# Contrato de Encargo del Tratamiento de Datos Personales

Versión 2026-11-04 · Vigente desde 4 de noviembre 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., NIF B85928117, domicilio en C/ Fuencarral 94, 5ºID, 28004, Madrid, representante de la plataforma GenProced.

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 GenProced. 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

3.1. El Cliente usa estos servicios solo con sus propias credenciales de los proveedores que decida habilitar en la configuración de la Plataforma. El Proveedor no tiene cuentas propias de inteligencia artificial ni de lectura documental para tratar datos del Cliente.

3.2. 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.

3.3. 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).

3.4. 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.

3.5. 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.

3.6. El Proveedor decide los parámetros técnicos de cada llamada y aplica antes del envío las medidas del Anexo II.

3.7. Lo mismo rige para los servicios de correo (servidores IMAP o SMTP) y de almacenamiento (OneDrive) que el Cliente conecte con sus propias credenciales.

## 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. Las operaciones que realiza en esos accesos y que la Plataforma registra quedan anotadas en el registro de actividad con indicación de que las realizó el Proveedor.

4.3. El Cliente puede consultar esas anotaciones en el registro de accesos de cada expediente y de cada contacto.

## 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://app.genproced.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 se ejecuta, y su base de datos y los documentos se alojan, en servidores situados en el Espacio Económico Europeo (Irlanda), operados por los subencargados 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 de los datos de un contacto, exportación de los datos de un contacto y de sus consentimientos, y anonimización de un contacto con revocación de sus consentimientos. Para los datos que esas funciones no cubren (documentos, correos, texto libre de los expedientes), el Proveedor asiste al Cliente a petición suya.

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.

## 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, si lo solicita, una exportación 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 elimina los datos de la base de datos y del almacenamiento y lo acredita por escrito si el Cliente lo solicita.

12.4. Durante el servicio, los documentos y contactos que el Cliente elimina se suprimen de la Plataforma en ese momento. Los expedientes que elimina se conservan ocultos hasta la terminación del servicio y siguen después el régimen de los apartados 12.2 y 12.3.

## 13. Responsabilidad y ley aplicable

13.1. Cada parte responde conforme al artículo 82 del RGPD.

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; clientes del despacho y sus representantes; partes contrarias, terceros y testigos de los asuntos; trabajadores, deudores, acreedores, socios y familiares (incluidos menores) que intervienen en los asuntos; personas de contacto del directorio; remitentes y destinatarios de los correos y comunicaciones que el Cliente incorpora.

Datos: identificativos y de contacto (nombre, NIF, dirección, email, teléfono); datos de los asuntos (descripción, incidencias, tareas, plazos, notas); documentos que el Cliente aporta (escrituras, contratos, nóminas, sentencias, informes y otros); correos y comunicaciones judiciales; datos económicos, de facturación y de horas dedicadas. Según la materia de cada asunto (por ejemplo, familia, laboral o penal), los documentos y textos que incorpora el Cliente pueden contener categorías especiales de datos (artículo 9 del RGPD) y datos relativos a infracciones penales (artículo 10 del RGPD). La Plataforma no tiene campos específicos para ellos; el Cliente decide si los incorpora y con qué base jurídica.

Operaciones: alojamiento y conservación; consulta, organización y búsqueda; generación de alertas y listas de comprobación a partir de los datos del expediente; sincronización del correo que el Cliente conecte;

importación de documentos desde el OneDrive del usuario; envío de avisos y notificaciones por correo; y, si el Cliente las activa, las funciones de inteligencia artificial y lectura documental siguientes.

Funciones que envían datos a inteligencia artificial o lectura documental (siempre con las credenciales del Cliente, cláusula 3):

Función · Datos enviados · Minimización
Asistente del expediente · Datos del expediente (código, cliente, área, resumen, abogado responsable), incidencias, nombres y observaciones de documentos, lista de comprobación, tareas, historial de la conversación y pregunta del usuario · Contexto limitado en tamaño y marcado como no confiable; detección de inyección de instrucciones
Análisis de contratos · Texto de las cláusulas del contrato analizado y del modelo de referencia · Cláusulas limitadas en tamaño y marcadas como no confiables; detección de inyección de instrucciones
Importación de normativa desde archivo · El archivo completo (lectura documental) y el texto resultante (inteligencia artificial) · Texto limitado en tamaño y marcado como no confiable
Extracción de datos de un documento · El archivo completo del documento seleccionado · Solo el documento que el usuario elige

Duración y ubicación: la del servicio más el bloqueo de la cláusula 12; Espacio Económico Europeo. Los proveedores que el Cliente habilita con sus credenciales tratan los datos donde establezcan sus contratos con el Cliente.

## Anexo II. Medidas técnicas y organizativas

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

Control de acceso

- [X] Contraseñas gestionadas por el servicio de autenticación, que solo guarda su hash; la Plataforma no las almacena.
- [X] Verificación en dos pasos (TOTP) disponible para todos los usuarios.
- [ ] Verificación en dos pasos obligatoria para administradores del Cliente y personal del Proveedor.
- [ ] Bloqueo temporal de la cuenta y límite de peticiones tras intentos fallidos.
- [X] Al desactivar un usuario, la Plataforma le deniega el acceso a los datos desde su siguiente petición.
- [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 para la propia aplicación.

Cifrado

- [X] Cifrado en tránsito (TLS con HSTS).
- [X] Credenciales de terceros y secretos de integración cifrados con AES-256-GCM.
- [ ] Documentos cifrados con una clave propia de cada cliente.

Acceso del personal del Proveedor

- [X] Las operaciones registradas que realiza el personal del Proveedor dentro de la cuenta del Cliente quedan identificadas como suyas.
- [ ] Acceso excepcional solo con autorización motivada, temporal, de solo lectura por defecto y notificada al Cliente.
- [ ] Registro a prueba de alteraciones de las operaciones de administración.

Trazabilidad

- [X] Registro de las conversaciones con el asistente y de los análisis de contratos, con contenido cifrado.
- [X] Registro de actividad y de accesos a expedientes, documentos y contactos, consultable por el administrador del Cliente.
- [ ] Registro de inicios de sesión.

Minimización y conservación

[X] Plazos de conservación aplicados automáticamente a los registros de actividad (2 años), de accesos (2 años; 5 años los de operaciones sensibles) y de inteligencia artificial (1 año).
[ ] Seudonimización de datos de contacto y económicos en las funciones de inteligencia artificial.
[ ] Bloqueo de lo eliminado y destrucción automática al vencer el plazo.

Seguridad de la aplicación

[X] Cabeceras de seguridad y política de seguridad de contenidos.
[X] Aislamiento del contenido no confiable en las peticiones a la inteligencia artificial; detección de inyección de instrucciones en el asistente y en el análisis de contratos.
[X] Lista cerrada de destinos para las peticiones a inteligencia artificial, lectura documental y OneDrive, y límites de consultas de inteligencia artificial por hora.
[X] Monitorización de errores sin variables ni datos personales del navegador, y grabación de sesión solo en caso de error, con textos enmascarados.

Continuidad y organización

[X] Compromisos de confidencialidad del personal autorizado (cláusula 4.1).
[ ] Copia de seguridad diaria de la base de datos con pruebas periódicas de restauración documentadas.
[ ] Procedimientos documentados de violaciones de seguridad y de atención de derechos.