

Acuerdo de Tratamiento de Datos

Global FullStack Service LLC | Versión 2.0 | 2026-09-22

Aplicable conforme a publicación y aceptación del documento

1. Partes y prioridad

El Negocio es responsable de los datos de sus clientes. Global FullStack Service LLC, 304 S Jones Blvd, Ste 8900, Las Vegas, NV 89107, Estados Unidos, es encargado y proveedor de la plataforma. Este DPA forma parte de los Términos de Servicio y prevalece en tratamiento de datos personales. Contacto: gfullstackservice@gmail.com.

2. Instrucciones y finalidad

Tratamos datos solo por instrucciones documentadas para atender consultas, gestionar citas, mantener registros y producir información operativa del servicio contratado. Las instrucciones son este DPA, el contrato, la configuración y solicitudes autorizadas. Informaremos instrucciones que consideremos ilícitas y podremos suspenderlas. No utilizamos datos para fines propios ajenos, de otro negocio, venta ni entrenamiento de modelos de IA propios o de terceros.

3. Anexo de tratamiento

Personas: clientes y potenciales clientes del Negocio. Datos: nombre, teléfono, idioma, citas, servicios, precios, historial, mensajes, transcripciones si se contrata voz, consentimientos y registros técnicos. Operaciones: recepción, registro, consulta, uso, actualización, comunicación a proveedores necesarios, conservación, devolución, anonimización y eliminación. No se solicitan datos sensibles innecesarios; si se aportan espontáneamente quedan sujetos a las mismas restricciones. Duración: vigencia del contrato y conservación autorizada.

4. Confidencialidad y medidas de seguridad

El personal autorizado está sujeto a confidencialidad y acceso limitado a sus funciones. Las medidas comprenden separación de datos por negocio; permisos mínimos de operación y consulta; cifrado en tránsito a bases de datos y terceros; acceso restringido a infraestructura; autorización independiente de las respuestas de IA; minimización de datos en enlaces y reportes; y eliminación o anonimización de identificadores e historial conversacional ante solicitudes procedentes. Mantendremos medidas apropiadas al riesgo y no reduciremos materialmente la protección sin informar.

5. Subencargados autorizados

Según funciones habilitadas: Twilio para mensajería y voz (teléfonos, mensajes, llamadas); Meta/WhatsApp para cuentas y red de mensajería (identificadores, teléfonos, mensajes, metadatos); Google Gemini para respuestas (conversación y contexto necesario); Railway para aplicaciones y bases de datos (datos de la plataforma); Netlify para páginas legales (documentos publicados y datos técnicos de acceso). No todos participan en cada configuración. Exigiremos obligaciones adecuadas por escrito y responderemos por los subencargados frente al Negocio.

6. Cambios de proveedores

El Negocio autoriza a los proveedores anteriores dentro del alcance necesario. Informaremos incorporaciones o sustituciones con al menos 30 días de antelación. Puede objetar por motivos razonables de protección de datos en ese plazo; si no se resuelve, cualquiera puede terminar sin penalidad. Al cesar un proveedor se exigirá detener el tratamiento y devolver o eliminar los datos correspondientes.

7. Derechos y asistencia

Ayudaremos razonablemente con acceso, corrección, eliminación, oposición, limitación, portabilidad, evaluaciones de impacto y consultas regulatorias cuando correspondan. Las solicitudes directas se canalizan al Negocio salvo obligación legal distinta. No revelamos datos de otro negocio ni seguimos instrucciones sin facultades verificadas.

8. Incidentes

Notificaremos al Negocio sin demora indebida y dentro de 48 horas de conocer una violación de seguridad de datos tratados por su cuenta. La notificación incluirá naturaleza, categorías y volumen aproximado, consecuencias, medidas y contacto en la medida disponible, con actualizaciones posteriores. El Negocio determina las notificaciones a personas y autoridades que le correspondan como responsable.

9. Conservación y finalización

Datos de clientes, conversaciones y citas se conservan durante la relación o hasta una solicitud procedente de eliminación. Las citas pueden conservarse anonimizadas. Los registros de ejecución pueden contener teléfonos y conversaciones y se conservan 14 días. La evidencia de consentimiento se conserva durante la relación y el plazo legal aplicable.

Al terminar, el Negocio tiene 30 días para solicitar una copia en formato estructurado de uso común o eliminación. Sin instrucciones se elimina o anonimiza salvo conservación legal informada. Los respaldos retenidos por su ciclo quedan restringidos; se reaplicarán eliminaciones si se restauran. Informaremos plazos pertinentes y no los reutilizaremos para operación ordinaria.

10. Transferencias y auditoría

La infraestructura de la plataforma se aloja en Estados Unidos; los proveedores pueden tratar datos en otros países según configuración. Las garantías internacionales exigidas se establecerán antes del tratamiento correspondiente. Facilitaremos información para demostrar cumplimiento. El Negocio puede auditar una vez al año con 30 días de preaviso, confidencialidad y sin afectar a otros negocios; asume los costos salvo incumplimiento sustancial del Proveedor. Esto no limita derechos imperativos de supervisión.