Contrato de Encargo del Tratamiento de Datos Personales

Versión 2026-10-27 · Vigente desde 27 de octubre de 2026

Artículo 28 del Reglamento (UE) 2016/679 (RGPD) y artículo 33 de la Ley Orgánica 3/2018 (LOPDGDD). Basado en las cláusulas contractuales tipo de la Decisión de Ejecución (UE) 2021/915 de la Comisión.

Partes

- Responsable del tratamiento (el «Cliente»): [razón social del Cliente], NIF [NIF del Cliente], domicilio en [domicilio del Cliente].
- Encargado del tratamiento (el «Proveedor»): Redes Formación y Consultoría S.L., CIF B85928117, domicilio en C/ Fuencarral 94, 5ºID, 28004, Madrid, representante de la plataforma GenLicit.

Este contrato forma parte de los Términos y Condiciones del Servicio y se acepta junto con ellos.

1. Objeto y duración

1.1. Este contrato regula el tratamiento de datos personales que el Proveedor realiza por cuenta del Cliente al prestar el servicio GenLicit. El tratamiento se describe en el Anexo I.

1.2. Tiene la misma duración que el servicio. Las obligaciones de confidencialidad, bloqueo y supresión de la cláusula 12 subsisten tras su terminación.

2. Instrucciones del Cliente

2.1. El Proveedor trata los datos únicamente siguiendo las instrucciones documentadas del Cliente, incluidas las relativas a transferencias internacionales, salvo obligación legal.

2.2. Son instrucciones documentadas este contrato, los Términos y la configuración que el Cliente o sus usuarios realicen en la Plataforma (funciones activadas, proveedores habilitados, usuarios y permisos, plazos de conservación y documentos enviados a tratamiento).

2.3. El Proveedor informará inmediatamente al Cliente si considera que una instrucción infringe la normativa de protección de datos.

2.4. El Proveedor no usa los datos para fines propios, no los comunica a terceros fuera de lo previsto en este contrato y no los emplea para entrenar modelos de inteligencia artificial.

3. Servicios de inteligencia artificial y de lectura documental

El Cliente puede usar estos servicios con sus propias credenciales o con las cuentas del Proveedor, y puede cambiar de una a otra en la configuración de la Plataforma sin modificar este contrato. A cada proveedor se le aplica el apartado que corresponda a la forma en que el Cliente lo tenga habilitado en cada momento.

3.A. Con credenciales del Cliente (BYOK).

3.A.1. El Cliente aporta sus propias credenciales de los proveedores de inteligencia artificial y de lectura documental que decida habilitar. Esos proveedores prestan el servicio al Cliente en virtud de sus propios contratos con él y actúan, en su caso, como encargados del Cliente; no son subencargados del Proveedor.

3.A.2. El Proveedor actúa como intermediario técnico: por instrucción del Cliente transmite a esos proveedores los contenidos necesarios para cada función y recibe su respuesta (Anexo I, apartado 4).

3.A.3. Corresponde al Cliente suscribir con cada proveedor el acuerdo de tratamiento que proceda, verificar las garantías de sus transferencias internacionales, elegir planes con condiciones adecuadas (retención, no entrenamiento, residencia de datos) y no usar planes gratuitos o de prueba.

3.A.4. El Proveedor custodia esas credenciales cifradas, las usa solo para prestar el servicio al propio Cliente y no las comunica a terceros. El Cliente puede revocarlas en cualquier momento.

3.B. Con las cuentas del Proveedor (modalidad gestionada).

3.B.1. El Proveedor presta los servicios de inteligencia artificial y de lectura documental con cuentas propias, contratadas con los proveedores que figuran en la página de subencargados. Esos proveedores son subencargados del Proveedor.

3.B.2. Cada uno de ellos está vinculado por un acuerdo de tratamiento conforme con el artículo 28 del RGPD. La ubicación del tratamiento y la conservación de los contenidos que reciben son las que establecen sus condiciones de servicio vigentes en cada momento. Si tratan datos fuera del Espacio Económico Europeo, se aplican las garantías de la cláusula 7.

3.B.3. El Proveedor no usa planes gratuitos, de prueba ni de evaluación para tratar datos del Cliente.

3.C. En ambos casos.

3.C.1. El Proveedor decide los parámetros técnicos de cada llamada y aplica antes del envío las medidas de minimización del Anexo II.

4. Confidencialidad y acceso del personal del Proveedor

4.1. Las personas autorizadas por el Proveedor para tratar los datos se han comprometido a respetar su confidencialidad.

4.2. El personal del Proveedor no accede al contenido de los datos del Cliente salvo para prestar soporte, resolver una incidencia o cumplir una obligación legal. Cada acceso de este tipo requiere una autorización excepcional con motivo registrado, es temporal (máximo 72 horas) y de solo lectura salvo justificación expresa, queda registrado con su detalle y se notifica al administrador del Cliente.

4.3. El Cliente puede consultar en cualquier momento los accesos de soporte a sus datos en su registro de accesos.

5. Medidas de seguridad

5.1. El Proveedor aplica las medidas del Anexo II. Solo figuran como aplicadas las que lo están; podrá añadir otras sin reducir el nivel de seguridad.

6. Subencargados

6.1. El Cliente otorga una autorización general para que el Proveedor recurra a los subencargados publicados en https://livegenapps.com/legal/subencargados.

6.2. El Proveedor informará con al menos 30 días de antelación de cualquier incorporación o sustitución. El Cliente podrá oponerse por motivos razonables de protección de datos y, si no se alcanza una solución, resolver el servicio afectado sin penalización.

6.3. El Proveedor impone a cada subencargado las mismas obligaciones de este contrato y responde ante el Cliente de su cumplimiento.

7. Ubicación de los datos y transferencias internacionales

7.1. La Plataforma, su base de datos y los documentos se alojan en servidores situados en el Espacio Económico Europeo, operados por el subencargado de alojamiento.

7.2. Si un subencargado trata datos fuera del EEE, la transferencia se ampara en una decisión de adecuación (incluido el Marco de Privacidad de Datos UE-EE. UU.) o en cláusulas contractuales tipo, con la evaluación de sus circunstancias.

8. Derechos de los interesados

8.1. Corresponde al Cliente atender los derechos de acceso, rectificación, supresión, limitación, portabilidad y oposición.

8.2. El Proveedor le asiste con las funciones de la Plataforma: consulta y edición, exportación de los datos de una persona o de un usuario, y eliminación con bloqueo de una persona con todos sus documentos.

8.3. Si el Proveedor recibe directamente una solicitud, la trasladará al Cliente en un máximo de 5 días hábiles.

9. Información a los interesados

9.1. El Cliente, como responsable, informa a los interesados (artículos 13 y 14 del RGPD), incluido el tratamiento con herramientas de inteligencia artificial, y garantiza que cuenta con base de licitud para cada tratamiento.

9.2. El Proveedor facilita los enlaces legales del Cliente a los colaboradores externos antes de que aporten documentación y un modelo de cláusula informativa del artículo 14.

10. Violaciones de la seguridad

10.1. El Proveedor notificará al Cliente toda violación de seguridad que afecte a sus datos sin dilación indebida y como máximo en 48 horas desde que tenga conocimiento de ella, con la información disponible, que completará de forma gradual.

10.2. Corresponde al Cliente notificar, en su caso, a la autoridad de control y a los interesados, con la asistencia del Proveedor.

11. Evaluación de impacto, registro y auditorías

11.1. El Proveedor asiste al Cliente en las evaluaciones de impacto y consultas previas, y mantiene el registro de actividades del artículo 30.2 del RGPD.

11.2. El Proveedor pone a disposición del Cliente la información necesaria para demostrar el cumplimiento y permite auditorías, con preaviso mínimo de 30 días, en horario laboral, sin afectar a la seguridad ni a otros clientes y como máximo una vez al año salvo violación de seguridad o requerimiento de la autoridad. Cada parte asume sus costes salvo incumplimiento relevante del Proveedor.

12. Destino de los datos al terminar el servicio

12.1. Al terminar el servicio, el Proveedor entrega al Cliente la exportación completa de sus datos en formato estructurado, junto con sus documentos.

12.2. Después, los datos se bloquean durante cinco (5) años (artículos 32 y 33.4 de la LOPDGDD): no se usan para ningún fin y solo se ponen a disposición de jueces, tribunales, Ministerio Fiscal o administraciones competentes.

12.3. Al vencer el bloqueo, el Proveedor destruye los datos de forma segura en la base de datos y en el almacenamiento y emite un certificado de destrucción.

12.4. El mismo régimen de bloqueo y destrucción se aplica durante el servicio a los datos que el Cliente elimine en la Plataforma.

13. Responsabilidad y ley aplicable

13.1. Cada parte responde conforme al artículo 82 del RGPD. [Límites de responsabilidad a definir por la asesoría jurídica.]

13.2. Este contrato se rige por la legislación española y de la Unión Europea.

Anexo I. Descripción del tratamiento

Interesados: usuarios de la Plataforma designados por el Cliente; profesionales y candidatos cuyos datos o currículum incorpora el Cliente; personal de organizaciones con las que concurre o colabora; colaboradores externos a los que solicita documentación; personas de contacto que figuran en documentos de licitación.

Datos: identificativos y de contacto; académicos y profesionales (currículum, titulaciones, certificaciones, idiomas, experiencia, referencias); económicos y laborales si el Cliente los registra (salario, coste por hora, contrato, disponibilidad); de uso y seguridad (credenciales cifradas, registros de actividad, de inteligencia artificial y de lectura, aceptaciones de confidencialidad). No se tratan categorías especiales del artículo 9 del RGPD.

Operaciones: alojamiento y conservación; lectura de documentos; extracción y estructuración con inteligencia artificial; generación asistida de ofertas y currículum; puntuación determinista de adecuación de profesionales (la decisión la toma siempre un usuario); comunicaciones por correo; soporte.

Funciones que envían datos a inteligencia artificial o lectura documental:

Función · Datos enviados · Minimización
Lectura de documentos · Fichero original · El servicio de lectura no conserva los documentos de personas
Extracción de currículum · Texto del currículum · —
Verificación de documentos · Texto del documento, nombre y perfil profesional · Sin contacto, salario ni notas; el número de identidad solo en documentos de identidad
Generación de currículum · Nombre, perfil profesional y requisitos del pliego · Sin contacto, salario ni notas
Asistente de la licitación · Nombre y perfil resumido de hasta 20 profesionales · Sin contacto, salario ni notas
Encaje con el pliego · Hechos del perfil y de la organización · Seudonimización de nombres e identificadores
Análisis de pliegos y redacción · Texto de los pliegos y del borrador · —

Duración y ubicación: la del servicio más el bloqueo de la cláusula 12; Espacio Económico Europeo.

Anexo II. Medidas técnicas y organizativas

Solo están marcadas las medidas aplicadas a la fecha de esta versión.

Control de acceso

[X] Contraseñas con Argon2id; mínimo 12 caracteres y comprobación contra contraseñas filtradas.
[X] Verificación en dos pasos (TOTP) obligatoria para el personal del Proveedor; disponible para todos los usuarios del Cliente, que puede exigirla a todos ellos.
[X] Bloqueo temporal de la cuenta y límite de peticiones tras intentos fallidos.
[X] Caducidad de la sesión (12 horas, o 30 días con «recordar») y revocación inmediata al desactivar un usuario.
[X] Permisos por rol dentro de cada cliente.

Aislamiento entre clientes

[X] El cliente de cada operación se toma siempre de la sesión autenticada, nunca de datos del navegador.
[ ] Seguridad a nivel de fila en la base de datos como barrera obligatoria.

Cifrado

[X] Cifrado en tránsito (TLS con HSTS).
[X] Credenciales de terceros y secretos de verificación cifrados (AES-256-GCM); la aplicación no arranca sin clave de cifrado.
[X] Documentos cifrados con una clave propia de cada cliente (AES-256-GCM).
[ ] Cifrado del disco del servidor y de las copias de seguridad.

Acceso del personal del Proveedor

[X] Acceso excepcional solo con autorización motivada, temporal (máximo 72 horas), de solo lectura por defecto y notificada al Cliente.
[X] Registro encadenado (a prueba de alteraciones) de las operaciones de administración, incluidas las consultas directas a la base de datos y los cambios de contraseña.

Trazabilidad

[X] Registro de cada operación de inteligencia artificial y de cada lectura de documentos.
[X] Registro de inicios de sesión, descargas de documentos y exportaciones, consultable por el administrador del Cliente.

Minimización y conservación

[X] Seudonimización en el encaje con pliegos y supresión de contacto, salario y notas en el resto de funciones de inteligencia artificial.
[X] Plazos de conservación por cliente aplicados automáticamente (texto de las peticiones de inteligencia artificial: 90 días; registros: 12 meses).
[X] Bloqueo de lo eliminado y destrucción automática al vencer el plazo, con registro.

Seguridad de la aplicación

[X] Cabeceras de seguridad y política de seguridad de contenidos con nonce.
[X] Aislamiento del contenido no confiable en las peticiones a la inteligencia artificial y detección de inyección de instrucciones.
[X] Protección frente a peticiones a destinos internos (SSRF) y límites de consumo de inteligencia artificial.
[X] Monitorización de errores sin variables ni contenidos sensibles y grabación de sesión solo en caso de error, con textos enmascarados.

Continuidad y organización

[X] Copia de seguridad diaria de la base de datos.
[ ] Copia externa en el EEE y pruebas periódicas de restauración documentadas.
[ ] Procedimientos documentados de violaciones de seguridad y de atención de derechos, y compromisos de confidencialidad del personal.