Contrato de Encargado del Tratamiento

Versión 1.1.0, publicada el 24 de noviembre de 2026

Ejemplar genérico del contrato que cada clínica acepta al crear su cuenta y firma después en la aplicación con su razón social, su NIF y su domicilio. El texto de la aplicación es idéntico a este.

Versión 1.1.0, publicada el 24 de noviembre de 2026. Sustituye a la versión 1.0.0.

Acuerdo conforme al artículo 28 del Reglamento (UE) 2016/679 (RGPD) entre la clínica (responsable del tratamiento) y FISIOOS LLC (encargado del tratamiento), con las condiciones del artículo 28.3 y las garantías de transferencia internacional.

RESPONSABLE DEL TRATAMIENTO (la Clínica)

Razón social: (se completa con los datos de la clínica al firmar en la aplicación)

NIF/CIF: (se completa con los datos de la clínica al firmar en la aplicación)

Domicilio: (se completa con los datos de la clínica al firmar en la aplicación)

Contacto: (se completa con los datos de la clínica al firmar en la aplicación)

(en adelante, «el Responsable» o «la Clínica»)

ENCARGADO DEL TRATAMIENTO

FISIOOS LLC

Estado de constitución: New Mexico (Estados Unidos)

Domicilio: 1209 Mountain Road Pl NE, Ste R, Albuquerque, New Mexico 87110, Estados Unidos

Número de identificación fiscal: EIN 39-5093651

Contacto: info@fisioos.io

Representante en la Unión (art. 27 RGPD): Prighter EU Rep GmbH, Schellinggasse 3/10, 1010 Viena, Austria.

(en adelante, «el Encargado» o «FISIOOS LLC»)

1. OBJETO

El presente contrato tiene por objeto regular las condiciones bajo las cuales el Encargado trata datos personales por cuenta del Responsable, en el marco de la prestación del servicio de software de gestión para clínicas de fisioterapia «Fisio.OS» (en adelante, «el Servicio»). Se celebra en cumplimiento del artículo 28 del Reglamento (UE) 2016/679 (RGPD) y de la Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

2. DEFINICIONES

Los términos «datos personales», «tratamiento», «responsable del tratamiento», «encargado del tratamiento», «interesado», «categorías especiales de datos» y «violación de la seguridad de los datos personales» tienen el significado que les atribuye el artículo 4 del RGPD. Se entiende por «subencargado» todo tercero contratado por el Encargado para tratar datos personales en el marco de este contrato. Los «Términos y condiciones del servicio» son el contrato de prestación del Servicio del que este documento forma parte.

3. ROL DE LAS PARTES

La Clínica es responsable del tratamiento de los datos de sus pacientes y de su personal. FISIOOS LLC actúa como encargado del tratamiento, tratando dichos datos únicamente para prestar el Servicio y siguiendo las instrucciones del Responsable. Los proveedores tecnológicos que el Encargado utiliza para prestar el Servicio actúan como subencargados (Anexo II).

Los datos de los usuarios de la cuenta (nombre, email, teléfono, credenciales y registros de acceso y seguridad) que FISIOOS LLC utiliza para dar acceso a la cuenta y protegerla, cobrar la suscripción, atender el soporte y acreditar la aceptación de los Términos y condiciones del servicio los trata como responsable del tratamiento, y se rigen por la Política de privacidad (https://www.fisioos.io/privacidad), conforme a los apartados 10.1 y 10.7 de los Términos y condiciones del servicio. Todo lo demás que se registre sobre esas personas dentro de la gestión de la Clínica (agenda, fichajes, permisos, actividad clínica) lo trata el Encargado por cuenta del Responsable.

4. INSTRUCCIONES DEL RESPONSABLE

El Encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del Responsable, incluidas las relativas a transferencias internacionales, salvo que esté obligado a ello por el Derecho de la Unión o de un Estado miembro. El uso del Servicio conforme a su documentación constituye instrucción del Responsable. Si el Encargado no puede cumplir una instrucción, informará al Responsable sin dilación indebida. Igualmente informará al Responsable si, en su opinión, una instrucción infringe el RGPD, la LOPDGDD u otra norma de protección de datos.

5. PROHIBICIÓN DE TRATAMIENTO PARA FINES PROPIOS

El Encargado y sus subencargados no utilizarán los datos personales para finalidades propias ni distintas de la prestación del Servicio, no los destinarán a otra finalidad, no los comunicarán a terceros salvo instrucción del Responsable u obligación legal, y no los emplearán para el entrenamiento de modelos de inteligencia artificial ni para elaborar perfiles o productos propios. Cualquier tratamiento del Encargado que determine por su cuenta los fines y medios lo convertiría en responsable respecto de dicho tratamiento (art. 28.10 RGPD).

El Responsable autoriza expresamente al Encargado a elaborar métricas técnicas de uso de la cuenta (qué funciones se usan y con qué frecuencia). Esas métricas no contienen datos de pacientes y FISIOOS LLC las trata como responsable, conforme al apartado 10.1 de los Términos y condiciones del servicio.

6. CONFIDENCIALIDAD Y SECRETO SANITARIO

El Encargado garantiza que las personas autorizadas para tratar los datos se han comprometido a respetar la confidencialidad o están sujetas a una obligación de confidencialidad de naturaleza estatutaria. El tratamiento comprende categorías especiales de datos (salud, art. 9 RGPD) sujetas al deber de secreto de la Ley 41/2002: el Encargado y sus subencargados quedan sujetos al deber de secreto respecto de la historia clínica, que subsiste indefinidamente tras la terminación del contrato, y limitan el acceso a estos datos al personal estrictamente necesario para la prestación y el mantenimiento del Servicio.

7. SEGURIDAD DEL TRATAMIENTO (art. 32 RGPD)

El Encargado aplica las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, reforzadas por tratarse de categorías especiales, y detalladas en el Anexo III. Entre ellas: cifrado en tránsito y en reposo, aislamiento por inquilino a nivel de base de datos, control de acceso granular, registro de auditoría de modificaciones y limitación de acceso según el principio de mínimo privilegio.

8. SUBENCARGADOS (art. 28.2 y 28.4)

El Responsable autoriza de forma general al Encargado a recurrir a los subencargados enumerados en el Anexo II. El Encargado impondrá a cada subencargado, mediante contrato, las mismas obligaciones de protección de datos estipuladas en el presente acuerdo (art. 28.4 RGPD), y seguirá siendo plenamente responsable ante el Responsable del cumplimiento de aquellos. El Encargado informará al Responsable de toda alta o sustitución de subencargados con una antelación mínima de treinta (30) días naturales; durante ese plazo el Responsable podrá oponerse por motivos razonables de protección de datos y, de no alcanzarse una solución, resolver la parte del Servicio afectada sin penalización. La falta de oposición en plazo se entenderá como aceptación.

9. ASISTENCIA AL RESPONSABLE

Teniendo en cuenta la naturaleza del tratamiento, el Encargado asistirá al Responsable con medidas técnicas y organizativas apropiadas para: atender las solicitudes de ejercicio de derechos de los interesados (el Servicio incorpora funciones de supresión/anonimización, art. 17, y de exportación estructurada, art. 20); y cumplir las obligaciones de los arts. 32 a 36 del RGPD (seguridad, notificación de violaciones y evaluaciones de impacto), a la vista de la información disponible para el Encargado.

10. NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD

El Encargado notificará al Responsable sin dilación indebida y, en todo caso, en un plazo máximo de cuarenta y ocho (48) horas desde que tenga conocimiento de una violación de la seguridad de los datos personales. La notificación incluirá, al menos: la naturaleza de la violación, las categorías y el número aproximado de interesados y de registros afectados, las consecuencias probables y las medidas adoptadas o propuestas (art. 33.3), para que el Responsable pueda cumplir su deber de notificación a la autoridad de control (art. 33) y a los interesados (art. 34).

11. DEVOLUCIÓN Y SUPRESIÓN AL FINALIZAR

11.1. Periodo de exportación. Desde que termine la prestación del Servicio por cualquier causa, el Responsable dispone de treinta (30) días naturales para obtener sus datos con las herramientas de exportación de la aplicación. Durante ese plazo puede pedir a info@fisioos.io la exportación completa de todos los datos tratados por su cuenta, que el Encargado entregará por un canal seguro en un plazo máximo de diez (10) días hábiles; si la entrega llega después del día 30, el plazo se prorroga hasta que el Responsable la haya recibido. Si el Responsable ha pedido el cambio de proveedor conforme a la sección 9 de los Términos y condiciones del servicio, se aplican los plazos de esa sección: al terminar el periodo transitorio dispone de al menos treinta (30) días naturales más de extracción, con entrega de la exportación completa en un máximo de diez (10) días hábiles, y la supresión se produce treinta (30) días después de terminar el periodo de extracción.

11.2. Bloqueo. Entre el día 31 y el día 90 desde el fin del Servicio los datos quedan bloqueados: nadie puede consultarlos ni modificarlos, salvo para preparar su devolución.

11.3. Devolución antes de suprimir. La historia clínica (Ley 41/2002) y las facturas emitidas están sujetas a obligaciones legales de conservación que recaen en el Responsable. El Encargado no suprimirá la historia clínica ni las facturas sin haberlas devuelto antes al Responsable o, por instrucción escrita de este, al nuevo encargado que designe (art. 28.3.g) RGPD y artículo 33.3 de la Ley Orgánica 3/2018). Si al llegar el día 60 el Responsable no ha descargado una exportación completa ni ha indicado otra cosa, el Encargado pondrá a su disposición de oficio, mediante un enlace de descarga seguro y personal enviado al email del administrador principal de la cuenta (rol CEO en la aplicación), un archivo con la historia clínica, los consentimientos y las facturas emitidas, en formato estructurado, disponible hasta el día 90. Avisará por email al enviar el enlace y de nuevo al menos quince (15) días antes de la supresión, y conservará prueba de esos envíos. Esa entrega tiene el valor de devolución de los datos al Responsable. Si el email de entrega no se puede entregar, o si el Responsable comunica antes del día 90 que no ha podido descargar el archivo, el Encargado conservará la historia clínica y las facturas bloqueadas, sin otro uso, hasta que la entrega se complete por un medio seguro acordado con el Responsable. Si el Responsable pide por escrito la supresión de datos que esté obligado a conservar (historia clínica, consentimientos o facturas), el Encargado le recordará esa obligación, se los devolverá antes mediante el enlace seguro y, una vez devueltos, los suprimirá en el plazo que indique el Responsable. Desde la devolución, la conservación de la historia clínica durante el plazo legal es responsabilidad exclusiva del Responsable.

11.4. Supresión. A los noventa (90) días naturales desde el fin del Servicio o, si hay cambio de proveedor, en los plazos de la sección 9 de los Términos y condiciones del servicio, el Encargado suprimirá de forma segura todos los datos personales tratados por cuenta del Responsable, incluidas la historia clínica y las facturas emitidas a sus pacientes, de sus sistemas y de los de sus subencargados, salvo que esté pendiente la devolución del apartado 11.3, que esté en curso un cambio de proveedor no finalizado o que se haya pactado por escrito un servicio de custodia tras la baja. Si el Responsable lo pide por escrito una vez descargados sus datos, la supresión se hará antes. Las copias de seguridad se eliminan en su ciclo ordinario de rotación, como máximo siete (7) días después; hasta entonces están cifradas y no se usan salvo para recuperar el Servicio ante un incidente. El Encargado confirmará la supresión por email si el Responsable lo pide.

11.5. Evidencias contractuales. El Encargado conservará, bloqueados y sin otro uso, únicamente los datos necesarios para acreditar la relación con el Responsable y atender posibles responsabilidades: este contrato firmado, los registros de aceptación de los Términos y condiciones del servicio, las facturas de la suscripción, que FISIOOS LLC trata como responsable y debe conservar por obligación fiscal y mercantil, y los registros de auditoría de la cuenta que no contengan datos clínicos de pacientes. Los conservará durante el plazo de prescripción de esas responsabilidades y solo los pondrá a disposición de jueces y tribunales, del Ministerio Fiscal o de las autoridades competentes (artículos 32 y 33.4 de la Ley Orgánica 3/2018).

12. INFORMACIÓN, AUDITORÍA Y COOPERACIÓN CON LA AUTORIDAD

El Encargado pondrá a disposición del Responsable la información necesaria para demostrar el cumplimiento del artículo 28, y permitirá y contribuirá a la realización de auditorías e inspecciones por el Responsable o un auditor por él mandatado, pudiendo facilitar certificaciones e informes de terceros cuando estén disponibles. El Encargado cooperará con la autoridad de control competente (Agencia Española de Protección de Datos) cuando esta lo solicite, y trasladará al Responsable sin dilación cualquier requerimiento que reciba de autoridades relativo a los datos tratados por cuenta de aquel (art. 31 RGPD).

13. LUGAR DEL TRATAMIENTO Y TRANSFERENCIAS INTERNACIONALES

Los datos personales tratados por cuenta del Responsable se alojan en la Unión Europea (Irlanda). El tratamiento que FISIOOS LLC realiza como encargado está sujeto directamente al RGPD (artículo 3). Como regla, el Encargado no accede a los datos del Responsable desde fuera del Espacio Económico Europeo ni permite ese acceso, salvo el tratamiento de los subencargados del Anexo II para las funciones que el Responsable active. Si fuera necesario un acceso puntual desde fuera del Espacio Económico Europeo (por ejemplo, durante un desplazamiento), se hará únicamente con las medidas técnicas del Anexo III.

Como garantías adicionales frente al riesgo de acceso de autoridades de terceros países, el Encargado se compromete a avisar al Responsable de cualquier petición de una autoridad de un tercer país salvo que la ley se lo prohíba, a impugnar las peticiones desproporcionadas, a entregar solo el mínimo necesario y a aplicar el cifrado y la seudonimización descritos en el Anexo III.

Las transferencias a subencargados situados en Estados Unidos se amparan en el Marco de Privacidad de Datos UE-EE. UU. (Decisión de Ejecución (UE) 2023/1795) cuando el subencargado figura certificado en la lista oficial y, en todo caso, en las cláusulas contractuales tipo de la Decisión de Ejecución (UE) 2021/914, módulo tres, firmadas con cada uno de ellos, junto con las medidas adicionales del Anexo III (minimización, cifrado, seudonimización, exclusión del entrenamiento de modelos y no conservación del audio). Para esas transferencias el Encargado ha realizado una evaluación de las transferencias conforme a las Recomendaciones 01/2020 del Comité Europeo de Protección de Datos; el Responsable puede pedir copia de esas garantías y un resumen de la evaluación en info@fisioos.io. El detalle por subencargado figura en el Anexo II.

Si la Comisión Europea adopta cláusulas contractuales tipo para importadores sujetos al artículo 3 del RGPD, o si una autoridad de control considera que el acceso del Encargado constituye una

transferencia internacional, las partes incorporarán esas cláusulas a este contrato sin necesidad de nueva aceptación.

14. REPRESENTANTE EN LA UNIÓN (art. 27 RGPD)

El Encargado ha designado como representante en la Unión, conforme al artículo 27 del RGPD, a Prighter EU Rep GmbH, Schellinggasse 3/10, 1010 Viena, Austria, a quien podrán dirigirse el Responsable, los interesados y las autoridades de control en todo lo relativo al tratamiento.

15. RESPONSABILIDAD Y DURACIÓN

La responsabilidad de las partes se rige por el RGPD y por los Términos y condiciones del servicio. El presente contrato permanecerá en vigor mientras el Encargado trate datos por cuenta del Responsable, incluidos los periodos de exportación, bloqueo y devolución de la cláusula 11, y se regirá, en lo no previsto por el RGPD y la LOPDGDD, por lo pactado en los Términos y condiciones del servicio.

16. LEY APLICABLE Y TRIBUNALES

Este contrato se rige por la ley española. Los conflictos entre las partes relacionados con él se resuelven conforme a la sección 26 de los Términos y condiciones del servicio (negociación previa de treinta días naturales y tribunales allí indicados). Nada de lo anterior limita los derechos de los interesados, que pueden reclamar ante la autoridad de control o ante los tribunales que les reconoce el RGPD (artículos 77, 79 y 82), ni las facultades de las autoridades de control españolas y europeas.

ANEXO I. DESCRIPCIÓN DEL TRATAMIENTO

Objeto y finalidad: Prestación del servicio de software de gestión para clínicas de fisioterapia (agenda, historia clínica, facturación, comunicaciones con pacientes, portal del paciente y funciones opcionales de inteligencia artificial).

Naturaleza del tratamiento: Recogida, registro, estructuración, conservación, consulta, uso, comunicación por transmisión, cotejo y supresión, por medios automatizados.

Duración: Mientras esté vigente la relación de prestación del Servicio y durante los periodos de exportación, bloqueo y devolución de la cláusula 11, sin perjuicio de los plazos de conservación legalmente exigibles.

Categorías de interesados: Pacientes de la Clínica; personal de la Clínica (profesionales, administración, recepción); contactos y representantes legales/tutores.

Categorías de datos: Datos identificativos y de contacto; datos de citas y asistencia; datos de facturación. Los datos de acceso de los usuarios de la cuenta (credenciales y registros de acceso y seguridad) los trata FISIOOS LLC como responsable (cláusula 3) y no forman parte de este encargo.

Categorías especiales (art. 9 RGPD): Datos de salud (historia clínica, notas de sesión, documentos clínicos, consentimientos informados y, cuando la función de transcripción esté activada, audio de valoración procesado en memoria y no persistido).

Base jurídica del Responsable: Corresponde a la Clínica como responsable. Con carácter general, la asistencia sanitaria (art. 9.2.h RGPD) amparada en el secreto profesional (Ley 41/2002) para la historia clínica; y el consentimiento u otras bases para usos accesorios (p. ej. comunicaciones comerciales).

Las funciones de inteligencia artificial son opcionales. Ningún dato se transfiere a los subencargados de inteligencia artificial salvo que la Clínica active expresamente la función correspondiente.

ANEXO II. SUBENCARGADOS AUTORIZADOS

Proveedores tecnológicos autorizados con carácter general. Su intervención depende de las funciones que la Clínica active.

- Supabase (Supabase Inc., Estados Unidos): base de datos, autenticación y almacenamiento de ficheros. Datos alojados en la Unión Europea (Irlanda). CCT.
- Vercel (Vercel Inc., Estados Unidos): alojamiento y publicación de la aplicación. Funciones en la Unión Europea (Dublín). CCT y, si figura certificado, Marco de Privacidad de Datos UE-EE. UU.
- Anthropic (Anthropic PBC, Estados Unidos): inteligencia artificial de texto (borradores de documentos clínicos, resúmenes y asistente). Tratamiento en Estados Unidos. CCT. Sin entrenamiento de modelos con los datos. Solo si la Clínica activa la función.
- OpenAI (contrato con OpenAI Ireland Ltd; tratamiento en Estados Unidos): transcripción de voz; el audio se procesa y no se conserva. CCT. Sin entrenamiento de modelos con los datos. Solo si la Clínica activa la función.
- Resend (Resend Inc., Estados Unidos): envío de correo electrónico transaccional y de comunicaciones. CCT.
- Sentry (Functional Software Inc., Estados Unidos): monitorización de errores y rendimiento, con redacción de datos personales previa al envío. CCT.
- Upstash (Upstash Inc., Estados Unidos): contadores de intentos por dirección IP y por email en el alta, para limitar el abuso; sin datos de pacientes. CCT.

CCT = cláusulas contractuales tipo de la Decisión de Ejecución (UE) 2021/914, módulo tres, incorporadas en el acuerdo de tratamiento de datos de cada subencargado. Cuando un subencargado figure además certificado en el Marco de Privacidad de Datos UE-EE. UU. (Decisión de Ejecución (UE) 2023/1795), dicho marco opera como garantía adicional (cláusula 13). El Encargado comunicará al Responsable las altas o sustituciones de subencargados con una antelación mínima de treinta (30) días naturales (cláusula 8). Lista vigente a la fecha de esta versión; la versión actualizada está disponible a requerimiento y en https://www.fisioos.io/encargado.

Stripe no es subencargado de los datos de pacientes: trata los datos de facturación de la Clínica como responsable propio y, en el cobro online al reservar, actúa bajo el contrato de la Clínica con Stripe (Stripe Connect), recibiendo de Fisio.OS solo importe, concepto y referencia.

ANEXO III. MEDIDAS TÉCNICAS Y ORGANIZATIVAS

- Cifrado en tránsito: HTTPS/TLS obligatorio en todas las comunicaciones (cliente/servidor y servidor/subencargados).
- Cifrado en reposo: AES-256 a nivel de almacenamiento, proporcionado por la infraestructura gestionada (Supabase). Credenciales de integraciones cifradas adicionalmente con AES-256-GCM a nivel de aplicación.
- Aislamiento multi-inquilino: Row Level Security (RLS) en el motor PostgreSQL: cada registro se vincula a su clínica y el filtro se evalúa contra la identidad autenticada, con independencia de la capa de aplicación.
- Control de acceso: Autenticación gestionada con rotación de tokens; roles por módulo; acceso granular a la historia clínica por usuario (mínimo privilegio). El personal del Encargado accede a los datos tratados por encargo solo para atender una solicitud de soporte, resolver una incidencia, hacer una migración encargada por la Clínica o cumplir una obligación legal, y únicamente desde conexiones cifradas con las credenciales de la cuenta.
- Seudonimización ante la inteligencia artificial: en la generación de informes y documentos clínicos con IA, la aplicación sustituye en memoria los datos identificativos del paciente, de sus tutores y de sus contactos (nombre, email, documento de identidad y teléfono) por alias antes de enviar el texto al subencargado de inteligencia artificial y los restaura al recibir la respuesta; la correspondencia entre alias e identidad no se guarda. Los pacientes marcados como excluidos de la IA no se envían.
- Registro de auditoría: Trazas inmutables (append-only) de modificaciones en operaciones sensibles (cobros, cambios de citas, fichajes y actividad de portal), con actor, marca temporal y estado anterior y posterior.
- Minimización en observabilidad: Redacción de datos personales (correo, documento de identidad, teléfono, IBAN, tarjeta) antes del envío a la herramienta de monitorización de errores.
- Copias de seguridad: copia diaria de la base de datos conservada 7 días; los ficheros subidos tienen redundancia en la Unión Europea pero no copia diaria.
- Limitación de frecuencia: Rate limiting en operaciones sensibles (exportaciones, IA, autenticación y alta) para mitigar el abuso.
- Gestión de secretos: Claves y secretos en el lado servidor; la clave de servicio nunca se expone al cliente.

Documento contractual. © FISIOOS LLC. Versión 1.1.0, publicada el 24 de noviembre de 2026.