

SKAILON

ACUERDO DE ENCARGO DE TRATAMIENTO

Data Processing Agreement (DPA) · Artículo 28 RGPD

Incorporado por referencia a los Términos de Servicio de Skailon

entre el Cliente (Responsable) y

ЕЙ АЙ СИСТЕМИ ЕООД (AI SYSTEMS EOOD) — Encargado

Versión 1.1 · En vigor desde el 21 de julio de 2026 · Ref. DPA-SKAILON-v1.1

Documento estándar de aceptación electrónica (art. 28.9 RGPD). Entidad: ЕЙ АЙ СИСТЕМИ ЕООД, ЕИК 208733960, IVA BG208733960, ул. Grigor Cheshmedzhiev No. 29, vh. A, et. 5, ap. 25A, 1404 Sofía, Bulgaria.

Partes y aceptación

El presente Acuerdo de Encargo de Tratamiento (el “Acuerdo”) se celebra entre **ЕЙ АЙ СИСТЕМИ ЕООД (AI SYSTEMS EOOD)**, sociedad búlgara con EIK 208733960 e IVA BG208733960, domicilio en ul. Grigor Cheshmedzhiev No. 29, vh. A, et. 5, ap. 25A, 1404 Sofía (Bulgaria), que opera comercialmente como “**Skailon**” (el “Encargado”), y **la persona jurídica que acepta los Términos de Servicio de Skailon** (el “Cliente” o “Responsable”), identificada mediante su cuenta y el registro de aceptación. No se requiere firma manuscrita ni la cumplimentación de datos en este documento: la identidad del Cliente se acredita por dicho registro.

Al marcar la casilla de aceptación durante el registro, el Cliente — a través de la persona que declara estar autorizada para obligarle — celebra el presente Acuerdo. Ello constituye la perfección del contrato de encargo **por escrito en formato electrónico** conforme al artículo 28.9 del RGPD. El Encargado conserva un registro de la aceptación que incluye la identidad de la cuenta, la fecha y hora, la dirección IP y la versión (con su huella/hash) de los documentos aceptados.

Exponen

- I. Que el Cliente ha contratado los servicios de Skailon para la gestión y automatización de comunicaciones comerciales omnicanal (WhatsApp, Instagram, Facebook, correo electrónico y voz) mediante agentes conversacionales basados en inteligencia artificial (el “Servicio”).
- II. Que la prestación del Servicio implica el tratamiento, por parte del Encargado y por cuenta del Cliente, de datos personales cuya responsabilidad corresponde al Cliente.
- III. Que, en cumplimiento del artículo 28 del RGPD, las partes regulan dicho encargo mediante el presente Acuerdo.

Cláusulas

1. Objeto y definiciones

1. El presente Acuerdo regula el tratamiento de datos personales que el Encargado realiza por cuenta del Cliente para la prestación del Servicio. El objeto, la naturaleza y la finalidad del tratamiento, los tipos de datos y las categorías de interesados se detallan en el **Anexo I**.
2. Los términos “datos personales”, “tratamiento”, “responsable”, “encargado”, “interesado” y “violación de la seguridad” se interpretarán conforme al artículo 4 del RGPD. “Normativa aplicable” comprende el RGPD, la Ley Orgánica 3/2018 (LOPDGDD), la Ley 34/2002 (LSSI-CE) y demás normativa de la Unión y de los Estados miembros aplicable en materia de protección de datos y comunicaciones electrónicas.

2. Duración

3. El Acuerdo entra en vigor con la aceptación y permanece vigente mientras se preste el Servicio. Finalizada la relación, subsisten las obligaciones de devolución o supresión (cláusula 12) y de confidencialidad, sin límite temporal.

3. Tratamiento según instrucciones documentadas

4. El Encargado tratará los datos personales únicamente siguiendo instrucciones documentadas del Cliente, incluidas las relativas a transferencias internacionales, salvo obligación legal, en cuyo caso informará al Cliente antes del tratamiento, salvo prohibición legal. Se consideran instrucciones iniciales las contenidas en este Acuerdo y en los Términos de Servicio.
5. El Encargado no tratará los datos para fines propios ni distintos de los instruidos y, en particular, **no utilizará los datos de los interesados para entrenar modelos de inteligencia artificial**. Informará al Cliente si, en su opinión, una instrucción infringe la Normativa aplicable, pudiendo suspenderla hasta su confirmación.

4. Confidencialidad

6. El Encargado garantizará que las personas autorizadas para tratar los datos se hayan comprometido a la confidencialidad o estén sujetas a una obligación de confidencialidad, aplicando el principio de mínimo privilegio. Esta obligación subsiste tras la finalización del Acuerdo.

5. Medidas de seguridad

7. El Encargado aplicará las medidas técnicas y organizativas apropiadas conforme al artículo 32 del RGPD, descritas en el **Anexo III**, y evaluará periódicamente su eficacia.

6. Subencargados

8. El Cliente autoriza con carácter general al Encargado a recurrir a los subencargados relacionados en el **Anexo II** y en la página actualizada skailon.com/legal/subprocesadores. El Encargado impondrá a cada subencargado obligaciones equivalentes en materia de protección de datos y responderá de su actuación.
9. El Encargado notificará cualquier cambio de subencargados con una antelación mínima de **30 días**, pudiendo el Cliente oponerse por motivos razonables de protección de datos y, de no resolverse, resolver la parte del Servicio afectada.

7. Transferencias internacionales

10. El tratamiento se realiza con carácter general en la Unión Europea. Cuando implique transferencia a un tercer país (por el uso de proveedores de IA con establecimiento en EE. UU.), el Encargado la amparará en un mecanismo válido del Capítulo V del RGPD: decisión de adecuación, Cláusulas Contractuales Tipo (SCC) de la Decisión (UE) 2021/914 con evaluación de impacto de la transferencia, o adhesión al EU-US Data Privacy Framework. El Anexo II identifica la ubicación y el mecanismo por subencargado.

8. Asistencia en los derechos de los interesados

11. El Encargado asistirá al Cliente, mediante medidas técnicas y organizativas apropiadas, para atender las solicitudes de los interesados (arts. 15 a 22 RGPD). Si recibe una solicitud directamente, no la responderá y la trasladará al Cliente en un máximo de **3 días hábiles**. El Encargado facilita funcionalidades de exportación en formato estructurado y de supresión efectiva.

9. Asistencia en seguridad, evaluaciones de impacto y consultas previas

12. El Encargado asistirá al Cliente en el cumplimiento de los artículos 32 a 36 del RGPD, teniendo en cuenta la naturaleza del tratamiento y la información de que disponga.

10. Notificación de violaciones de seguridad

13. El Encargado notificará al Cliente, sin dilación indebida y a más tardar en **48 horas** desde que tenga conocimiento de una violación de seguridad, para que el Cliente pueda cumplir el plazo de 72 horas del artículo 33. La notificación describirá la naturaleza, categorías y número aproximado de interesados y registros afectados, consecuencias y medidas adoptadas.

11. Auditoría e información

14. El Encargado pondrá a disposición del Cliente la información necesaria para demostrar el cumplimiento del artículo 28 y permitirá auditorías con preaviso de al menos **30 días naturales**, con un máximo de una al año — salvo requerimiento de una autoridad de control o incidente grave —, sin comprometer la seguridad ni la confidencialidad de otros clientes, y admitiéndose certificaciones o informes de terceros independientes.

12. Devolución o supresión al finalizar

15. A la finalización del Servicio, a elección del Cliente, el Encargado devolverá o suprimirá todos los datos personales y sus copias, salvo obligación legal de conservación. La supresión abarca bases de datos, índices vectoriales, registros, transcripciones y almacenamiento de media; las copias de seguridad se purgan en el siguiente ciclo de rotación. El Encargado certificará la supresión dentro de **30 días**.

13. Datos anonimizados y agregados

16. El Encargado podrá generar y utilizar datos **anonimizados de forma irreversible y agregados**, que no permitan identificar ni singularizar a ningún interesado, con la finalidad de operar, mantener y mejorar el Servicio. Tales datos, al no ser datos personales, quedan fuera del ámbito del presente Acuerdo. El Encargado no revertirá la anonimización ni la combinará con otros datos para reidentificar a los interesados.

14. Responsabilidad e indemnidad

17. Cada parte responderá de los daños causados por el incumplimiento de las obligaciones que la Normativa aplicable y este Acuerdo le atribuyen. Todo límite de responsabilidad pactado en los Términos de Servicio se aplica **entre las partes**, sin excluir la responsabilidad directa frente a los interesados o las autoridades de control conforme al artículo 82 del RGPD.
18. El Cliente mantendrá indemne al Encargado frente a reclamaciones, sanciones o daños derivados del incumplimiento de sus garantías conforme a la cláusula 15, en particular la falta de base jurídica, de consentimiento o de la información debida a los interesados.

15. Obligaciones y garantías del Responsable

19. El Cliente actúa como responsable del tratamiento, determina sus fines y medios y garantiza disponer de una base jurídica válida (art. 6 RGPD) para cada tratamiento que instruya.
20. El Cliente garantiza haber obtenido, cuando resulte necesario, el consentimiento de los interesados — en particular el exigido por el artículo 21 de la LSSI-CE y las normas equivalentes sobre comunicaciones comerciales electrónicas en otros países — y ser capaz de acreditarlo. El Encargado facilita los medios técnicos para registrar y conservar dicha prueba.
21. El Cliente facilitará a los interesados la información exigida por los artículos 13 y 14 del RGPD, incluida la relativa al uso de los canales y a la intervención del Encargado.
22. El Cliente se abstendrá de introducir por los canales datos de categorías especiales (art. 9 RGPD) salvo base reforzada y comunicación previa al Encargado.

16. Transparencia del sistema de IA (Reglamento de IA)

23. El Servicio se presta mediante un sistema de inteligencia artificial. El Encargado, en su condición de **proveedor** del sistema, lo diseña de modo que informe al interesado de que interactúa con una IA, conforme al artículo 50 del Reglamento (UE) 2024/1689. El Cliente, en su condición de **desplegador**, se obliga a no desactivar ni alterar dicha divulgación y a cumplir las obligaciones que le correspondan como desplegador.

17. Legislación aplicable y jurisdicción

24. El Acuerdo se rige por el Derecho de la Unión Europea y por el Derecho de la República de Bulgaria. Para cualquier controversia, las partes se someten a los juzgados y tribunales competentes de la ciudad de Sofía (Bulgaria), sin perjuicio de la competencia imperativa de las autoridades de control y de los tribunales que correspondan conforme al RGPD.

La aceptación de este Acuerdo se produce por medios electrónicos conforme a la sección “Partes y aceptación”; no requiere firma manuscrita. La constancia de la aceptación (cuenta, fecha y hora, IP y versión) obra en los registros del Encargado.

Anexo I — Descripción del tratamiento

Objeto	Gestión y automatización de comunicaciones comerciales y de atención por cuenta del Cliente mediante agentes conversacionales de IA (Skailon).
Naturaleza y finalidad	Recepción, procesamiento y respuesta autónoma de mensajes; cualificación y seguimiento de leads; agendado de citas; transcripción y análisis; gestión del embudo comercial; registro de auditoría; sincronización con los sistemas del Cliente.
Duración	Mientras dure el Servicio, conforme a los periodos de retención del Anexo III.
Categorías de interesados	Leads, clientes potenciales y clientes del Cliente que interactúan por los canales gestionados.
Categorías de datos	Identificativos y de contacto (nombre, teléfono, usuario de red social, correo); identidades vinculadas entre canales; contenido de conversaciones (texto, audio/notas de voz, imágenes) y transcripciones; metadatos de mensajería; datos derivados (etiquetas, cualificación, etapa del embudo, resúmenes, vectores/embeddings); origen/atribución; citas; registros de consentimiento; registro de auditoría.
Categorías especiales (art. 9)	No previstas. El Cliente se obliga a no introducirlas sin base reforzada y aviso previo.

Anexo II — Subencargados autorizados

Lista vigente a la fecha de esta versión. La versión actualizada se publica en skailon.com/legal/subprocesadores.

Subencargado	Finalidad	Ubicación del tratamiento	Transferencia
Supabase, Inc.	Base de datos (PostgreSQL) y almacenamiento (media)	Alemania — eu-central-1 (UE)	UE; SCC para eventual soporte desde EE. UU.
Upstash, Inc.	Cola y caché (Redis / BullMQ)	Alemania — eu-central-1, sin réplicas fuera de la UE	UE; SCC para eventual soporte desde EE. UU.
Anthropic, PBC	Modelos de lenguaje (generación y clasificación)	EE. UU.	SCC + TIA / DPF; no-entrenamiento; retención mínima
Microsoft (Azure — Speech + Translator)	Transcripción de audio y traducción	UE — North Europe (Irlanda)	UE; SCC/DPF de Microsoft
Meta Platforms Ireland Ltd.	Canal de mensajería (WhatsApp, Instagram, Facebook)	Irlanda (UE) / EE. UU.	Adecuación (IE) + SCC/DPF; términos de WhatsApp Business

Exclusiones: Stripe procesa datos de facturación del Cliente-negocio (relación en la que el Encargado es responsable), no datos de los interesados. El único tratamiento de contenido fuera de la UE corresponde a Anthropic (EE. UU.), amparado por SCC/TIA.

Anexo III — Medidas técnicas y organizativas de seguridad

A. Control de acceso e identidad

- Autenticación individual con MFA para accesos administrativos; control de acceso por roles (RBAC) y mínimo privilegio; aislamiento por cliente (multi-tenant).
- Registro y revisión periódica de accesos; revocación inmediata al cesar la relación con el personal.

B. Cifrado y protección de datos

- En tránsito: TLS 1.2 o superior en todas las comunicaciones y en todos los subencargados.
- En reposo: base de datos principal (Supabase) cifrada con AES-256; Azure con cifrado por defecto. La cola/caché (Upstash) opera con TLS en tránsito y con minimización de datos personales en los payloads; el cifrado en reposo de la cola se activa mediante el plan Prod Pack del proveedor.
- Gestión segura de secretos y credenciales (almacén de secretos, rotación).

C. Infraestructura y disponibilidad

- Alojamiento en la UE (Alemania — Frankfurt); transcripción/traducción en la UE (Azure North Europe, Irlanda); copias de seguridad cifradas con pruebas de restauración y política de retención definida.
- Monitorización, registro de eventos y capacidad de detección de incidentes.

D. Tratamiento por IA

- Minimización de datos enviados a los modelos; compromiso contractual de no-entrenamiento y retención mínima con el proveedor; prohibición de proveedores fuera de política en producción.
- Registro probatorio del consentimiento (marca temporal, texto y canal) en almacén separado del historial.

E. Medidas organizativas

- Confidencialidad del personal; Registro de Actividades de Tratamiento (art. 30) actualizado; procedimientos de brechas y de derechos; formación básica.

F. Periodos de conservación

Tipo de dato	Periodo
Contenido de conversaciones (incl. transcripciones)	24 meses tras la última actividad del lead (default configurable por el Cliente)
Audio/notas de voz (crudo)	Supresión tras la transcripción (buffer breve para reprocesar)
Imágenes entrantes	90 días tras el cierre de la conversación
Vectores/embeddings derivados	Se purgan con la conversación de origen
Registro de auditoría (append-only)	24 meses (PII redactada de inmediato en caso de supresión)
Registros de consentimiento	Vigencia de la relación + 3 años como prueba
Copias de seguridad	Purga en el siguiente ciclo de rotación (30 días)

Los plazos de datos de leads son valores por defecto que el Cliente, como responsable, puede ajustar mediante instrucción documentada.