Acordo de Tratamento de Dados do Lumez

Acordo que rege os dados pessoais tratados pelo fornecedor do Lumez sob instruções de um cliente, incorporado ao contrato de serviço e complementado pelos anexos de tratamento, segurança, suboperadores e transferências específicos da contratação.

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. Partes e incorporação contratual

Este Acordo de Tratamento de Dados, ou DPA, abrange o fornecedor identificado neste documento, que atua sob o nome comercial Digital Directive, e o cliente identificado no contrato de serviço. Seu objeto é o tratamento de dados pessoais pelo Lumez, disponível em lumez.digital-directive.com, em nome do cliente. Ele integra o contrato das partes quando validamente incorporado a essa relação.

Contato de privacidade e suporte: arthurgfcardozo@gmail.com. As partes devem identificar suas entidades jurídicas, contatos e papéis e documentar um aceite válido. Os anexos específicos da contratação integram o acordo e devem especificar o tratamento efetivo, as medidas de segurança, os suboperadores autorizados e os mecanismos de transferência aplicáveis. As informações necessárias devem ser preenchidas e verificadas antes do início do tratamento correspondente; a publicação, por si, não comprova implementação técnica nem substitui esses anexos.

2. Papéis e legislação de proteção de dados aplicável

Nas operações regidas por este DPA, o cliente atua como controlador e o fornecedor como operador, salvo se o anexo de tratamento preenchido estabelecer uma relação lícita entre operador e suboperador. Nesse caso, o cliente deve possuir a autorização necessária e transmitir as instruções aplicáveis de seu controlador. Os papéis dependem das atividades efetivas, não apenas do nome usado em contrato.

Cada parte deve observar a legislação de proteção de dados aplicável ao seu papel e às suas operações. Isso pode incluir a LGPD brasileira, o GDPR da União Europeia ou do Reino Unido e a CCPA da Califórnia, alterada pela CPRA, quando preenchidos seus requisitos de incidência. Tratamentos do fornecedor para finalidades próprias, determinadas de forma independente, devem ser identificados separadamente e não podem ser incluídos silenciosamente nas instruções do cliente.

3. Instruções documentadas e limites de finalidade

O fornecedor deve tratar os dados abrangidos apenas sob instruções documentadas e lícitas e para as finalidades acordadas do serviço, inclusive nas transferências. O contrato, os anexos preenchidos e as configurações autorizadas podem registrar instruções. Uma mudança relevante de finalidade ou escopo exige acordo registrado; acesso técnico amplo não autoriza uso alheio ao serviço.

O fornecedor deve informar imediatamente ao cliente quando, em sua avaliação, uma instrução violar a legislação aplicável de proteção de dados, solicitar esclarecimentos e não executar a instrução ilícita. Se a lei exigir tratamento além das instruções, o fornecedor deve identificar a exigência legal e notificar o cliente antes do tratamento, salvo se essa lei proibir a notificação.

Quando atuar como prestador de serviços ou contratado nos termos da CCPA, o fornecedor não deve vender ou compartilhar as informações pessoais abrangidas, conservá-las, utilizá-las ou divulgá-las fora das finalidades especificadas ou da relação comercial direta, nem combiná-las com outros dados, salvo quando expressamente permitido pela lei aplicável. Deve garantir o nível de proteção exigido, notificar a impossibilidade de cumprir suas obrigações e viabilizar medidas lícitas do cliente para verificar, interromper e corrigir usos não autorizados.

4. Anexo obrigatório de tratamento

As partes devem preencher um anexo que descreva o tratamento efetivo antes do início das operações correspondentes. As categorias abaixo indicam pontos a avaliar; não autorizam todas as categorias, não fixam retenção universal nem afirmam que determinada integração está ativa em produção.

- Objeto, natureza e finalidades: funções contratadas de contatos e conversas, armazenamento, organização, acesso, transmissão, exportação, exclusão e automações ou tratamentos por IA expressamente autorizados.
- Categorias de dados: identificadores pertinentes, dados de contato, mensagens e anexos, metadados de interação e dados de pedidos ou agendamentos contratados. Dados sensíveis, dados de crianças e outras categorias restritas exigem avaliação explícita e salvaguardas antes da inclusão.

- Titulares: usuários, pessoal, representantes, leads, contatos, clientes do contratante e outras pessoas cujos dados sejam licitamente incluídos no serviço definido.
- Duração e retenção: período do serviço, instruções de retenção por categoria, procedimento de devolução ou exclusão, ciclo de backups e retenções legais específicas. Identificar também os direitos e deveres do cliente e os contatos autorizados para instruções e incidentes.

5. Responsabilidades do cliente e avaliação conjunta

O cliente deve definir finalidades e bases legais lícitas, fornecer os avisos exigidos e obter autorizações quando necessárias, estabelecer acesso e retenção proporcionais e enviar instruções compatíveis com a lei aplicável e os direitos dos titulares. Deve avaliar se o serviço contratado é adequado aos tipos de dados e atividades que pretende tratar.

O fornecedor deve disponibilizar as informações razoavelmente necessárias a essa avaliação e apontar limitações relevantes identificadas. O cliente não deve assumir os deveres legais próprios do fornecedor. Nenhuma parte pode tratar uma garantia genérica da outra como substituto da resolução de uma situação de tratamento sabidamente ilícita ou insegura.

6. Confidencialidade e anexo de segurança

O fornecedor deve limitar o acesso ao pessoal autorizado que necessite dos dados para o serviço e esteja sujeito à confidencialidade ou a dever legal adequado. Deve implementar e manter medidas técnicas e organizacionais apropriadas à natureza, ao contexto e aos riscos do tratamento acordado. O anexo de segurança deve identificar as medidas efetivamente implementadas, seu alcance e as funções responsáveis.

O anexo de segurança deve ser verificado antes do início do tratamento correspondente e revisto diante de mudanças relevantes nos riscos ou no tratamento. O fornecedor não deve reduzir materialmente a proteção acordada sem tratar o risco e cumprir as exigências aplicáveis de aviso e concordância. Cada controle listado deve descrever fielmente sua implementação e alcance.

- Gestão de acessos, privilégio mínimo, autenticação, proteção de credenciais e retirada de acessos desnecessários.
- Proteção dos dados em trânsito e armazenamento, separação de ambientes de clientes e tratamento seguro de segredos, conforme os riscos.
- Registros de eventos, correção de vulnerabilidades, controle de mudanças, detecção de incidentes e orientação do pessoal.
- Proteção de backups, restauração, resiliência, descarte seguro e avaliação periódica da eficácia das medidas.

7. Suboperadores e alterações na lista

O fornecedor somente pode contratar um suboperador com autorização prévia e escrita do cliente, na forma exigida pela lei aplicável. A infraestrutura do Lumez inclui AWS, Google Cloud, Vercel e infraestrutura própria do fornecedor. O anexo deve identificar as entidades jurídicas, funções contratadas, locais de tratamento e mecanismos de transferência efetivamente envolvidos em cada operação. O fornecedor deve impor por contrato deveres equivalentes de proteção de dados e continua responsável pelo desempenho de seu suboperador conforme exigido por lei.

Se for escolhida autorização geral, o canal operacional acordado deve comunicar previamente inclusões ou substituições pretendidas e oferecer oportunidade efetiva de oposição por motivos de proteção de dados antes do início do tratamento afetado. As partes devem registrar no anexo o procedimento de aviso e oposição, examinar alternativas e resolver a objeção. Objeções lícitas não resolvidas não podem ser tratadas como autorização automática; eventual suspensão ou encerramento deve preservar os direitos obrigatórios do cliente e suas opções de devolução dos dados.

8. Transferências internacionais

O anexo de transferências deve mapear as entidades exportadoras e receptoras, os países de tratamento, acessos remotos e transferências posteriores. Para cada fluxo sujeito a restrições, as partes devem identificar mecanismo válido e avaliações ou medidas complementares exigidas. Uma decisão de adequação só se aplica dentro de seu efetivo alcance territorial e material; uma decisão de um sistema jurídico não atende automaticamente a outro.

Quando forem necessárias cláusulas padrão oficiais, o instrumento, módulo, partes e anexos corretos devem ser preenchidos e validamente incorporados, sem reescrever ou contrariar o texto obrigatório. As cláusulas da União Europeia, o IDTA ou Addendum britânico e as cláusulas da ANPD são instrumentos distintos. Este DPA não os reproduz, celebra ou substitui, e um link ou anexo em branco não constitui mecanismo de transferência completo.

9. Pedidos de direitos e assistência regulatória

Considerando o tratamento e as informações disponíveis, o fornecedor deve auxiliar o cliente no acesso, correção, exclusão, restrição, portabilidade, oposição e demais direitos aplicáveis, por medidas técnicas e organizacionais adequadas. Deve encaminhar prontamente os pedidos referentes aos dados abrangidos ao contato designado pelo cliente e responder diretamente somente quando autorizado ou legalmente obrigado.

A assistência deve permitir o cumprimento dos prazos legais aplicáveis, inclusive quando as ferramentas existentes de exportação ou exclusão não abrangerem todos os dados pertinentes. As partes devem manter um processo operacional de encaminhamento e conclusão para o tratamento abrangido. O fornecedor também deve auxiliar no cumprimento de obrigações de segurança, avaliações de impacto, consultas prévias e solicitações de autoridades, conforme exigido, sem divulgar dados alheios de outros clientes.

10. Incidentes com dados pessoais

O fornecedor deve notificar o contato designado pelo cliente sem demora indevida após tomar conhecimento de um incidente de segurança com dados pessoais abrangidos e cumprir eventual exigência legal de prazo menor. Deve adotar medidas apropriadas de contenção, investigação, mitigação e correção, preservar evidências pertinentes e colaborar com a avaliação e as comunicações exigidas do cliente.

O aviso deve fornecer as informações então disponíveis sobre a natureza do incidente, dados e pessoas afetados, consequências prováveis, medidas adotadas ou propostas e contato para acompanhamento. Informações faltantes devem ser fornecidas progressivamente, sem atrasar o aviso inicial. Os deveres de comunicação do controlador não justificam atraso do operador; o fornecedor não deve fazer admissões ou comunicações em nome do cliente sem autorização, salvo quando a lei as exigir.

11. Informações, verificação e auditorias

O fornecedor deve disponibilizar as informações necessárias para demonstrar o cumprimento deste DPA e dos deveres aplicáveis ao operador e permitir e colaborar com auditorias, inclusive inspeções pelo cliente ou auditor autorizado. Evidências existentes e pertinentes podem apoiar a verificação, mas não substituir uma auditoria legalmente exigida nem ocultar uma lacuna relevante.

As partes podem coordenar escopo, momento e confidencialidade para proteger a segurança e as informações de outros clientes, sem tornar a verificação ineficaz ou impedir ação urgente ou acesso lícito de autoridades. Deficiências identificadas devem ser investigadas e corrigidas com acompanhamento documentado. Afirmações sobre certificações, auditorias concluídas ou conformidade devem ser sustentadas por evidências aplicáveis e verificáveis.

12. Devolução, exclusão e retenção necessária

Ao término do serviço de tratamento pertinente, o fornecedor deve, à escolha do cliente, devolver ou excluir os dados pessoais abrangidos e excluir as cópias existentes, salvo retenção exigida pela lei aplicável. O anexo deve definir o método prático, alcance da exportação, etapas de conclusão e tratamento dos backups. O fornecedor deve fornecer registro fiel da conclusão, identificando eventual retenção legal, seu fundamento e duração ou critérios de determinação.

A retenção não pode se justificar somente por conveniência técnica. Dados que devam permanecer precisam ser isolados, protegidos e utilizados exclusivamente para a finalidade exigida até que sua exclusão seja lícita. As partes devem validar um ciclo definido de exclusão de backups e controles para impedir a reintrodução de dados excluídos. Ferramentas automáticas limitadas exigem assistência complementar; exclusão de workspace, exclusão de conta e eliminação de cópias em destinatários independentes são operações distintas.

13. Meta, IA e destinos escolhidos pelo cliente

O papel da Meta, do WhatsApp e de cada integração deve ser determinado pelo fluxo real de dados e pelo contrato aplicável. Um destinatário escolhido de forma independente pelo cliente, como o destino de webhook de uma automação, não é automaticamente suboperador contratado pelo fornecedor. O anexo deve identificar o destinatário, as instruções e a responsabilidade pertinentes, sem transferir os deveres próprios do fornecedor ao cliente.

O tratamento por IA em produção exige documentação prévia do fornecedor real, finalidade, dados transmitidos, retenção, acesso e mecanismo de transferência, quando aplicável. Os dados abrangidos não devem ser utilizados no treinamento de modelo de propósito geral nem em finalidades alheias do fornecedor sob este DPA. Simulações não estabelecem relação com fornecedor de produção; qualquer tratamento adicional exige avaliação lícita separada, aviso adequado e instruções ou acordo válidos.

14. Prevalência, alterações e continuidade dos deveres

Para o tratamento abrangido, este DPA prevalece sobre disposições gerais conflitantes do serviço, enquanto a lei obrigatória e instrumentos de transferência validamente incorporados prevalecem na medida exigida. Ele não reduz direitos dos titulares, poderes das autoridades ou reparações que não possam ser limitados por contrato. Nenhuma disposição comercial de responsabilidade pode afastar uma proteção obrigatória da lei aplicável.

Alterações devem ser registradas, comunicadas e validamente acordadas quando necessário. As partes devem revisar os anexos diante de mudanças relevantes no tratamento e interromper qualquer operação afetada que esteja sem base legal ou salvaguarda exigida até sua regularização. Os deveres de confidencialidade, segurança, assistência e exclusão continuam para os dados mantidos após o encerramento. Os anexos específicos do cliente e o registro do aceite permanecem essenciais a um acordo completo.