BORRADOR pendiente de revisión legal. No firmar ni usar como contrato definitivo.

Contrato de encargo del tratamiento (art. 28 RGPD)

Versión 2026-10-01-borrador · huella SHA-256 a23cb97d2108ca52f03069de1b17179f15f5cc1283bc5d4ac789abd9bb553a5e

1. Partes y objeto

De una parte, la consulta o profesional que contrata Psynthia e identificado en la aceptación de este contrato (el «Responsable»). De otra, [RAZÓN SOCIAL DEL TITULAR DE PSYNTHIA], con NIF [NIF] y domicilio en [DOMICILIO SOCIAL], titular del servicio Psynthia (el «Encargado»).

Este contrato regula el tratamiento de datos personales que el Encargado realiza por cuenta del Responsable al prestarle el servicio Psynthia (gestión de consulta, grabación y transcripción de sesiones, asistencia de inteligencia artificial, informes, agenda y reservas), conforme al artículo 28 del Reglamento (UE) 2016/679 (RGPD) y a la Ley Orgánica 3/2018 (LOPDGDD). Forma parte de las condiciones del servicio y prevalece sobre ellas en materia de protección de datos.

2. Naturaleza, finalidad y duración del tratamiento

El Encargado trata los datos únicamente para prestar el servicio contratado: almacenarlos, mostrarlos al Responsable y a los miembros de su consulta según sus permisos, transcribir el audio de las sesiones, generar con IA resúmenes, notas e informes a petición del Responsable, gestionar citas y enviar las comunicaciones que el Responsable active.

El tratamiento dura mientras esté vigente la cuenta del Responsable. Al terminar se aplica la cláusula 11.

3. Tipos de datos y categorías de interesados

Interesados: pacientes del Responsable (y, en su caso, sus tutores legales), y los profesionales y personal de la consulta que usan el servicio.

- Datos identificativos y de contacto: nombre, fecha de nacimiento, sexo, correo electrónico, teléfono.
- Categorías especiales (art. 9 RGPD), datos de salud: historia clínica, notas de sesión, grabaciones de audio, transcripciones, hechos clínicos, objetivos e intervenciones, informes y documentos firmados.
- Datos de agenda y reserva: citas, solicitudes de reserva, consentimientos otorgados y su evidencia.
- Conversaciones con el asistente de IA relativas a pacientes.
- Datos de los usuarios de la consulta: cuenta, rol, registros de acceso y de uso.

4. Instrucciones del Responsable

El Encargado trata los datos siguiendo las instrucciones documentadas del Responsable, que son este contrato y el uso que el Responsable hace de las funciones del servicio. No los trata para fines propios

ni los usa para entrenar modelos de inteligencia artificial. Si una instrucción le parece contraria al RGPD u otra norma, lo comunicará de inmediato al Responsable.

El Responsable garantiza que tiene base jurídica para el tratamiento, en particular el consentimiento de los pacientes para grabar y transcribir sesiones, y que informa a los interesados.

5. Confidencialidad

Las personas autorizadas por el Encargado para tratar los datos están sujetas a un deber de confidencialidad, contractual o legal, que subsiste tras terminar su relación. Sólo acceden a datos de pacientes cuando es imprescindible para prestar soporte pedido por el Responsable o para resolver un incidente, y ese acceso queda registrado.

6. Seguridad del tratamiento

El Encargado aplica las medidas técnicas y organizativas del artículo 32 RGPD descritas en el Anexo I, y las revisa periódicamente. Puede actualizarlas siempre que no reduzcan el nivel de protección.

7. Subencargados

El Responsable otorga una autorización general para que el Encargado recurra a los subencargados del Anexo II, publicados en https://psynthia.app/legal/subprocessors con su función, los datos que reciben y su ubicación.

El Encargado informará al Responsable, con al menos 30 días de antelación y por correo electrónico o aviso en la aplicación, de cualquier alta o sustitución de un subencargado. El Responsable podrá oponerse por motivos razonables de protección de datos; si no se encuentra solución, podrá resolver el contrato sin penalización.

El Encargado impone a cada subencargado, por contrato, las mismas obligaciones de protección de datos de este contrato y responde ante el Responsable de su cumplimiento.

8. Transferencias internacionales

El Encargado prioriza proveedores y regiones del Espacio Económico Europeo. Cuando un subencargado trate datos fuera del EEE, la transferencia se ampara en una decisión de adecuación (incluido el Marco de Privacidad de Datos UE-EE. UU. si el proveedor está certificado) o en las cláusulas contractuales tipo de la Comisión Europea, con las medidas complementarias que procedan.

9. Asistencia al Responsable

El Encargado ayuda al Responsable a atender las solicitudes de ejercicio de derechos de los interesados (acceso, rectificación, supresión, limitación, portabilidad y oposición), entre otras cosas mediante las funciones de exportación y borrado de datos del paciente del servicio. Si recibe una solicitud directamente, la remitirá al Responsable sin responderla.

También le asiste, teniendo en cuenta la información de que dispone, en la seguridad del tratamiento, la notificación de brechas, las evaluaciones de impacto y la consulta previa a la autoridad de control (arts. 32 a 36 RGPD).

10. Violaciones de seguridad

El Encargado notificará al Responsable, sin dilación indebida y en un plazo máximo de 48 horas desde que tenga conocimiento, toda violación de la seguridad que afecte a sus datos, con la información disponible para que el Responsable pueda notificarla a la autoridad de control y, en su caso, a los interesados (arts. 33 y 34 RGPD).

11. Fin del tratamiento: devolución y supresión

Antes de cerrar su cuenta, el Responsable puede exportar los datos desde el servicio. Al terminar el contrato, el Encargado suprimirá los datos personales y sus copias en un plazo máximo de [30] días, salvo que una norma exija conservarlos; las copias de seguridad se eliminan en su ciclo ordinario de rotación, de [N] días.

12. Demostración del cumplimiento y auditorías

El Encargado pondrá a disposición del Responsable la información necesaria para demostrar el cumplimiento de este contrato y permitirá y contribuirá a auditorías, incluidas inspecciones, del Responsable o de un auditor autorizado por él, con un preaviso razonable, en horario laboral y sin comprometer la seguridad ni la confidencialidad de otros clientes.

13. Responsabilidad, vigencia y ley aplicable

Cada parte responde de sus obligaciones conforme al artículo 82 RGPD. Este contrato está vigente mientras lo esté la prestación del servicio. Si el Encargado modifica este contrato, publicará una nueva versión y pedirá al Responsable que la acepte en la aplicación. Se rige por la ley española; [FUERO].

Contacto de protección de datos del Encargado: privacy@psynthia.app.

Anexo I. Medidas técnicas y organizativas

- Cifrado en tránsito (HTTPS/TLS) en todas las comunicaciones con el servicio y con los subencargados.
- Cifrado en reposo de la base de datos y del almacenamiento de ficheros, proporcionado por el proveedor de infraestructura.
- Aislamiento por consulta: cada consulta sólo accede a sus datos, impuesto en la base de datos con políticas de seguridad a nivel de fila.
- Control de acceso por roles (propietario, administrador, terapeuta): cada terapeuta ve la información clínica de sus pacientes; los accesos de administradores a pacientes de otros terapeutas quedan registrados.
- Autenticación con contraseña y gestión de sesiones del proveedor de identidad; credenciales de

servicio sólo en el servidor.

- Registro de consentimientos de pacientes (para grabar, y para el tratamiento de datos de salud en la reserva) como evidencia inalterable.
- Minimización: las direcciones IP se guardan resumidas (hash) y los proveedores de IA y transcripción se configuran, cuando lo permiten, para no conservar ni usar los datos para entrenamiento.
- Copias de seguridad gestionadas por el proveedor de base de datos. [PENDIENTE: confirmar PITR y periodo de retención].
- Monitorización de errores con eliminación de datos personales en los informes. [PENDIENTE: confirmar configuración].

Anexo II. Subencargados

La lista vigente, con la función, los datos tratados y la ubicación de cada subencargado, está en https://psynthia.app/legal/subprocessors. La copia incluida en el PDF descargado es la vigente en la fecha de descarga.

Subencargados vigentes a 2026-10-05

Proveedor	Función	Datos	Ubicación
Supabase	Base de datos, autenticación, almacenamiento de ficheros y funciones del servidor	Todos los datos del servicio: pacientes, sesiones, audios, transcripciones, informes, conversaciones con la IA, cuentas	UE: Irlanda (AWS eu-west-1)
Google Cloud (Vertex AI)	Modelos de IA (Gemini) para el asistente, resúmenes, notas, informes, diarización y búsqueda semántica	Texto clínico: transcripciones, notas, datos del paciente incluidos en la petición	UE: multirregión europea (IA) y Fráncfort, europe-west3 (búsqueda)
Speechmatics	Transcripción del audio de las sesiones (modelo médico, en directo y tras la sesión)	Audio de la sesión y la transcripción resultante	UE: endpoints europeos de Speechmatics (Azure). El audio en directo no se conserva; el de tras la sesión se borra en cuanto se recoge la transcripción. No se usa para entrenar modelos. Entidad en el Reino Unido, con decisión de adecuación de la UE.
ElevenLabs	Transcripción del audio de las sesiones (alternativa)	Audio de la sesión y la transcripción resultante	EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Deepgram	Transcripción del audio de las	Audio de la sesión y la	UE: endpoint europeo

Proveedor	Función	Datos	Ubicación
	sesiones (alternativa, en directo o por lotes)	transcripción resultante	de Deepgram; el audio se procesa en la UE, no se conserva tras procesarlo ni se usa para entrenar modelos. Posible acceso desde EE. UU. para soporte. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Resend	Envío de correos: recordatorios de cita, reservas, invitaciones y acceso	Nombre y correo del paciente y del profesional, fecha de la cita	EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Stripe	Cobro de la suscripción y de los créditos	Datos de facturación y pago del profesional (nunca datos de pacientes)	UE (Irlanda), con posibles transferencias a EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Netlify	Alojamiento de la aplicación web y ejecución de sus funciones de servidor	Las peticiones a la aplicación en tránsito (incluido audio enviado a transcribir); no almacena datos de pacientes	EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Sentry	Registro de errores técnicos de la aplicación	Trazas técnicas e identificador interno del usuario; sin cuerpos de petición, cookies, IP ni texto de consola. La grabación de sesiones está desactivada	EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Cloudflare (Turnstile)	Verificación anti-bots (sin CAPTCHA visual) en el acceso, el registro, la recuperación de contraseña y la solicitud pública de cita	Dirección IP, agente de usuario y señales técnicas del navegador de quien rellena el formulario; no recibe el contenido del formulario ni datos clínicos	Red global de Cloudflare; entidad en EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad de Datos UE-EE. UU.
Google Calendar	Sincronización con el calendario de Google del profesional, si la activa	Fecha y hora de las citas e iniciales del paciente	UE, con posibles transferencias a EE. UU. Transferencia amparada en cláusulas contractuales tipo o en el Marco de Privacidad

Proveedor	Función	Datos	Ubicación
			de Datos UE-EE. UU.

Aceptación

Este contrato se acepta electrónicamente en Psynthia (Ajustes Contrato de encargo del tratamiento).

Si se firma en papel:

El Responsable	El Encargado
_____	_____
Nombre, NIF y firma	[RAZÓN SOCIAL DEL TITULAR DE PSYNTHIA]