

## CONTRATO DE ENCARGO DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL (DPA)

Conforme al Artículo 28 del Reglamento General de Protección de Datos (RGPD) y al Artículo 33 de la Ley Orgánica 3/2018 (LOPDGDD)

En Madrid, a la fecha de formalización electrónica telemática

### REUNIDOS

**DE UNA PARTE, OPEN ENGINEERING KNOWLEDGE, S.L.**, sociedad mercantil válidamente constituida y existente con arreglo a las leyes de España, con NIF **B-16416661**, con domicilio social sito en C/ Alfredo Marquerie 5, 28034 Madrid (España), debidamente representada por su Administrador Legal, D. Iker Alday Bonilla (en adelante, el **"ENCARGADO DEL TRATAMIENTO"** o el **"PROVEEDOR"**).

**Y DE OTRA PARTE, EL CLIENTE**, entidad mercantil o profesional sanitario titular de centro asistencial constituido conforme a la legislación española, con NIF/CIF y domicilio registrados telemáticamente en la plataforma Somma, debidamente representado por su titular o representante legal acreditado (en adelante, el **"RESPONSABLE DEL TRATAMIENTO"** o la **"CLÍNICA"**).

El ENCARGADO y el RESPONSABLE podrán ser denominados conjuntamente como las **"Partes"** e individualmente como la **"Parte"**. Ambas Partes se reconocen mutua y recíprocamente capacidad legal y jurídica suficiente para formalizar el presente Contrato de Encargo del Tratamiento, y al efecto:

### EXPONEN

**I.** Que las Partes han formalizado un **Contrato Marco de Prestación de Servicios de Software en la Nube (SaaS)** para el acceso y uso de la plataforma tecnológica de gestión clínica y recepción telefónica inteligente denominada **Verso / Somma** (en adelante, el "Contrato Principal").

**II.** Que para la correcta prestación de los servicios objeto del Contrato Principal (gestión de citas médicas, historiales clínicos, comunicaciones transaccionales y atención telefónica automatizada mediante Inteligencia Artificial), resulta imprescindible que el PROVEEDOR acceda y trate datos de carácter personal y de salud titularidad del RESPONSABLE.

**III.** Que en estricto cumplimiento del artículo 28 del **Reglamento (UE) 2016/679 (RGPD)** y del artículo 33 de la **Ley Orgánica 3/2018 (LOPDGDD)**, las Partes formalizan el presente Contrato de Encargo del Tratamiento con **carácter universal e integral para todos los módulos y funcionalidades de la Plataforma**, el cual se regirá por las siguientes:

### CLÁUSULAS

#### **PRIMERA.- OBJETO Y ALCANCE UNIVERSAL DEL ENCARGO**

**1.1.** Mediante el presente Contrato se habilita a **OPEN ENGINEERING KNOWLEDGE, S.L.**, en calidad de Encargado del Tratamiento, para tratar por cuenta de la CLÍNICA, en calidad de Responsable del Tratamiento, los datos de carácter personal estrictamente necesarios para prestar los servicios de software en la nube de la plataforma Verso / Somma.

**1.2.** El presente encargo tiene **carácter integral y universal**, amparando contractualmente la totalidad de los módulos tecnológicos de la Plataforma con el fin de evitar la formalización de anexos adicionales en caso de sucesivas activaciones de funcionalidades:

- Gestión de agenda médica, calendarios en tiempo real y asignación de citas multiprofesional.
- Administración de fichas de pacientes, historiales clínicos, notas de evolución asistencial (formato SOAP) y consentimientos informados.
- Atención telefónica automatizada de llamadas entrantes mediante agentes conversacionales de Inteligencia Artificial (IA), incluyendo procesamiento de voz, transcripción en tiempo real y resúmenes estructurados de citas.
- Comunicaciones automatizadas de confirmación, recordatorios de cita y avisos transaccionales a través de WhatsApp Business API y SMS.
- Control de bonos/packs de sesiones, cobros en recepción y emisión de facturas o justificantes de pago.

**1.3.** Las operaciones autorizadas comprenderán exclusivamente: recogida, registro, estructuración, conservación, consulta, cotejo, transmisión a subencargados autorizados, supresión y destrucción en los términos requeridos para la ejecución del servicio.

**SEGUNDA.- COLECTIVOS DE INTERESADOS Y CATEGORÍAS DE DATOS AFECTADAS**

**2.1. Colectivos de interesados:** Pacientes y usuarios del centro sanitario; potenciales clientes que contactan para solicitar información o concertar cita; y profesionales sanitarios colegiados, fisioterapeutas y personal laboral de la CLÍNICA.

**2.2. Categorías de datos tratados:**

- **Datos identificativos y de contacto:** Nombre, apellidos, DNI/NIE/Pasaporte, número de teléfono móvil, correo electrónico, fecha de nacimiento y dirección postal.
- **Datos de categorías especiales (Datos de Salud — Art. 9 RGPD):** Motivo de consulta médica, antecedentes de salud, diagnósticos fisioterápicos, notas clínicas asistenciales (formato SOAP), tratamientos prescritos, informes de evolución y consentimientos informados.
- **Registros de voz y transcripciones (Voz IA):** Grabaciones de audio y transcripciones textuales generadas durante las llamadas gestionadas por el asistente telefónico inteligente de la clínica.
- **Metadatos de comunicaciones:** Fecha, hora, duración, número de origen/destino y estados de entrega de llamadas telefónicas y mensajes transaccionales de WhatsApp.
- **Datos económicos y de facturación:** Historial de citas facturadas, bonos adquiridos, importes devengados, medios de pago y facturas emitidas.

**TERCERA.- DURACIÓN Y DESTINO DE LOS DATOS AL FINALIZAR EL SERVICIO**

**3.1.** El presente Contrato entrará en vigor en la fecha de su firma y mantendrá su vigencia durante todo el tiempo en que permanezca activo el Contrato Principal de Prestación de Servicios SaaS.

**3.2.** A la terminación de la relación contractual por cualquier causa, el ENCARGADO facilitará a la CLÍNICA un plazo de **treinta (30) días naturales** para la exportación completa de sus bases de datos en formato digital estructurado, estándar y legible por máquina (CSV / JSON / PDF).

**3.3.** Transcurrido dicho plazo, el ENCARGADO procederá a la **destrucción y supresión segura y definitiva de todas las copias** de los datos de sus servidores de producción, emitiendo previa solicitud certificado de destrucción, salvo la obligación de conservar los datos debidamente bloqueados durante los plazos legalmente exigibles para la atención de responsabilidades administrativas o judiciales.

**CUARTA.- OBLIGACIONES DEL ENCARGADO DEL TRATAMIENTO**

El ENCARGADO DEL TRATAMIENTO y su personal dependiente se comprometen expresamente a:

**4.1. Finalidad exclusiva e instrucciones documentadas:** Tratar los datos personales únicamente conforme a las instrucciones documentadas del RESPONSABLE y para las finalidades del servicio. En ningún caso utilizará los datos con fines propios ni para fines comerciales ajenos.

**4.2. Prohibición expresa de entrenamiento de modelos públicos de IA (Zero Data Retention):** El ENCARGADO garantiza de forma taxativa que **ningún dato personal, nota clínica, conversación o transcripción de los pacientes de la CLÍNICA será utilizado para entrenar, reentrenar o mejorar modelos de inteligencia artificial públicos, comerciales o de terceros**. Todo el procesamiento de lenguaje natural y síntesis de voz opera bajo acuerdos corporativos B2B con cláusulas de estricta cero retención de datos (*Zero Data Retention*).

**4.3. Deber de secreto y confidencialidad:** Garantizar que todo el personal autorizado para acceder a los datos está sujeto a un deber contractual formal de confidencialidad y secreto profesional, el cual subsistirá de forma indefinida tras la extinción de su vinculación laboral o mercantil.

**4.4. Registro de actividades de tratamiento (RAT) y capacitación:** Mantener por escrito el registro de actividades de tratamiento exigido por el art. 30.2 del RGPD y asegurar la formación continua de su equipo en seguridad de datos sanitarios.

**QUINTA.- MEDIDAS DE SEGURIDAD TÉCNICAS Y ORGANIZATIVAS (ART. 32 RGPD)**

Atendiendo al estado de la técnica y a la naturaleza de los datos tratados (que incluyen categorías especiales de datos de salud), el ENCARGADO ha implantado y mantendrá operativas las siguientes medidas de seguridad:

- **Cifrado robusto en tránsito y reposo:** Comunicaciones protegidas en tránsito extremo a extremo mediante protocolos avanzados **TLS 1.3**. Cifrado de bases de datos y archivos en reposo mediante el estándar de cifrado militar **AES-256**.
- **Aislamiento lógico multi-tenant:** Separación estricta de datos por clínica mediante políticas forzosas a nivel de fila (*Row Level Security — RLS*) con validación obligatoria de `clinic_id` en todas las consultas de base de datos.
- **Principio de mínimo privilegio y control de accesos:** Control de accesos basado en roles (RBAC). El acceso técnico a entornos de producción está estrictamente restringido, tokenizado y sometido a registro de auditoría.
- **Copias de seguridad y continuidad operativa:** Copias de seguridad automáticas diarias (*backups*) con redundancia geográfica en centros de datos europeos de alta seguridad certificados ISO/IEC 27001 y SOC 2 Tipo II (Fráncfort, Alemania).
- **Trazabilidad y auditoría inmutable:** Registro detallado de logs de auditoría que monitorizan las operaciones relevantes y los accesos a los datos.

**SEXTA.- SUBENCARGADOS DEL TRATAMIENTO AUTORIZADOS**

**6.1. Autorización general previa:** De conformidad con el artículo 28.2 del RGPD, la CLÍNICA autoriza de forma general y expresa al ENCARGADO a subcontratar los proveedores tecnológicos necesarios para la infraestructura cloud, telecomunicaciones y computación de IA.

**6.2. Lista oficial de subencargados autorizados:** La CLÍNICA aprueba expresamente la intervención de los siguientes subencargados, con los cuales el ENCARGADO tiene suscritos contratos vinculantes con garantías equivalentes:

| SUBENCARGADO                  | SEDE SOCIAL                     | FUNCIÓN / SERVICIO                                               | UBICACIÓN SERVIDORES               | GARANTÍA JURÍDICA                                       |
|-------------------------------|---------------------------------|------------------------------------------------------------------|------------------------------------|---------------------------------------------------------|
| Supabase Inc.                 | San Francisco, EE.UU.           | Base de datos PostgreSQL cloud, autenticación y almacenamiento.  | Unión Europea (Fráncfort / AWS)    | Data Privacy Framework (DPF) / Cláusulas Tipo (SCC).    |
| Render Services Inc.          | San Francisco, EE.UU.           | Alojamiento y computación de la API backend de la aplicación.    | Unión Europea (Fráncfort) / EE.UU. | Data Privacy Framework (DPF) / SCC.                     |
| Retell Inc.                   | San Francisco, EE.UU.           | Orquestación conversacional de voz para la recepcionista IA.     | EE.UU.                             | Acuerdo B2B con Zero Data Retention / SCC.              |
| OpenAI LLC                    | San Francisco, EE.UU.           | Modelos LLM para comprensión del habla y citas.                  | EE.UU.                             | Acuerdo B2B sin entrenamiento comercial / DPF / SCC.    |
| Cartesia Inc.                 | San Francisco, EE.UU.           | Síntesis de voz ultra-rápida y texto a voz (TTS) para el agente. | EE.UU.                             | Acuerdo B2B sin retención de voz / SCC.                 |
| ElevenLabs Inc.               | Nueva York, EE.UU.              | Síntesis de voz natural de alta fidelidad y texto a voz (TTS).   | EE.UU.                             | Acuerdo B2B sin uso para entrenamiento / SCC.           |
| Twilio Ireland Ltd. / Zadarma | Dublín, Irlanda / Riga, Letonia | Red de telecomunicaciones, SIP Trunking y numeración.            | Unión Europea (Irlanda / Letonia)  | Entidades radicadas en la UE / RGPD directo.            |
| Meta Platforms Ireland Ltd.   | Dublín, Irlanda                 | Infraestructura oficial de WhatsApp Business API.                | Unión Europea (Irlanda)            | Entidad radicada en la UE / Términos WhatsApp Business. |
| Stripe Payments Europe, Ltd.  | Dublín, Irlanda                 | Pasarela segura de pagos y tokenización bancaria.                | Unión Europea (Irlanda)            | Entidad UE / Certificación PCI-DSS Nivel 1.             |

**6.3. Modificaciones y garantía en cadena:** El ENCARGADO notificará cambios en subencargados con al menos quince (15) días de antelación, pudiendo la CLÍNICA oponerse motivadamente. El ENCARGADO formalizará contratos escritos vinculantes que impongan las mismas garantías a cada subencargado.

**SÉPTIMA.- NOTIFICACIÓN DE BRECHAS DE SEGURIDAD (48 HORAS)**

**7.1.** El ENCARGADO notificará a la CLÍNICA cualquier violación de la seguridad de los datos personales (brecha de datos) sin dilación indebida y en todo caso en un **plazo máximo de cuarenta y ocho (48) horas** tras tener constancia confirmada de la misma.

**7.2.** Dicho plazo de 48 horas tiene como finalidad exclusiva garantizar que la CLÍNICA disponga del margen temporal legalmente requerido para evaluar el incidente y efectuar, si procede, la preceptiva notificación a la **Agencia Española de Protección de Datos (AEPD) dentro del plazo improrrogable de setenta y dos (72) horas** fijado en el artículo 33 del RGPD.

**7.3.** La notificación detallará como mínimo la naturaleza del incidente, categorías y número estimado de interesados afectados, medidas correctoras inmediatas aplicadas y datos de contacto del responsable de seguridad del ENCARGADO.

**OCTAVA.- EJERCICIO DE DERECHOS DE LOS INTERESADOS**

**8.1.** El ENCARGADO asistirá técnicamente a la CLÍNICA para que esta pueda dar debida respuesta a las solicitudes de ejercicio de derechos de acceso, rectificación, supresión, oposición, limitación del tratamiento, portabilidad y a no ser objeto de decisiones individuales automatizadas formuladas por los pacientes.

**8.2.** En caso de que el ENCARGADO reciba directamente una solicitud de un interesado, se la trasladará a la CLÍNICA por vía telemática en un plazo no superior a **dos (2) días hábiles**, absteniéndose de resolverla de forma autónoma.

**NOVENA.- EVALUACIONES DE IMPACTO Y AUDITORÍA**

**9.1.** El ENCARGADO cooperará con la CLÍNICA facilitándole la documentación técnica disponible necesaria para la elaboración de Evaluaciones de Impacto relativas a la Protección de Datos (EIPD) y consultas previas a la autoridad de control conforme a los artículos 35 y 36 del RGPD.

**9.2.** El ENCARGADO facilitará al RESPONSABLE la información razonablemente requerida para acreditar el cumplimiento de sus obligaciones y admitirá auditorías documentales periódicas, concertadas con un preaviso mínimo de quince (15) días hábiles.

**DÉCIMA.- OBLIGACIONES DEL RESPONSABLE DEL TRATAMIENTO (LA CLÍNICA)**

Corresponde a la CLÍNICA, en su condición de Responsable del Tratamiento: (i) Disponer de base jurídica legítima conforme a los artículos 6 y 9.2.h) del RGPD para el tratamiento asistencial de los datos de salud; (ii) Informar a los pacientes en su primera visita sobre la utilización de herramientas digitales de gestión y recepción telefónica inteligente; y (iii) Administrar de forma diligente las credenciales de sus profesionales sanitarios conforme al principio de acceso estrictamente necesario.

**UNDÉCIMA.- LEGISLACIÓN APLICABLE Y JURISDICCIÓN**

El presente Contrato se rige íntegramente por el **Reglamento (UE) 2016/679 (RGPD)**, la **Ley Orgánica 3/2018 (LOPDGDD)** y el Derecho común español. Para cualquier discrepancia o litigio, las Partes se someten con renuncia a su fuero propio a los **Juzgados y Tribunales de la ciudad de Madrid** (España).

Y en prueba de conformidad con cuanto antecede, las Partes suscriben el presente Contrato de Encargo del Tratamiento de Datos por duplicado ejemplar y a un solo efecto, mediante firma digital en la fecha y lugar indicados en el encabezamiento.

**POR EL ENCARGADO DEL TRATAMIENTO:****OPEN ENGINEERING KNOWLEDGE, S.L.**

D. Iker Alday Bonilla

Administrador Legal

**POR EL RESPONSABLE DEL TRATAMIENTO:****La Entidad Contratante / Clínica Sanitaria**

Representante Legal / Titular Acreditado

Titularidad de Centro Sanitario

---

*Firma electrónica cualificada y sello de tiempo*

---

*Firma electrónica cualificada y sello de tiempo*