

Contrato de encargado del tratamiento (modelo)

CONTRATO DE ENCARGADO DEL TRATAMIENTO

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

REUNIDOS

De una parte, La entidad cliente, con CIF , y domicilio en , (), representado/a por en calidad de , en adelante **«EL RESPONSABLE DEL TRATAMIENTO»**.

De otra parte, Edilia Tech, S.L., con CIF B-27552728, y domicilio en Calle Mayor 13, 3.º Izquierda, 28013 Madrid (Madrid), representada por Roberto López Miquel en calidad de Administrador, en adelante **«EL ENCARGADO DEL TRATAMIENTO»**.

Ambas partes, reconociéndose la capacidad legal necesaria, suscriben el presente contrato de encargado del tratamiento al amparo del artículo 28 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales (en adelante, RGPD), y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD).

CLÁUSULAS

PRIMERA. - Objeto y finalidad del tratamiento

El presente contrato tiene por objeto regular las condiciones en las que EL ENCARGADO tratará datos personales por cuenta de EL RESPONSABLE, en el marco de la acceso a la base de datos jurídico-administrativa **Edilia** con asistencia inteligente para la gestión municipal.

La finalidad del tratamiento es exclusivamente la prestación del servicio contratado, que comprende:

- Generación automatizada de documentos administrativos mediante inteligencia artificial.
- Almacenamiento y gestión de expedientes y documentos.
- Gestión de usuarios y permisos de la entidad local.
- Firma electrónica de documentos.
- Registro de auditoría de accesos y operaciones.

SEGUNDA. - Datos tratados y categorías de interesados

Categorías de datos personales tratados:

- Datos identificativos de empleados municipales: nombre, apellidos, DNI/NIF, cargo, email corporativo.
- Datos de acceso: credenciales de usuario, dirección IP, agente de navegador, registros de sesión.
- Datos contenidos en expedientes administrativos: datos identificativos de ciudadanos, empresas y terceros que figuren en los formularios completados por el usuario.
- Firmas electrónicas: hash del documento, datos del certificado digital, evidencias de firma.

Categorías de interesados:

- Empleados y cargos públicos del municipio.
- Ciudadanos, empresas y terceros cuyos datos figuren en los expedientes tramitados.

TERCERA. - Duración

El presente contrato de encargado del tratamiento tendrá la misma duración que el Contrato de Acceso a la base de datos Edilia al que complementa. Finalizada la relación contractual, EL ENCARGADO devolverá o destruirá los datos conforme a lo establecido en la cláusula novena.

CUARTA. - Obligaciones del encargado del tratamiento

EL ENCARGADO se compromete a:

- **a)** Tratar los datos personales únicamente siguiendo las instrucciones documentadas de EL RESPONSABLE, incluidas las transferencias de datos a un tercer país o una organización internacional.

- **b)** Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- **c)** Tomar todas las medidas de seguridad exigidas en el artículo 32 del RGPD.
- **d)** No recurrir a otro encargado del tratamiento sin la autorización previa por escrito de EL RESPONSABLE, salvo los subencargados expresamente autorizados en la cláusula sexta.
- **e)** Asistir a EL RESPONSABLE en la atención del ejercicio de los derechos de los interesados (acceso, rectificación, supresión, portabilidad, limitación y oposición).
- **f)** Asistir a EL RESPONSABLE en el cumplimiento de las obligaciones relativas a la seguridad del tratamiento, la notificación de violaciones de seguridad a la autoridad de control, la evaluación de impacto y la consulta previa.
- **g)** Poner a disposición de EL RESPONSABLE toda la información necesaria para demostrar el cumplimiento de las obligaciones del artículo 28 del RGPD, así como para permitir y contribuir a la realización de auditorías o inspecciones.

QUINTA. - Medidas de seguridad (art. 32 RGPD)

EL ENCARGADO aplicará las siguientes medidas técnicas y organizativas:

Cifrado en tránsito	TLS 1.3 para todas las comunicaciones entre cliente y servidor.
Cifrado en reposo	AES-256 para bases de datos y almacenamiento de archivos.
Procesamiento IA en Europa	Toda la generación de documentos con IA se procesa a través de Google Cloud Vertex AI en la región europa-west1 (Bélgica, UE) como proveedor principal, con Amazon Bedrock en la región eu-central-1 (Fráncfort, Alemania, UE) como respaldo automático en caso de indisponibilidad. Los datos nunca abandonan el Espacio Económico Europeo.
Control de acceso	Autenticación con sesión única por usuario, bloqueo tras intentos fallidos, separación de roles.

Aislamiento de datos	Separación lógica completa por municipio (multi-tenant con aislamiento por municipio_id).
Copias de seguridad	Copias diarias automáticas con retención de 30 días. Posibilidad de copia manual por el cliente.
Auditoría	Registro inmutable de todos los accesos, operaciones y eventos de seguridad.

SEXTA. - Subencargados del tratamiento

EL RESPONSABLE autoriza expresamente a EL ENCARGADO la utilización de los siguientes subencargados:

Subencargado	Finalidad	Ubicación	Garantías
Google Cloud (Vertex AI)	Generación de documentos y clasificación con modelos Claude (Anthropic) vía Vertex AI. ZDR (Zero Data Retention) activo.	europe-west1 (Bélgica, UE)	DPA Google Cloud (26/03/2026). RGPD. ISO 27001/27017/27018. SOC 1/2/3. Sin retención de datos (ZDR). Datos procesados exclusivamente en la UE.
Mistral AI	Embeddings para búsqueda semántica RAG (codestral-embed). No se utiliza para generación de documentos. Solo vectorización de consultas de búsqueda legislativa.	Francia (UE)	RGPD. ZDR activo. Servidores propios en Francia. Solo procesa consultas de búsqueda, no datos de expedientes.

Amazon Web Services (Bedrock)	Respaldo automático (fallback) para generación de documentos con modelos Claude (Anthropic) vía Amazon Bedrock. Se activa únicamente en caso de indisponibilidad temporal de Vertex AI.	eu-central-1 (Fráncfort, Alemania, UE)	Amazon Web Services EMEA SARL, en virtud del Acuerdo de Procesamiento de Datos RGD incorporado a los Términos del Servicio de AWS desde el 25 de mayo de 2018, que incluye las Cláusulas Contractuales Tipo de la UE aprobadas por la Comisión Europea. ISO 27001/27017/27018. SOC 1/2/3. Sin retención de datos. Datos procesados exclusivamente en la UE.
IONOS SE	Alojamiento de infraestructura (servidores y BBDD)	Alemania (UE)	ISO 27001, RGD, centros de datos en la UE

Para la incorporación de nuevos subencargados, EL ENCARGADO informará previamente a EL RESPONSABLE con un plazo mínimo de 30 días, pudiendo éste oponerse de forma motivada en un plazo de 15 días.

SÉPTIMA. - Notificación de violaciones de seguridad

EL ENCARGADO notificará a EL RESPONSABLE, sin dilación indebida y en un plazo máximo de **48 horas**, cualquier violación de la seguridad de los datos personales de la que tenga conocimiento, proporcionando como mínimo la siguiente información:

- Descripción de la naturaleza de la violación.
- Categorías y número aproximado de interesados afectados.
- Posibles consecuencias de la violación.
- Medidas adoptadas o propuestas para poner remedio a la violación.

Este plazo permite a EL RESPONSABLE cumplir con la obligación de notificación a la AEPD en las 72 horas establecidas en el artículo 33 del RGD.

OCTAVA. - Delegado de Protección de Datos

EL ENCARGADO designará un Delegado de Protección de Datos (DPD) conforme al artículo 37 del RGPD cuando sea legalmente exigible. Las consultas relativas a protección de datos podrán dirigirse a: **contacto@edilia.tech**.

NOVENA. - Destino de los datos a la finalización

A la finalización de la relación contractual, EL ENCARGADO, a elección de EL RESPONSABLE:

- **a)** Devolverá todos los datos personales a EL RESPONSABLE mediante exportación en formato estándar (ZIP con documentos y base de datos en formato CSV/JSON).
- **b)** Suprimirá todos los datos personales, certificando por escrito dicha supresión.

EL ENCARGADO podrá conservar los datos bloqueados durante el plazo legalmente exigido para atender posibles responsabilidades derivadas del tratamiento.

DÉCIMA. - Derecho de auditoría

EL RESPONSABLE podrá auditar el cumplimiento del presente contrato por parte de EL ENCARGADO, con un preaviso de quince (15) días laborables, pudiendo realizarse la auditoría de forma remota o presencial. EL ENCARGADO facilitará toda la documentación e información necesaria.

Y en prueba de conformidad, ambas partes firman el presente contrato en la fecha indicada en las firmas electrónicas.