Acuerdo de tratamiento de datos de Lumez

Acuerdo que rige los datos personales tratados por el proveedor de Lumez siguiendo instrucciones de un cliente, incorporado al contrato de servicio y complementado por los anexos de tratamiento, seguridad, subencargados y transferencias específicos de la contratación.

Versión: 2026-09-18.1
Actualizado el: 2026-09-18

Proveedor 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

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

Privacidad y soporte: arthurgfcardozo@gmail.com

Mercado inicial: América del Sur

Infraestructura: AWS, Google Cloud, Vercel e infraestructura propia de Digital Directive

Digital Directive es el nombre comercial declarado por el titular. Lumez es el producto cubierto por estos documentos; los demás productos no se incluyen automáticamente.

1. Partes e incorporación contractual

Este Acuerdo de tratamiento de datos, o DPA, corresponde al proveedor identificado en este documento, que opera bajo el nombre comercial Digital Directive, y al cliente identificado en el contrato de servicio. Su objeto es el tratamiento de datos personales mediante Lumez, disponible en lumez.digital-directive.com, por cuenta del cliente. Forma parte del contrato de las partes cuando se incorpora válidamente a esa relación.

Contacto de privacidad y soporte: arthurgfcardozo@gmail.com. Las partes deben identificar sus entidades jurídicas, contactos y funciones y documentar una aceptación válida. Los anexos específicos de la contratación forman parte del acuerdo y deben especificar el tratamiento real, las medidas de seguridad, los subencargados autorizados y los mecanismos de transferencia aplicables. La información necesaria debe completarse y verificarse antes de iniciar el tratamiento correspondiente; la publicación por sí sola no acredita la implementación técnica ni sustituye esos anexos.

2. Funciones y legislación aplicable de protección de datos

En las operaciones regidas por este DPA, el cliente actúa como responsable y el proveedor como encargado del tratamiento, salvo que el anexo completado establezca una relación lícita entre encargado y subencargado. En ese caso, el cliente debe tener la autorización necesaria y transmitir las instrucciones aplicables de su responsable. Las funciones dependen de las actividades reales, no solo de la denominación contractual.

Cada parte debe cumplir la legislación de protección de datos aplicable a su función y operaciones. Puede incluir la LGPD brasileña, el RGPD de la Unión Europea o del Reino Unido, o la CCPA de California modificada por la CPRA, cuando se cumplan sus requisitos de aplicación. Los tratamientos del proveedor para finalidades propias determinadas de manera independiente deben identificarse por separado y no pueden incluirse silenciosamente en las instrucciones del cliente.

3. Instrucciones documentadas y límites de finalidad

El proveedor debe tratar los datos comprendidos únicamente conforme a instrucciones documentadas y lícitas y para las finalidades acordadas del servicio, incluidas las transferencias. El contrato, los anexos completados y las configuraciones autorizadas pueden registrar instrucciones. Un cambio sustancial de finalidad o alcance requiere un acuerdo registrado; un acceso técnico amplio no autoriza usos ajenos al servicio.

El proveedor debe informar inmediatamente al cliente si, a su juicio, una instrucción infringe la legislación aplicable de protección de datos, solicitar aclaraciones y abstenerse de ejecutar la instrucción ilícita. Si la ley exige un tratamiento distinto de las instrucciones, debe identificar la exigencia legal y notificar al cliente antes del tratamiento, salvo que esa ley prohíba notificarlo.

Cuando actúe como prestador de servicios o contratista conforme a la CCPA, el proveedor no debe vender ni compartir la información personal comprendida, conservarla, usarla o divulgarla fuera de las finalidades especificadas o de la relación comercial directa, ni combinarla con otros datos salvo autorización expresa de la ley aplicable. Debe ofrecer el nivel de protección exigido, notificar la imposibilidad de cumplir y permitir medidas lícitas del cliente para verificar, detener y corregir usos no autorizados.

4. Anexo obligatorio de tratamiento

Las partes deben completar un anexo que describa el tratamiento real antes de iniciar las operaciones correspondientes. Las categorías siguientes indican aspectos que deben evaluarse; no autorizan todas las categorías, no fijan una conservación universal ni afirman que determinada integración esté activa en producción.

- Objeto, naturaleza y finalidades: funciones contratadas de contactos y conversaciones, almacenamiento, organización, acceso, transmisión, exportación, eliminación y automatizaciones o tratamientos por IA expresamente autorizados.

- Categorías de datos: identificadores pertinentes, datos de contacto, mensajes y adjuntos, metadatos de interacción y datos contratados de pedidos o citas. Los datos sensibles, de menores y otras categorías restringidas requieren una evaluación explícita y salvaguardias antes de incluirse.
- Interesados: usuarios, personal, representantes, posibles clientes, contactos, clientes del contratante y otras personas cuyos datos se incluyan lícitamente en el servicio definido.
- Duración y conservación: período del servicio, instrucciones por categoría, procedimiento de devolución o eliminación, ciclo de copias de seguridad y conservaciones legales específicas. Identificar también los derechos y obligaciones del cliente y los contactos autorizados para instrucciones e incidentes.

5. Responsabilidades del cliente y evaluación conjunta

El cliente debe establecer finalidades y bases jurídicas lícitas, facilitar los avisos exigidos y obtener autorizaciones cuando sean necesarias, definir accesos y conservación proporcionados y dar instrucciones compatibles con la legislación aplicable y los derechos de los interesados. Debe evaluar si el servicio contratado es adecuado para los tipos de datos y actividades que pretende tratar.

El proveedor debe facilitar la información razonablemente necesaria para esa evaluación y señalar las limitaciones sustanciales identificadas. El cliente no debe asumir las obligaciones legales propias del proveedor. Ninguna parte puede considerar una garantía genérica de la otra como sustituto de resolver un tratamiento que se sepa ilícito o inseguro.

6. Confidencialidad y anexo de seguridad

El proveedor debe limitar el acceso al personal autorizado que necesite los datos para el servicio y esté sujeto a confidencialidad o a un deber legal adecuado. Debe aplicar y mantener medidas técnicas y organizativas apropiadas a la naturaleza, el contexto y los riesgos del tratamiento acordado. El anexo de seguridad debe identificar las medidas efectivamente implantadas, su alcance y las funciones responsables.

El anexo de seguridad debe verificarse antes de iniciar el tratamiento correspondiente y revisarse cuando cambien sustancialmente los riesgos o el tratamiento. El proveedor no debe reducir sustancialmente la protección acordada sin abordar el riesgo y cumplir los requisitos aplicables de aviso y acuerdo. Cada control enumerado debe describir fielmente su implementación y alcance.

- Gestión de accesos, mínimo privilegio, autenticación, protección de credenciales y retirada de accesos innecesarios.
- Protección de datos en tránsito y almacenamiento, separación de entornos de clientes y gestión segura de secretos, según los riesgos.
- Registros de eventos, corrección de vulnerabilidades, control de cambios, detección de incidentes y concienciación del personal.
- Protección de copias de seguridad, restauración, resiliencia, eliminación segura y evaluación periódica de la eficacia de las medidas.

7. Subencargados y cambios en la lista

El proveedor solo puede contratar a un subencargado con autorización previa y escrita del cliente, en la forma exigida por la ley aplicable. La infraestructura de Lumez incluye AWS, Google Cloud, Vercel e infraestructura propia del proveedor. El anexo debe identificar las entidades jurídicas, funciones contratadas, lugares de tratamiento y mecanismos de transferencia efectivamente implicados en cada operación. El proveedor debe imponer por contrato obligaciones equivalentes de protección de datos y sigue siendo responsable de la actuación de su subencargado según lo exija la ley.

Si se elige una autorización general, el canal operativo acordado debe avisar previamente de las incorporaciones o sustituciones previstas y ofrecer una oportunidad efectiva de oponerse por motivos de protección de datos antes de iniciar el tratamiento afectado. Las partes deben registrar en el anexo el proceso de aviso y oposición, examinar alternativas y resolver la objeción. Las objeciones lícitas no resueltas no pueden considerarse autorización automática; toda suspensión o finalización debe preservar los derechos imperativos del cliente y sus opciones de devolución de datos.

8. Transferencias internacionales

El anexo de transferencias debe identificar las entidades exportadoras y receptoras, los países de tratamiento, los accesos remotos y las transferencias ulteriores. Para cada flujo sujeto a restricciones, las partes deben identificar un mecanismo válido y las evaluaciones o medidas complementarias exigidas. Una decisión de adecuación solo se aplica dentro de su alcance territorial y material real; una decisión de un sistema jurídico no satisface automáticamente otro.

Cuando se requieran cláusulas tipo oficiales, deben completarse e incorporarse válidamente el instrumento, módulo, partes y anexos correctos, sin reescribir ni contradecir el texto obligatorio. Las cláusulas de la Unión Europea, el IDTA o Addendum británico y las cláusulas de la ANPD son instrumentos distintos. Este DPA no los reproduce, celebra ni sustituye, y un enlace o anexo vacío no constituye un mecanismo de transferencia completo.

9. Solicitudes de derechos y asistencia regulatoria

Teniendo en cuenta el tratamiento y la información disponible, el proveedor debe ayudar al cliente con el acceso, rectificación, supresión, limitación, portabilidad, oposición y demás derechos aplicables mediante medidas técnicas y organizativas apropiadas. Debe remitir sin demora las solicitudes relativas a los datos comprendidos al contacto designado por el cliente y responder directamente solo cuando esté autorizado o legalmente obligado.

La asistencia debe permitir cumplir los plazos legales aplicables, incluso cuando las herramientas existentes de exportación o eliminación no abarquen todos los datos pertinentes. Las partes deben mantener un proceso operativo de escalamiento y finalización para el tratamiento comprendido. El proveedor también debe asistir en obligaciones de seguridad, evaluaciones de impacto, consultas previas y solicitudes de autoridades cuando se exija, sin divulgar datos ajenos de otros clientes.

10. Incidentes con datos personales

El proveedor debe notificar al contacto designado por el cliente sin dilación indebida cuando tenga conocimiento de una violación de seguridad de los datos personales comprendidos, y cumplir cualquier plazo legal más breve que resulte aplicable. Debe adoptar medidas apropiadas de contención, investigación, mitigación y corrección, conservar pruebas pertinentes y colaborar con la evaluación y las notificaciones exigidas al cliente.

El aviso debe facilitar la información disponible sobre la naturaleza del incidente, los datos y personas afectados, sus posibles consecuencias, las medidas adoptadas o propuestas y un contacto de seguimiento. La información faltante debe facilitarse progresivamente, sin retrasar el aviso inicial. Los deberes de notificación del responsable no justifican retrasos del encargado; el proveedor no debe realizar admisiones ni comunicaciones en nombre del cliente sin autorización, salvo exigencia legal.

11. Información, verificación y auditorías

El proveedor debe facilitar la información necesaria para demostrar el cumplimiento de este DPA y de las obligaciones aplicables al encargado, y permitir y contribuir a las auditorías, incluidas inspecciones por el cliente o un auditor autorizado. Las pruebas existentes y pertinentes pueden apoyar la revisión, pero no sustituir una auditoría legalmente exigida ni ocultar una carencia sustancial.

Las partes pueden coordinar alcance, fechas y confidencialidad para proteger la seguridad y la información de otros clientes, sin hacer ineficaz la revisión ni impedir actuaciones urgentes o accesos lícitos de las autoridades. Las deficiencias identificadas deben investigarse y corregirse con seguimiento documentado. Las afirmaciones sobre certificaciones, auditorías concluidas o cumplimiento deben estar respaldadas por pruebas pertinentes y verificables.

12. Devolución, eliminación y conservación necesaria

Al terminar el servicio de tratamiento pertinente, el proveedor debe, a elección del cliente, devolver o eliminar los datos personales comprendidos y eliminar las copias existentes, salvo conservación exigida por la ley aplicable. El anexo debe definir el método práctico, alcance de la exportación, pasos de finalización y tratamiento de copias de seguridad. El proveedor debe facilitar un registro fiel de la finalización e identificar toda conservación legal, su fundamento y duración o criterios para determinarla.

La conservación no puede justificarse únicamente por conveniencia técnica. Los datos que deban permanecer deben aislarse, protegerse y utilizarse solo para la finalidad exigida hasta que sea lícito eliminarlos. Las partes deben validar un ciclo definido de eliminación de copias de seguridad y controles para impedir reintroducir datos eliminados. Las herramientas automáticas limitadas requieren asistencia complementaria; eliminar un espacio de trabajo, una cuenta y las copias en destinatarios independientes son operaciones distintas.

13. Meta, IA y destinos elegidos por el cliente

La función de Meta, WhatsApp y cada integración debe determinarse según el flujo real de datos y el contrato aplicable. Un destinatario seleccionado independientemente por el cliente, como el destino de un webhook de automatización, no es automáticamente un subencargado contratado por el proveedor. El anexo debe identificar al destinatario, las instrucciones y la responsabilidad pertinentes, sin transferir al cliente las obligaciones propias del proveedor.

El tratamiento por IA en producción requiere documentación previa del proveedor real, finalidad, datos transmitidos, conservación, acceso y mecanismo de transferencia cuando corresponda. Los datos comprendidos no deben usarse para entrenar un modelo de propósito general ni para finalidades ajenas del proveedor al amparo de este DPA. Las simulaciones no establecen una relación con un proveedor de producción; todo tratamiento adicional exige una evaluación lícita separada, información adecuada e instrucciones o acuerdo válidos.

14. Prevalencia, cambios y continuidad de las obligaciones

Para el tratamiento comprendido, este DPA prevalece sobre disposiciones generales del servicio incompatibles, mientras que la ley imperativa y los instrumentos de transferencia válidamente incorporados prevalecen en la medida exigida. No reduce los derechos de los interesados, las facultades de las autoridades ni los recursos que no puedan limitarse por contrato. Ninguna disposición comercial de responsabilidad puede excluir una protección imperativa de la ley aplicable.

Los cambios deben registrarse, comunicarse y acordarse válidamente cuando corresponda. Las partes deben revisar los anexos ante cambios sustanciales del tratamiento y detener toda operación afectada que carezca de base jurídica o de una salvaguardia exigida hasta que se resuelva. Las obligaciones de confidencialidad, seguridad, asistencia y eliminación continúan para los datos conservados tras la finalización. Los anexos específicos del cliente y el registro de aceptación siguen siendo esenciales para un acuerdo completo.