Política de Privacidade

Como os dados pessoais são usados no Lumez, quem responde por cada uso e quais são os limites atuais de retenção, compartilhamento e atendimento de direitos.

Versão: 2026-09-18.1
Atualizado em: 2026-09-18

Fornecedor responsável

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

Domínio oficial: https://lumez.digital-directive.com

Privacidade e suporte: arthurgfcardozo@gmail.com

Atuação inicial: América do Sul

Infraestrutura: AWS, Google Cloud, Vercel e infraestrutura própria da Digital Directive

Digital Directive é o nome comercial informado pelo titular. Lumez é o produto abrangido por estes documentos; outros produtos não estão automaticamente incluídos.

1. Abrangência e responsabilidade

Esta política trata do Lumez, oferecido em lumez.digital-directive.com pelo fornecedor identificado neste documento sob o nome comercial Digital Directive. Lumez não é uma pessoa jurídica separada. O mercado inicial é a América do Sul. Outros produtos da Digital Directive podem utilizar outros subdomínios de digital-directive.com; compartilhar esse domínio não estende esta política nem suas finalidades de tratamento a esses produtos.

O fornecedor determina as finalidades da administração das próprias contas, das solicitações recebidas pelo site, do relacionamento comercial, do suporte e da segurança do serviço, atuando como controlador nessas atividades. O cliente empresarial normalmente decide por que seus contatos e conversas são tratados; o fornecedor trata esse conteúdo operacional segundo instruções documentadas do cliente. Os papéis dependem da atividade efetiva, e um acordo de tratamento de dados deve definir as instruções e responsabilidades pertinentes.

Como padrão comum de proteção, os direitos devem ser facilitados gratuitamente, com verificação proporcional de identidade, sem criação desnecessária de conta, exigência excessiva de documentos ou retaliação. Qualquer cobrança ou recusa permitida exige fundamento jurídico individual e possibilidade de contestação. Permanecem os direitos locais obrigatórios mais favoráveis; uma relação entre empresas não exclui direitos sobre dados pessoais.

2. Categorias de dados e fontes

As informações podem vir diretamente de um usuário ou interessado, da empresa que administra um workspace, das pessoas que se comunicam com essa empresa ou de uma integração habilitada. A existência de campos não significa que todo cliente os utiliza. O modelo atual pode conter as categorias a seguir.

- Dados de conta e equipe: nome, e-mail, imagem de perfil, registros de autenticação e verificação, papel, convites e vínculo com o workspace. Registros de sessão podem incluir endereço IP, informações do navegador e horários de acesso.
- Dados empresariais: nomes da organização e das unidades, dados cadastrais, endereço, fuso horário, idioma, configurações e identificadores de integrações autorizadas.
- Dados de contatos e conversas: nomes, telefones, e-mails, documentos, data de nascimento, notas, etiquetas e campos personalizados; conteúdo de mensagens, anexos, localização ou contatos quando enviados, status de entrega e leitura, responsáveis e notas internas.
- Registros relacionados a recursos habilitados: pedidos, endereços de entrega, agendamentos, instruções de automação e registros de execução. Sua presença no software não comprova inclusão em uma assinatura específica.
- Dados de solicitações pelo site: nome, e-mail, WhatsApp, segmento, tamanho da equipe, objetivo, preferência de contato e escolhas de consentimento. Parâmetros de campanha e o endereço reduzido da página de origem podem acompanhar a solicitação; parâmetros de consulta e fragmentos são removidos do endereço de referência.

3. Finalidades e bases do tratamento

Uma base legal deve estar ligada a uma finalidade específica e à relação com o titular. A aceitação de uma política de privacidade não constitui consentimento genérico. O mapeamento abaixo descreve as finalidades e bases a aplicar conforme o tratamento efetivo e a legislação pertinente.

- Criar uma conta e prestar um serviço solicitado por uma pessoa pode se apoiar na execução contratual ou em procedimentos preliminares solicitados por ela. Para empregados ou representantes do cliente empresarial que não são partes desse contrato, a base adequada deve ser avaliada separadamente, inclusive legítimos interesses proporcionais quando admitidos.
- Autenticação, controle de acesso, prevenção de abuso, diagnóstico de falhas e segurança podem se apoiar em legítimos interesses, observadas necessidade, proporcionalidade e direitos dos titulares. Obrigação legal é utilizada apenas quando uma norma aplicável realmente exige o tratamento.
- Responder a um pedido de demonstração atende à solicitação do interessado. O formulário atual registra a autorização de contato sobre esse pedido separadamente do consentimento opcional de marketing, com versão e data dessas escolhas.
- Marketing opcional deve utilizar a base e as autorizações de comunicação exigidas na jurisdição do destinatário. A pessoa pode revogar consentimento ou se opor ao marketing direto escrevendo para arthurgfcardozo@gmail.com, indicando Digital Directive - Privacidade/Lumez, ou por

correspondência ao endereço identificado neste documento. Para marketing controlado por um cliente empresarial, o pedido pode ser dirigido a essa empresa.

- Para conteúdo controlado pelo cliente, cabe a ele estabelecer as bases aplicáveis, prestar informações e emitir instruções lícitas. O acesso do fornecedor para executar o serviço contratado não lhe confere um direito independente de reutilizar esse conteúdo para publicidade alheia ao serviço ou outros produtos.

4. Destinatários, WhatsApp e integrações do cliente

Quando o cliente habilita o WhatsApp, mensagens, destinatários, mídias, informações de entrega e identificadores de ativos empresariais passam pelos serviços pertinentes da Meta ou do WhatsApp. O fornecedor armazena registros operacionais necessários às funções configuradas. Meta ou WhatsApp podem ter responsabilidades jurídicas e avisos próprios; este documento não os substitui nem promete eliminação nos sistemas desses terceiros.

A infraestrutura utilizada pelo Lumez inclui AWS, Google Cloud, Vercel e infraestrutura própria do fornecedor. Essa identificação não significa que cada fornecedor receba todas as categorias de dados. O registro de suboperadores e transferências distingue essa infraestrutura da Meta/WhatsApp e das integrações escolhidas pelo cliente. Serviços específicos, entidades contratantes, regiões de tratamento e salvaguardas contratuais devem ser analisados para cada fluxo efetivo; não se atribui aqui a um fornecedor país ou contrato não verificado.

- Membros autorizados do workspace acessam dados conforme suas permissões. Fornecedores de infraestrutura, armazenamento, e-mail e suporte podem receber apenas os dados pertinentes ao serviço atribuído, sob instrumentos adequados ao seu papel.
- Uma automação pode enviar um conteúdo JSON a um endereço HTTPS público escolhido pelo cliente. Cabe ao cliente avaliar esse destinatário e suas instruções; um destino escolhido pelo cliente não é automaticamente um fornecedor contratado pelo prestador do Lumez.
- A divulgação a autoridades ou outros terceiros deve ter fundamento jurídico válido e ser limitada ao pedido ou à obrigação pertinente. Esta política não autoriza divulgação irrestrita pelo simples recebimento de uma solicitação.

5. Cookies, armazenamento no navegador e idioma

A aplicação examinada usa armazenamento no navegador para autenticação, preferência de idioma e continuidade do cadastro. A revisão atual do código não identificou pixel publicitário ativo ou integração externa de análise de audiência. Trata-se de uma constatação da implementação, não de uma afirmação sobre serviços de hospedagem não examinados ou futuras integrações.

O aviso de armazenamento no navegador detalha essas funções. Novas tecnologias opcionais exigem inventário atualizado e os avisos, consentimentos ou outros controles requeridos pela legislação local antes da ativação. Bloquear o armazenamento essencial da sessão pode impedir o acesso; limpar o armazenamento de idioma pode redefinir a preferência.

- A autenticação está configurada com sessões de até 14 dias, cache de sessão cifrado de cinco minutos, etapa de dois fatores de dez minutos e, quando selecionada, confiança no dispositivo por até 30 dias. Sessões individuais podem terminar antes.
- O cookie lumez_locale guarda o idioma escolhido por até um ano. Sem escolha salva, a aplicação considera as preferências de idioma do navegador e depois um cabeçalho de país disponível na infraestrutura; caso contrário, utiliza inglês. Esse fluxo não solicita localização GPS precisa.
- A entrada lumez:pending-onboarding no armazenamento local contém o nome da empresa e o tamanho da equipe informados no cadastro. É removida ao concluir o onboarding ou quando não é possível interpretar o registro armazenado; não foi identificada expiração automática por tempo.
- Quando a persistência local de tabelas está ativa, lumez:grid:{workspace}:{user}:{screen} guarda ordenação, texto de busca, filtros, colunas, densidade e paginação. Buscas e filtros podem conter dados pessoais. Novas escolhas podem substituir o registro e redefinir a visualização pode removê-lo; isso não apaga automaticamente uma visualização salva no servidor.

6. Informações sensíveis, crianças e recursos automatizados

Mensagens livres, notas e anexos podem conter informações que o serviço não solicitou especificamente, inclusive dados sensíveis. Os clientes devem limitar a coleta ao necessário para sua atividade e estabelecer a base específica, as proteções e as instruções exigidas para dados sensíveis ou informações sobre crianças. O produto atual é uma ferramenta empresarial e não é apresentado como serviço dirigido a crianças. A implementação examinada não oferece verificação etária nem controles de consentimento parental.

O ambiente de testes de IA examinado utiliza simulação local, e os provedores externos de IA não estão habilitados. Não há, portanto, fundamento nesta implementação para identificar um provedor específico de modelos como destinatário atual. Automações baseadas em regras podem executar ações configuradas; o cliente deve avaliar seus efeitos e disponibilizar revisão humana adequada. Antes de introduzir IA externa, definição de perfis ou decisões com efeitos jurídicos ou igualmente significativos, é necessário avaliar os fluxos reais, as exigências legais e os procedimentos de revisão, atualizando os documentos.

7. Segurança e tratamento de incidentes

Os controles implementados incluem permissões de acesso por workspace e isolamento no banco, proteção de credenciais Meta no servidor com criptografia autenticada, verificação de assinaturas de webhooks, limites de requisições e remoção de segredos reconhecidos de determinados registros de erro. A autenticação oferece verificação de e-mail e dois fatores. Essas medidas descrevem controles específicos e não representam certificação ou garantia contra todo incidente de segurança.

A eficácia e a cobertura de criptografia, hospedagem e proteção de backups dependem das configurações e dos serviços efetivamente utilizados; esta política não afirma criptografia de todas as informações armazenadas nem estabelece nível fixo de serviço para disponibilidade ou comunicação de incidentes. As obrigações legais aplicáveis permanecem relevantes. O controlador responsável deve

avaliar incidentes, documentar decisões e comunicar titulares ou autoridades quando as normas exigirem, com assistência do operador quando cabível.

8. Retenção e descarte

A retenção depende da finalidade, das configurações autorizadas do cliente, das obrigações aplicáveis e da categoria efetiva dos dados. A implementação atual não permite afirmar que todos os dados pessoais desaparecem após um único prazo. Os limites abaixo devem ser considerados no atendimento de uma solicitação.

- Uma rotina diária do workspace utiliza prazo padrão de 90 dias, conforme o limite configurado. Ela remove mídias elegíveis, limpa conteúdo e payloads de mensagens, payloads de webhooks e detalhes de auditoria, e anonimiza campos de contatos inativos que atendam aos critérios.
- Essa rotina não alcança toda identidade de contato, nota interna, campo relacionado de pedido ou agendamento, payload de automação ou outro registro associado. Essas categorias exigem decisão documentada de retenção e ação complementar quando pertinentes ao pedido. A conclusão da rotina não comprova eliminação integral.
- Solicitações de demonstração têm expiração de 90 dias no banco, renovada quando uma solicitação repetida atualiza o registro. Um processo em segundo plano elimina registros vencidos. E-mails de notificação e cópias mantidas em outros locais não são removidos por essa rotina do banco.
- Arquivos de exportação gerados tornam-se elegíveis à remoção 30 dias após a conclusão. A remoção é assíncrona; a implementação atual não estabelece um instante exato de expiração para toda cópia ou download.
- Uma determinação de preservação registrada pode suspender o expurgo do workspace. Qualquer conservação adicional deve ser justificada, limitada e revisada. Esta política não informa prazo uniforme verificado de retenção de backups de produção nem promete remoção imediata de toda cópia de segurança. Cópias pertinentes devem ser consideradas na avaliação de retenção e exclusão, inclusive restrições de acesso e efeitos de eventual restauração.

9. Tratamento e transferências internacionais

O foco inicial na América do Sul não significa que todo tratamento ocorra nessa região. AWS, Google Cloud, Vercel, infraestrutura própria do fornecedor, WhatsApp e integrações escolhidas pelo cliente podem envolver participantes e localidades diferentes. A configuração efetiva determina cada fluxo; não se afirma aqui país exclusivo de armazenamento nem região de tratamento não verificada.

Antes de ativar cada fluxo internacional pertinente, devem ser identificados seus participantes, países, papéis e regras de transferência aplicáveis. Uma decisão válida de adequação pode abranger determinado fluxo; caso contrário, deve ser avaliada uma salvaguarda lícita disponível ou outro mecanismo permitido. Um mecanismo europeu não satisfaz automaticamente as exigências brasileiras ou britânicas, e transferências posteriores exigem avaliação própria. Assinar ou publicar esta política não cria, por si, cláusulas contratuais padrão nem valida uma transferência.

10. Direitos previstos na legislação brasileira

Quando a LGPD se aplica, o titular pode exercer os direitos pertinentes à sua situação, incluindo confirmação e acesso, correção, informação sobre compartilhamento e as medidas descritas a seguir. Identidade e poderes de representação devem ser verificados proporcionalmente. O documento de direitos e exclusão explica as funções existentes e seus limites.

- Solicitar anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados ilicitamente, e eliminação de dados tratados com consentimento quando cabível, observadas as hipóteses legais de conservação.
- Revogar consentimento e obter informação sobre a possibilidade e as consequências de recusá-lo; solicitar portabilidade nas condições regulamentares aplicáveis; opor-se ao tratamento nas hipóteses legais.
- Solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado que afetem seus interesses e as informações exigidas por lei sobre os critérios e procedimentos pertinentes.
- Dirigir-se ao cliente empresarial quanto ao conteúdo que ele controla ou ao fornecedor quanto às atividades próprias, e utilizar os procedimentos de reclamação da autoridade competente quando cabíveis. A resposta completa de confirmação ou acesso e os demais direitos podem ter prazos legais distintos; a data-alvo da fila técnica não os substitui.

11. EEE e Reino Unido

O GDPR e as regras britânicas de proteção de dados se aplicam conforme seus âmbitos territorial e material, inclusive estabelecimento, oferta dirigida ou monitoramento pertinentes. A mera disponibilidade de páginas traduzidas não significa que toda regra incida sobre toda atividade. Quando aplicáveis, o controlador responsável deve fornecer o aviso e a base exigidos, e as partes devem implementar os instrumentos de operador e as demais salvaguardas requeridas por suas atividades.

Sujeitos às condições aplicáveis, os direitos incluem acesso, retificação, apagamento, limitação, portabilidade, oposição e retirada do consentimento sem afetar o tratamento lícito anterior. O titular pode reclamar à autoridade de controle competente. As exigências de representantes, encarregado ou avaliações de impacto dependem da atividade efetiva; esta política não designa essas pessoas por si só nem comprova a conclusão de uma avaliação.

- A oposição ao marketing direto deve ser respeitada, inclusive quanto à definição de perfis relacionada quando abrangida pela lei.
- Quando incidirem regras sobre decisões exclusivamente automatizadas com efeitos jurídicos ou igualmente significativos, devem existir as proteções e as vias de intervenção ou revisão exigidas.
- O responsável deve observar os prazos de resposta aplicáveis e o procedimento de eventual prorrogação lícita. As funções atuais de exportação e exclusão não implementam, por si, todos os direitos ou todas as obrigações de comunicação.

12. Califórnia, canais de contato e alterações

As exigências da Califórnia devem ser avaliadas conforme a atividade, o papel jurídico e os critérios legais de incidência. Se a CCPA se aplicar, os direitos pertinentes podem incluir conhecer e acessar informações, corrigir, eliminar, recusar venda e recusar compartilhamento para publicidade comportamental entre contextos distintos, conforme definido pela CCPA, limitar certos usos de informações sensíveis e proteção contra discriminação ilícita pelo exercício de direitos. Contratos com clientes também podem impor deveres de prestador de serviços ou contratado.

Identificar os fornecedores de infraestrutura não define a classificação jurídica de cada fluxo como venda, compartilhamento ou uso de informações sensíveis. Esta política não faz uma declaração genérica de ausência de venda nem afirma existir mecanismo automatizado de oposição ou de tratamento do Global Privacy Control implementado. Qualquer atividade abrangida por essas regras deve respeitar os direitos aplicáveis e disponibilizar os avisos e controles exigidos; os pedidos podem ser dirigidos ao fornecedor pela via de contato abaixo.

Para os tratamentos próprios do fornecedor, envie pedidos de direitos ou reconsideração para arthurgfcardozo@gmail.com, indicando Digital Directive - Privacidade/Lumez, ou por correspondência ao endereço identificado neste documento. Os controles autenticados de exportação e exclusão são vias adicionais para usuários autorizados; não é necessário criar conta apenas para exercer direitos. Para conversas controladas pelo cliente, contate a empresa com que interagiu. O domínio oficial para consulta desta política e de suas alterações relevantes é lumez.digital-directive.com. Prevalecem os direitos locais obrigatórios mais favoráveis, inclusive os aplicáveis nos países da América do Sul; nem o foco geográfico nem as traduções disponíveis comprovam conformidade universal.