ACUERDO DE ENCARGADO DEL TRATAMIENTO (DPA)

Conforme al Articulo 28 del Reglamento General de Proteccion de Datos (UE 2016/679)

PARTES

RESPONSABLE DEL TRATAMIENTO (en adelante, "el Responsable"): El cliente usuario de Gestoria Lite que, en el ejercicio de su actividad profesional como gestoria o asesoria, determina los fines y medios del tratamiento de datos personales de sus propios clientes.

ENCARGADO DEL TRATAMIENTO (en adelante, "el Encargado"):

Campo	Valor
Denominacion	Gestoria Lite
Titular	Yevhen Klymenko
NIF	Z0424973F
Direccion	Carrer Sant Antoni 68, 1-2, Calella, Barcelona, 08370
Email	legal@gestorialite.com
Web	www.gestorialite.com

1. OBJETO DEL ACUERDO

El presente acuerdo tiene por objeto regular las condiciones en las que el Encargado tratara datos personales por cuenta del Responsable, en el marco de la prestacion del servicio de gestion documental a traves de la plataforma Gestoria Lite.

2. NATURALEZA Y FINALIDAD DEL TRATAMIENTO

Aspecto	Descripcion
Servicio	Plataforma SaaS de gestion documental para gestorias
Finalidad	Almacenamiento, organizacion y gestion de documentos fiscales y administrativos de los clientes del Responsable

Aspecto	Descripcion
Duracion	Mientras el Responsable mantenga activa su cuenta en la plataforma
Tipo de tratamiento	Almacenamiento, organizacion, consulta, transmision (notificaciones), supresion

---

3. TIPOS DE DATOS PERSONALES TRATADOS

Datos personales de los clientes del Responsable:

- **Datos identificativos:** nombre, email, telefono, identificador fiscal (NIE, CIF, DNI)
- **Datos de clasificacion:** tipo de cliente (autonomo, empresa, particular), estado
- **Documentos:** documentos fiscales y administrativos subidos a la plataforma (NIE, contratos, facturas, modelos tributarios, certificados, etc.)
- **Datos de gestion:** notas, checklists asignados, estado de documentos, plazos

---

4. CATEGORIAS DE INTERESADOS

- Clientes del Responsable: autonomos, empresas y particulares que reciben servicios de gestoria/asesoria

---

5. OBLIGACIONES DEL ENCARGADO

El Encargado se compromete a:

5.1 Instrucciones del Responsable

- Tratar los datos personales unicamente siguiendo las instrucciones documentadas del Responsable
- No utilizar los datos para finalidades propias ni cederlos a terceros salvo obligacion legal
- Informar al Responsable si considera que alguna instruccion infringe el RGPD

5.2 Confidencialidad

- Garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad
- Limitar el acceso a los datos al personal estrictamente necesario

5.3 Medidas de seguridad (Art. 32 RGPD)

El Encargado implementa las siguientes medidas tecnicas y organizativas:

Categoria	Medida implementada
Cifrado en transito	TLS 1.3 / HTTPS con HSTS (1 ano, preload)
Cifrado en reposo	AES-256 (Cloudflare R2)
Control de acceso	Autenticacion passwordless (magic link), JWT, RBAC (OWNER/GESTOR)
Aislamiento de datos	Separacion logica por gestoriaId; cada gestoria solo accede a sus datos
Validacion de entrada	class-validator, whitelist, validacion magic bytes en archivos
Cabeceras de seguridad	Helmet (CSP, X-Frame-Options: DENY, HSTS, nosniff)
Rate limiting	Proteccion contra fuerza bruta (3-10 req/min por IP)
Auditoria	Registro inmutable de todas las acciones (triggers PostgreSQL impiden modificacion)
Seguridad de archivos	Whitelist MIME, magic bytes, limite 10MB, URLs prefirmadas (1h)
Seguridad de pagos	Delegado integramente a Stripe (PCI DSS Level 1)

5.4 Subencargados

El Encargado utiliza los siguientes subencargados del tratamiento:

Subencargado	Servicio	Ubicacion	Garantias
Google Ireland Ltd	Analitica web (GA4) y medicion de conversiones (Google Ads)	UE (con posible transferencia a EE.UU.)	RGPD, EU-US Data Privacy Framework, Google Consent Mode v2
Cloudflare Inc.	Almacenamiento de documentos (R2)	UE	Clausulas contractuales tipo, cifrado AES-256
Resend Inc.	Email transaccional	EE.UU.	RGPD, Clausulas Contractuales Tipo (SCC)

Subencargado	Servicio	Ubicacion	Garantias
Render Inc.	Hosting de aplicacion	UE	RGPD, aislamiento de contenedores
Stripe Inc.	Procesamiento de pagos	UE (SCC)	PCI DSS Level 1, RGPD

El Encargado se compromete a: - Informar al Responsable de cualquier cambio en los subencargados - Garantizar que los subencargados ofrezcan garantias suficientes (Art. 28.4 RGPD) - Formalizar contratos con los subencargados que impongan las mismas obligaciones

5.5 Asistencia al Responsable

El Encargado asistira al Responsable en: - La atencion de solicitudes de ejercicio de derechos de los interesados (acceso, rectificacion, supresion, portabilidad, oposicion, limitacion) - El cumplimiento de las obligaciones de los articulos 32 a 36 del RGPD (seguridad, notificacion de brechas, evaluaciones de impacto) - La realizacion de auditorias o inspecciones por parte del Responsable o un auditor designado

5.6 Notificacion de brechas

El Encargado notificara al Responsable sin dilacion indebida cualquier brecha de seguridad que afecte a datos personales tratados por su cuenta, proporcionando: - Naturaleza de la brecha - Categorias y numero aproximado de interesados afectados - Consecuencias probables - Medidas adoptadas o propuestas

---

6. OBLIGACIONES DEL RESPONSABLE

El Responsable se compromete a: - Garantizar que tiene base juridica para el tratamiento de los datos de sus clientes - Informar a sus clientes sobre el tratamiento de datos conforme al RGPD - Proporcionar instrucciones licitas al Encargado - Cumplir con sus obligaciones como Responsable del Tratamiento

---

7. DESTINO DE LOS DATOS AL FINALIZAR EL SERVICIO

A la finalizacion de la relacion contractual, el Encargado:

1. **A eleccion del Responsable:**
   - Devolvera los datos mediante la funcion de exportacion (JSON) disponible en Ajustes > Cuenta > Exportar datos

- O suprimira todos los datos mediante la funcion de eliminacion de cuenta (cascada completa incluyendo documentos en S3)

2. **Plazos:**
   - Los datos permaneceran disponibles 30 dias tras la cancelacion de la suscripcion
   - Transcurrido ese plazo, se procedera a la eliminacion definitiva
   - Las obligaciones de retencion legal (fiscal) prevaleceran cuando apliquen (maximo 5 anos)
3. **Certificacion:**
   - La eliminacion queda registrada en el audit log con referencia “GDPR Article 17 - Right to erasure”

---

8. TRANSFERENCIAS INTERNACIONALES

Se realizan las siguientes transferencias de datos personales fuera del Espacio Economico Europeo (EEE):

Subencargado	Pais	Base juridica de la transferencia
Google Ireland Ltd	EE.UU. (posible)	EU-US Data Privacy Framework (Decision de adecuacion de la Comision Europea de 10/07/2023)
Resend Inc.	EE.UU.	Clausulas Contractuales Tipo (SCC) - Decision de Ejecucion (UE) 2021/914
Stripe Inc.	EE.UU.	Clausulas Contractuales Tipo (SCC) - Decision de Ejecucion (UE) 2021/914

Los demas subencargados (Cloudflare R2, Render) operan integramente dentro de la Union Europea. Todos los subencargados mantienen las garantias adecuadas previstas en el articulo 46 del RGPD.

---

9. DURACION Y VIGENCIA

Este acuerdo entra en vigor en el momento del registro del Responsable en la plataforma y permanece vigente mientras dure la relacion contractual. Las obligaciones de confidencialidad y seguridad sobreviven a la terminacion del acuerdo.

---

10. LEGISLACION APLICABLE Y JURISDICCION

Este acuerdo se rige por: - Reglamento (UE) 2016/679 (RGPD) - Ley Organica 3/2018 (LOPDGDD) - Legislacion espanola aplicable

Para cualquier controversia, las partes se someten a los Juzgados y Tribunales de Barcelona.

---

11. CONTACTO

Para cualquier cuestion relacionada con este acuerdo: - **Email:** legal@gestorialite.com - **Privacidad:** privacidad@gestorialite.com