode pratique, la portée de l'exportation, les étapes d'achèvement et le traitement des sauvegardes. Le fournisseur doit fournir un relevé fidèle de la réalisation, identifiant toute conservation légale, son fondement et sa durée ou ses critères de détermination.

La conservation ne peut être justifiée par la seule commodité technique. Les données devant subsister doivent être isolées, protégées et utilisées uniquement pour la finalité requise jusqu'à ce que leur suppression soit licite. Les parties doivent valider un cycle défini de suppression des sauvegardes et des contrôles empêchant la réintroduction de données supprimées. Les outils automatisés limités nécessitent une assistance complémentaire ; la suppression d'un espace de travail, d'un compte et des copies détenues par des destinataires indépendants sont des opérations distinctes.

13. Meta, IA et destinations choisies par le client

Le rôle de Meta, de WhatsApp et de chaque intégration doit être déterminé selon le flux réel de données et le contrat applicable. Un destinataire choisi indépendamment par le client, tel que la destination d'un webhook d'automatisation, n'est pas automatiquement un sous-traitant ultérieur engagé par le fournisseur. L'annexe doit identifier le destinataire, les instructions et la responsabilité pertinents, sans transférer au client les obligations propres du fournisseur.

Le traitement par IA en production exige une documentation préalable du fournisseur réel, de la finalité, des données transmises, de la conservation, des accès et du mécanisme de transfert applicable. Les données couvertes ne doivent pas servir à entraîner un modèle à usage général ni à des finalités étrangères du fournisseur au titre de ce DPA. Les simulations n'établissent pas une relation avec un fournisseur de production ; tout traitement supplémentaire exige une évaluation licite distincte, une information appropriée et des instructions ou un accord valables.

14. Priorité, modifications et maintien des obligations

Pour le traitement couvert, ce DPA prévaut sur les dispositions générales contradictoires du service, tandis que le droit impératif et les instruments de transfert valablement incorporés prévalent dans la mesure requise. Il ne réduit ni les droits des personnes concernées, ni les pouvoirs des autorités, ni les recours qui ne peuvent être limités par contrat. Aucune disposition commerciale de responsabilité ne peut écarter une protection impérative du droit applicable.

Les modifications doivent être consignées, communiquées et valablement convenues lorsque cela est requis. Les parties doivent revoir les annexes en cas de changement important du traitement et arrêter toute opération concernée dépourvue de fondement juridique ou de garantie requise jusqu'à résolution. Les obligations de confidentialité, de sécurité, d'assistance et de suppression subsistent pour les données conservées après la fin du contrat. Les annexes propres au client et la preuve d'acceptation restent essentielles à un accord complet.