CONTRATO DE ENCARGADO DE TRATAMIENTO

Artículo 28 del Reglamento (UE) 2016/679 (RGPD)

> Plantilla reutilizable. Firmar con **todo tercero que acceda o trate datos de pacientes por cuenta de la responsable** (software de historia clínica en la nube, gestoría, laboratorio, destrucción documental, agencia de marketing, mantenimiento informático). Sin este contrato, cada acceso o comunicación es una cesión ilícita. Rellenar el Anexo I por cada proveedor. Cuando el proveedor imponga sus propias condiciones de tratamiento (habitual en software SaaS), adjuntar el Acuerdo de Encargo (DPA) del proveedor y verificar que cubre las cláusulas de este modelo.

REUNIDOS

De una parte, **[Nombre y apellidos de la médica]**, con NIF [ ] y domicilio profesional en [dirección], en su condición de **RESPONSABLE DEL TRATAMIENTO** (en adelante, “el Responsable”).

De otra parte, **[Razón social del proveedor]**, con NIF/CIF [ ] y domicilio en [dirección], representada por [nombre] con DNI [ ], en su condición de **ENCARGADO DEL TRATAMIENTO** (en adelante, “el Encargado”).

Ambas partes se reconocen capacidad para contratar y

EXPONEN

Que el Encargado presta al Responsable el servicio de **[descripción del servicio: alojamiento de la historia clínica, asesoría fiscal, destrucción documental, marketing, mantenimiento IT, etc.]**, cuya prestación conlleva el acceso a datos personales de los que el Responsable es titular del tratamiento. Que, conforme al art. 28.3 RGPD, dicho acceso debe regularse por contrato. A tal fin suscriben las siguientes

CLÁUSULAS

1. Objeto

El Encargado tratará por cuenta del Responsable los datos personales necesarios para prestar el servicio descrito en el **Anexo I**, que detalla el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos y las categorías de interesados (art. 28.3 RGPD).

2. Instrucciones del Responsable

El Encargado tratará los datos **únicamente siguiendo instrucciones documentadas del Responsable**, incluidas las relativas a transferencias internacionales. Si el Encargado considera que una instrucción infringe el RGPD, la LOPDGDD u otra norma de protección de

datos, informará de inmediato al Responsable. El Encargado no tratará los datos para fines propios ni distintos de los pactados.

3. Confidencialidad y deber de secreto

El Encargado mantendrá la **confidencialidad** de los datos, obligación que subsiste tras la finalización del contrato. Garantizará que las personas autorizadas para tratar los datos se hayan comprometido, expresamente y por escrito, a respetar la confidencialidad, y que estén sujetas a las obligaciones de secreto adecuadas. Al tratarse de **datos de salud**, el personal del Encargado queda sujeto al deber de secreto reforzado (art. 9.3 RGPD, art. 5 LOPDGDD).

4. Medidas de seguridad (art. 32 RGPD)

El Encargado aplicará las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, atendiendo al carácter especial de los datos de salud. Como mínimo: **cifrado** de los datos en reposo y en tránsito; capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia de los sistemas; control de acceso individualizado con doble factor de autenticación; registro de accesos; copias de seguridad con restauración verificada; y un proceso de verificación y evaluación periódica de la eficacia de estas medidas. Las medidas concretas se detallan en el **Anexo II**.

5. Subencargados (art. 28.2 y 28.4 RGPD)

El Encargado **no recurrirá a otro encargado (subencargado) sin autorización** previa, específica o general, por escrito del Responsable. En caso de autorización general, el Encargado informará de cualquier cambio de subencargados con antelación suficiente, dando al Responsable la posibilidad de oponerse. El Encargado impondrá al subencargado, mediante contrato, **las mismas obligaciones** de protección de datos que las de este contrato, y responderá plenamente ante el Responsable del incumplimiento del subencargado.

Subencargados autorizados en la fecha de firma: [listar / ninguno].

6. Transferencias internacionales

El Encargado **no transferirá datos fuera del Espacio Económico Europeo** sin instrucción o autorización previa del Responsable. Toda transferencia autorizada deberá ampararse en una **decisión de adecuación (art. 45 RGPD)** o en **garantías adecuadas (art. 46 RGPD)**, típicamente cláusulas contractuales tipo, e incorporar las medidas suplementarias que procedan. La ubicación de los servidores y las garantías aplicables constan en el **Anexo I**.

7. Asistencia al Responsable

El Encargado asistirá al Responsable, teniendo en cuenta la naturaleza del tratamiento:

- (a) En la respuesta a las solicitudes de **ejercicio de derechos** de los interesados (acceso, rectificación, supresión, oposición, limitación y portabilidad), dando traslado inmediato de las que reciba directamente (art. 28.3.e).

- (b) En el cumplimiento de las obligaciones de **seguridad** (art. 32), **notificación de brechas** (arts. 33 y 34) y, en su caso, **evaluación de impacto** (art. 35) y consulta previa (art. 36), poniendo a disposición la información necesaria (art. 28.3.f).

8. Notificación de violaciones de seguridad (art. 33.2)

El Encargado notificará al Responsable, **sin dilación indebida y en un plazo máximo de [24/48] horas** desde que tenga constancia, cualquier violación de la seguridad de los datos, con la información necesaria para que el Responsable cumpla, en su caso, su deber de notificación a la AEPD en 72 horas: naturaleza de la brecha, categorías y número aproximado de afectados y de registros, consecuencias probables y medidas adoptadas o propuestas.

9. Devolución o supresión al finalizar (art. 28.3.g)

A la terminación del contrato, y según elija el Responsable, el Encargado **devolverá** los datos y sus soportes o los **suprimirá de forma segura**, incluidas las copias existentes, salvo que una norma exija su conservación, en cuyo caso los bloqueará. El Encargado certificará por escrito la devolución o supresión. - Opción elegida por el Responsable: ☐ Devolución ☐ Supresión

10. Auditoría (art. 28.3.h)

El Encargado pondrá a disposición del Responsable toda la información necesaria para demostrar el cumplimiento de sus obligaciones y **permitirá y contribuirá a auditorías**, incluidas inspecciones, realizadas por el Responsable o por un auditor autorizado por él. Se admiten certificaciones vigentes (p. ej. ISO 27001, Esquema Nacional de Seguridad) como medio de acreditación.

11. Duración

Este contrato produce efectos mientras dure la prestación del servicio principal descrito en el Anexo I. Las obligaciones de confidencialidad y las derivadas de las cláusulas 3 y 9 subsisten tras su terminación.

12. Responsabilidad

El incumplimiento por el Encargado de las obligaciones de este contrato le convierte en **responsable** respecto de los tratamientos que realice apartándose de las instrucciones (art. 28.10 RGPD), respondiendo de los daños que cause conforme al art. 82 RGPD.

Firmado en [localidad], a [fecha].

El Responsable	El Encargado
[Nombre y apellidos]	[Razón social y representante]
Firma:	Firma:

ANEXO I, Descripción del tratamiento

Elemento	Contenido
Servicio prestado	[ ]
Objeto del encargo	[ ]
Naturaleza y finalidad del tratamiento	[ ]
Categorías de interesados	Pacientes / empleados / [ ]
Categorías de datos	Identificativos, de contacto, **datos de salud (art. 9)**, imagen, económicos [ajustar]
Operaciones autorizadas	Recogida, almacenamiento, consulta, modificación, comunicación, supresión [ajustar]
Duración	[ ]
Ubicación de los servidores / tratamiento	[País/EEE]
Transferencia internacional y garantía	[No / Sí — art. 45 o art. 46, cláusulas tipo]
Subencargados autorizados	[ ]

ANEXO II, Medidas de seguridad aplicadas por el Encargado

[Detallar: cifrado en reposo y en tránsito; control de acceso y 2FA; registro de accesos; copias de seguridad y restauración; seudonimización; gestión de soportes y destrucción segura; certificaciones vigentes.]

Nota de aplicación (no forma parte del contrato)

- **Software de HC en la nube:** verificar antes de firmar la ubicación de servidores y el DPA del proveedor; exigir cifrado y 2FA. Es el encargo crítico.
- **Gestoría:** trata facturación de pacientes y datos de empleados.
- **Laboratorio / anatomía patológica:** si actúa por cuenta del centro, es encargado; si determina fines propios, es responsable independiente y no procede este contrato.
- **Destrucción documental:** exigir certificado de destrucción.
- **Marketing / community manager y plataforma de email:** encargados; revisar transferencias internacionales.
- **Mantenimiento IT:** encargado por acceso potencial a datos de salud.
- **Pasarela de pago / TPV:** normalmente responsable propio; verificar según servicio.