Contrato de Encargo del Tratamiento de Datos Personales

Versión 2026-11-05 · Vigente desde 5 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 FormaProcesos.

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 FormaProcesos. El tratamiento se describe en el Anexo I.

1.2. Tiene la misma duración que el servicio. Las obligaciones de confidencialidad 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 de IA habilitados con su clave, usuarios y permisos, 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

La Plataforma ofrece funciones opcionales de inteligencia artificial y de lectura documental que el Cliente activa con sus propias credenciales (BYOK). Mientras el Cliente no las configure, la Plataforma no envía ningún dato a estos servicios.

3.1. El Cliente aporta sus propias credenciales de los proveedores de inteligencia artificial (OpenAI, Anthropic o Google) y de lectura documental (Datalab) 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.

3.2. 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).

3.3. 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.

3.4. El Proveedor custodia esas credenciales cifradas (AES-256-GCM), las usa solo para prestar el servicio al propio Cliente y no las comunica a terceros. El Cliente puede revocarlas en cualquier momento.

3.5. El Proveedor decide los parámetros técnicos de cada llamada y aplica antes del envío las medidas 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. Estos accesos se limitan a lo imprescindible.

4.3. El Cliente puede consultar en la Plataforma el registro de accesos de cada uno de sus proyectos.

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://formaprocesos.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, 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 de los datos de cada persona, exportación del calendario (ICS) y del registro de accesos, y eliminación de registros, que quedan retirados de la vista del Cliente.

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. A la terminación del servicio, el Proveedor, siguiendo instrucciones del Cliente, le devuelve o suprime los datos personales tratados por su cuenta y los documentos asociados.

12.2. Si una norma exige conservar determinados datos (por ejemplo, con efectos fiscales o de facturación), el Proveedor los conserva bloqueados durante el plazo legal aplicable, sin usarlos para ningún otro fin, y los suprime al vencer.

12.3. La eliminación de un registro en la Plataforma lo retira de la vista del Cliente; el dato se suprime de forma definitiva de la base de datos y del almacenamiento cuando deja de ser necesario para las finalidades y obligaciones anteriores.

13. Responsabilidad y ley aplicable

13.1. Cada parte responde conforme al artículo 82 del RGPD. Los límites de responsabilidad son los previstos en los Términos y Condiciones del Servicio.

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; docentes y candidatos cuyos datos y currículum incorpora el Cliente; participantes y alumnado de las acciones formativas; y personas de contacto de los clientes y proveedores del Cliente.

Datos: datos identificativos y de contacto; datos profesionales y académicos (currículum, experiencia, formación, certificaciones, idiomas); datos de participación en acciones formativas; y datos de facturación. No se tratan categorías especiales del artículo 9 del RGPD; el Cliente se compromete a no incorporarlas.

Operaciones: alojamiento y conservación; gestión de proyectos, cursos, participantes, docentes, tareas, hitos, documentos y calendario; seguimiento de facturación; lectura y estructuración de currículums con inteligencia artificial (opcional, con credenciales del Cliente); envío de correos de servicio; y soporte.

Funciones que envían datos a inteligencia artificial o lectura documental (solo si el Cliente las activa con su clave):

Función · Datos enviados · Minimización
Lectura y estructuración del CV de un docente · El documento de CV (PDF/DOCX) que sube el Cliente · Se envía únicamente el documento indicado, a los proveedores que el Cliente ha configurado con su propia clave; el contenido se trata como fuente no confiable y no se usa para entrenamiento

Duración y ubicación: la del servicio; Espacio Económico Europeo (los proveedores de IA/lectura documental con credenciales del Cliente, según las condiciones que el propio Cliente contrate).

Anexo II. Medidas técnicas y organizativas

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

Control de acceso

[X] Contraseñas cifradas con scrypt y salt aleatorio por usuario.
[X] Verificación en dos pasos (TOTP) disponible para todos los usuarios.
[X] Límite de peticiones y bloqueo temporal tras intentos fallidos de inicio de sesión.
[X] Sesión con caducidad y revocación inmediata del acceso al desactivar un usuario.
[X] Permisos por rol y por capacidades dentro de cada cliente.

Aislamiento entre clientes

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

Cifrado

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

Acceso del personal del Proveedor

[X] Acceso al contenido del Cliente solo para soporte, incidencias u obligación legal, limitado a lo imprescindible.
[ ] Registro a prueba de alteraciones de las operaciones de administración.

Trazabilidad

[X] Registro de inicios de sesión y de accesos a los proyectos, consultable por el administrador del Cliente.
[X] Registro de actividad sobre los datos (altas, cambios de estado, documentos).

Seguridad de la aplicación

[X] Cabeceras de seguridad (HSTS, X-Frame-Options DENY) y Content-Security-Policy.
[X] Aislamiento del contenido no confiable en las peticiones a la inteligencia artificial y marcado frente a inyección de instrucciones.
[X] Endpoints de IA fijos (sin SSRF) y límites de consumo por petición.
[X] Monitorización de errores en servidor sin datos personales; grabación de sesión en el navegador con todo el texto enmascarado.

Continuidad y organización

[X] Copia de seguridad gestionada por el proveedor de alojamiento en el EEE.
[ ] Pruebas periódicas de restauración documentadas.
[X] Compromisos de confidencialidad del personal.