

S K A I L O N

ACUERDO DE ENCARGO DE TRATAMIENTO

Acuerdo de Encargo de Tratamiento de Skailon · versión 1.2

Encargado del tratamiento: ЕЙ АЙ СИСТЕМИ ЕООД (AI SYSTEMS EOOD), sociedad unipersonal de responsabilidad limitada constituida en Bulgaria, que opera comercialmente como «Skailon». EIK 208733960 · IVA BG208733960 · ul. Grigor Cheshmedzhiev No. 29, vh. A, et. 5, ap. 25A, 1404 Sofía (Bulgaria) · hola@skailon.com.

Responsable del tratamiento: el Cliente que acepta los Términos de Servicio de Skailon, identificado mediante su Cuenta y el registro de aceptación.

Versión 1.2 · Ref. DPA-SKAILON-v1.2. Para las altas nuevas, en vigor desde el 20 de octubre de 2026. Para quienes ya eran Clientes, desde el 20 de noviembre de 2026, conforme a la cláusula 19 de los Términos. Documento estándar de aceptación electrónica (artículo 28.9 del RGPD).

Partes y aceptación

Este Acuerdo de Encargo de Tratamiento (el «Acuerdo») se celebra entre ЕЙ АЙ СИСТЕМИ ЕООД (AI SYSTEMS EOOD) (el «Encargado») y la persona jurídica o el profesional que acepta los Términos de Servicio de Skailon (el «Cliente» o «Responsable»), identificado mediante su Cuenta y el registro de aceptación. No se requiere firma manuscrita.

Al marcar la casilla de aceptación durante el registro, o al aceptar una nueva versión desde el panel, el Cliente, a través de la persona que declara estar autorizada para obligarle, celebra este Acuerdo. Ello perfecciona el contrato de encargo por escrito en formato electrónico conforme al artículo 28.9 del RGPD. El Encargado conserva un registro de la aceptación con la identidad de la Cuenta, la fecha y hora, la dirección IP y la versión de los documentos aceptados, con su huella (hash). Las versiones posteriores se aceptan conforme a la cláusula 19 de los Términos.

Exponen

Que el Cliente ha contratado Skailon para gestionar y automatizar sus comunicaciones comerciales y de atención por WhatsApp, Instagram, Facebook, correo electrónico, SMS y llamadas, mediante agentes conversacionales de inteligencia artificial (el «Servicio»).

Que la prestación del Servicio implica que el Encargado trate, por cuenta del Cliente, datos personales cuya responsabilidad corresponde al Cliente.

Que, en cumplimiento del artículo 28 del RGPD, las partes regulan ese encargo mediante este Acuerdo.

Cláusulas

1. Objeto y definiciones

Este Acuerdo regula el tratamiento de datos personales que el Encargado realiza por cuenta del Cliente para prestar el 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.

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 normativa búlgara de protección de datos, 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

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

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 que la ley lo prohíba. Son instrucciones del Cliente las contenidas en este Acuerdo y en los Términos de Servicio, y las que da mediante la configuración del Servicio.

El Servicio es estándar e igual para todos los clientes, y el Encargado no suscribe anexos ni acuerdos individuales. Si el Cliente necesita una instrucción que el Servicio estándar no permite ejecutar, el Encargado se lo comunicará y el Cliente podrá resolver este Acuerdo y los Términos sin penalización.

El Encargado no tratará los datos para fines propios ni distintos de los instruidos y, en particular, no los utilizará para entrenar modelos de inteligencia artificial. Informará al Cliente si, en su opinión, una instrucción infringe la Normativa aplicable, y podrá suspenderla hasta que el Cliente la confirme o la modifique.

4. Confidencialidad

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

5. Medidas de seguridad

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

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 de protección de datos equivalentes a las de este Acuerdo y responderá de su actuación.

El Encargado notificará por correo electrónico al administrador de la Cuenta cualquier incorporación o sustitución de subencargados con una antelación mínima de 30 días. El Cliente podrá oponerse por motivos razonables de protección de datos y, si no se resuelve, resolver la parte del Servicio afectada, con la devolución del saldo no consumido prevista en la cláusula 7 de los Términos.

7. Transferencias internacionales

Los datos se alojan en la Unión Europea. Fuera de ella tratan contenido Anthropic (el texto que se envía a los modelos de IA), Telnyx (llamadas y SMS, solo si el Cliente usa esos canales) y Resend (los correos del Servicio, que pueden incluir el nombre de un interesado). Además, varios subencargados con sede en EE. UU. pueden acceder a los datos desde allí para prestar soporte. Cuando haya transferencia a un tercer país, el Encargado la amparará en un mecanismo válido del Capítulo V del RGPD: una decisión de adecuación, incluida la adhesión del proveedor al Marco de Privacidad de Datos UE-EE. UU., o las cláusulas contractuales tipo de la Decisión (UE) 2021/914, con evaluación del impacto de la transferencia. El Anexo II identifica la ubicación, la sede y el mecanismo de cada subencargado.

8. Asistencia en los derechos de los interesados

El Encargado asistirá al Cliente, mediante medidas técnicas y organizativas apropiadas, para atender las solicitudes de los interesados (artículos 15 a 22 del RGPD). Si recibe una solicitud directamente, no la responderá y la trasladará al Cliente en un máximo de 3 días hábiles.

El Encargado pone a disposición del Cliente funciones para consultar, rectificar y eliminar contactos y para exportar la lista de contactos. La exportación completa de un interesado y su supresión definitiva, con certificado si se pide, las ejecuta el Encargado a petición del Cliente en un máximo de 10 días.

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

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. En particular, le facilitará la información necesaria para la evaluación de impacto cuando el Cliente trate categorías especiales de datos (cláusula 18).

10. Notificación de violaciones de seguridad

El Encargado notificará al Cliente cualquier violación de la seguridad de los datos tratados por su cuenta sin dilación indebida y, a más tardar, en 48 horas desde que tenga conocimiento de ella, para que el Cliente pueda cumplir el plazo de 72 horas del artículo 33 del RGPD. La notificación describirá la naturaleza de la violación, las categorías y el número aproximado de interesados y de registros afectados, sus posibles consecuencias y

las medidas adoptadas o propuestas. Si no es posible facilitar toda la información a la vez, se facilitará por fases. El Encargado gestiona las violaciones conforme a un procedimiento interno y las documenta en un registro.

11. Auditoría e información

El Encargado pondrá a disposición del Cliente la información necesaria para demostrar el cumplimiento del artículo 28 del RGPD y permitirá auditorías con un preaviso de al menos 30 días naturales, con un máximo de una al año, salvo requerimiento de una autoridad de control o incidente grave. Las auditorías no podrán comprometer la seguridad ni la confidencialidad de otros clientes, y se admitirán certificaciones o informes de terceros independientes.

12. Fin del Servicio: devolución y supresión

12.1 Suspensión y terminación. La suspensión del Servicio no pone en marcha los plazos de esta cláusula. Los plazos corren desde la terminación del Servicio por cualquier causa: la baja del Cliente o la resolución del contrato, incluida la resolución por impago (cláusula 18 de los Términos). Durante una suspensión por impago, el Encargado sigue recibiendo y guardando los mensajes de los interesados y atiende por correo las instrucciones del Cliente sobre sus datos. Una Cuenta sin Suscripción se considera terminada tras 60 días sin que nadie la use.

12.2 Devolución. Terminado el Servicio, el Cliente dispone de al menos 30 días para pedir la devolución de sus datos, en los formatos de la cláusula 8 bis de los Términos. Si el Cliente ha pedido cambiar de proveedor, se aplican los plazos de esa cláusula.

12.3 Avisos. El Encargado avisará al administrador de la Cuenta al empezar el plazo y, si quedan más de 7 días, también cuando falten 7, indicando en cada aviso la fecha de supresión.

12.4 Supresión. Vencido el plazo, el Encargado suprimirá todos los datos personales tratados por cuenta del Cliente y sus copias, salvo que el Derecho de la Unión o de un Estado miembro exija conservarlos. La supresión abarca las bases de datos, los registros, las transcripciones y el almacenamiento de archivos. Las copias de seguridad se sobrescriben en su ciclo de rotación, en un máximo de 30 días adicionales, los registros técnicos de errores caducan solos a los 30 días y los del servidor, a los 7. Si el Cliente lo pide, el Encargado certificará la supresión.

13. Datos anonimizados y agregados

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

Se exceptúan los datos obtenidos a través de las plataformas de Meta (WhatsApp, Instagram y Facebook), incluidos los anonimizados, agregados o derivados: el Encargado solo los trata para prestar el Servicio al Cliente.

14. Responsabilidad e indemnidad

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, salvo en caso de dolo o culpa grave, y no excluye la responsabilidad directa frente a los interesados o las autoridades de control conforme al artículo 82 del RGPD.

El Cliente mantendrá indemne al Encargado frente a reclamaciones, sanciones o daños derivados del incumplimiento de sus garantías de las cláusulas 15 y 18, en particular la falta de base jurídica, de consentimiento o de la información debida a los interesados.

15. Obligaciones y garantías del Responsable

El Cliente actúa como responsable del tratamiento, determina sus fines y sus medios esenciales y garantiza disponer de una base jurídica válida (artículo 6 del RGPD) para cada tratamiento que instruya.

El Cliente garantiza haber obtenido, cuando sea 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 de otros países, y poder acreditarlo. El Encargado facilita los medios técnicos para registrar y conservar esa prueba.

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, a la intervención del Encargado y al uso de inteligencia artificial.

El Cliente no introducirá por los canales datos de categorías especiales (artículo 9 del RGPD) salvo en los términos de la cláusula 18.

16. Transparencia del sistema de IA

La transparencia del sistema de IA frente a los interesados se regula en la cláusula 11 de los Términos de Servicio. No es una instrucción de tratamiento de datos y, por eso, no forma parte de este Acuerdo.

17. Legislación aplicable y jurisdicción

Este Acuerdo se rige 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.

18. Datos de salud y otras categorías especiales

18.1 Servicio estándar. Esta cláusula se aplica por igual a todo Cliente que trate categorías especiales de datos a través del Servicio, que es estándar e igual para todos (cláusula 3).

18.2 Decisión y garantías del Cliente. Tratar datos relativos a la salud u otras categorías especiales (artículo 9 del RGPD) a través del Servicio es una decisión exclusiva del Cliente. Antes de hacerlo, el Cliente lo declarará en la opción habilitada en el panel (Ajustes › Cumplimiento), y solo podrá retirar la declaración cuando deje de tratar esos datos a través del Servicio. Además, garantiza que:

- a) dispone de una excepción válida del artículo 9.2 y de una base jurídica del artículo 6 del RGPD;
- b) ha realizado, cuando proceda, la evaluación de impacto (artículo 35) y, en su caso, la consulta previa (artículo 36);
- c) ha informado a los interesados conforme a los artículos 13 y 14, incluida la intervención del Encargado y el uso de inteligencia artificial;
- d) ha designado delegado de protección de datos cuando sea obligatorio;
- e) limita los datos a los estrictamente necesarios para la finalidad y fija sus plazos de conservación;
- f) ha revisado las medidas del Anexo III y del apartado 18.3 y las considera adecuadas para su tratamiento (artículo 28.1 del RGPD).

18.3 Medidas y asistencia. El Encargado trata estos datos únicamente como parte del Servicio estándar, con los subencargados y las transferencias del Anexo II y de las cláusulas 6 y 7. Aplica las medidas del Anexo III y, mientras la declaración del apartado 18.2 esté activa, también estas:

- a) verificación en dos pasos obligatoria para todos los Usuarios de la Cuenta del Cliente;
- b) envío de conversiones a plataformas publicitarias desactivado;
- c) repetición del aviso de IA al inicio de cada sesión, conforme a la cláusula 11.2.b de los Términos.

El Encargado facilitará al Cliente la información necesaria para su evaluación de impacto (artículo 28.3.f del RGPD). El Encargado no garantiza que el Servicio sea adecuado para una finalidad sanitaria concreta.

18.4 El Servicio no es un producto sanitario. El Servicio no está diseñado ni destinado a diagnosticar, prevenir o tratar enfermedades, a priorizar clínicamente a pacientes (triaje), a clasificar o priorizar llamadas de emergencia ni a adoptar decisiones clínicas, y el Cliente no lo utilizará con esos fines. Las respuestas del sistema de IA pueden contener errores. Su supervisión, y cualquier decisión que se tome a partir de ellas, corresponden al Cliente.

18.5 Configuración e integraciones del Cliente. Corresponden exclusivamente al Cliente:

- a) la configuración de su Cuenta: instrucciones, reglas, contexto, ajustes de privacidad y la activación o desactivación de funciones, incluidas las que comunican datos a terceros, como plataformas publicitarias;
- b) los sistemas y conexiones que vincule al Servicio (fuentes, API, webhooks, servicios locales o de terceros), incluidos su seguridad, los datos que expongan o devuelvan, sus registros de acceso y las operaciones que ejecuten, también las de modificación o borrado de datos;
- c) el uso de las credenciales y claves de API de su Cuenta.

Si el Cliente configura que el sistema consulte o revele información clínica por cualquier canal, se asegurará antes de que solo la revele al propio interesado, por ejemplo limitándola al teléfono o al correo que constan en su ficha.

En la relación entre las partes, y sin perjuicio del artículo 82 del RGPD ni de la responsabilidad por dolo o culpa grave, el Encargado no responderá de los daños derivados de esas configuraciones, sistemas o usos.

18.6 Menores y representación. Cuando el tratamiento afecte a menores o a personas con representante legal, verificar la representación y decidir si se tratan sus datos corresponde al Cliente.

18.7 Conservación y fin del Servicio. Los datos se conservan según el Anexo III. Al terminar el Servicio por cualquier causa, se aplica la cláusula 12.

18.8 Responsabilidad. La cláusula 14 y los límites de responsabilidad de los Términos se aplican a esta cláusula, salvo en caso de dolo o culpa grave. El Cliente mantendrá indemne al Encargado frente a reclamaciones, sanciones o daños derivados de tratar categorías especiales sin cumplir las garantías del apartado 18.2, o de las configuraciones, sistemas y usos del apartado 18.5. Nada de lo dispuesto en esta cláusula limita los derechos de los interesados frente a cualquiera de las partes (artículo 82 del RGPD).

19. Integraciones, canales de Meta y uso de la API por el Cliente

Las integraciones que el Cliente conecta con sus propias cuentas (por ejemplo ElevenLabs, Fathom, Zoom, Google Calendar, GoHighLevel o ManyChat), sus webhooks, sus fuentes de datos y el uso que haga de la API de la Plataforma son elección y responsabilidad del Cliente. Esos servicios no son subencargados del Encargado: los datos se les envían por instrucción del Cliente y se rigen por la relación entre el Cliente y cada servicio. El Encargado no responde de las operaciones que el Cliente ejecute con ellos, incluidas las de modificación o borrado de datos. Lo mismo se aplica a los terceros a quienes el Cliente da acceso a su Cuenta, por ejemplo quien le implanta el Servicio: el Cliente les da un usuario propio, responde de lo que hagan y firma con ellos el contrato de encargo que exija el artículo 28 del RGPD. No son subencargados del Encargado.

Lo mismo se aplica a los canales de WhatsApp, Instagram y Facebook, que el Cliente conecta con sus propias cuentas de Meta: Meta trata los mensajes con las condiciones que el Cliente acepta con ella y no es subencargada del Encargado.

20. Soporte y accesos del Encargado

20.1 Canales. El soporte que implique datos de los interesados se presta desde el panel. El correo (hola@skailon.com) y el WhatsApp de soporte («Hablar con el equipo») no son canales de tratamiento de esos datos. Si el Cliente los envía por esas vías, el Encargado los trasladará al panel y los borrará de ellas.

20.2 Sesión de soporte. Para entrar en la Cuenta del Cliente, el personal del Encargado abre una sesión de soporte con motivo obligatorio y un límite de 2 horas. La sesión queda registrada con quién la abre, el motivo y las horas de entrada y de salida, y lo que el personal cambie en la Cuenta queda atribuido a «Soporte de Skailon». Mientras dura, el administrador y el director de la Cuenta ven en el panel quién ha entrado, con qué motivo y desde qué hora. Después, la sesión queda en un historial que el Cliente puede consultar en el panel.

20.3 Accesos sin sesión. Sin abrir una sesión de soporte, el personal del Encargado solo puede:

- a) ver la lista de mensajes que no se pudieron recibir o que están retenidos, con el teléfono o usuario y el nombre de quien escribió, para reintentarlos o pasarlos a la bandeja del Cliente. Solo los elimina a petición del Cliente;
- b) ejecutar las exportaciones y supresiones que pida el Cliente;
- c) conceder cortesías y crédito, sin acceder a datos de los interesados;
- d) leer los comentarios que los Usuarios envían desde el panel.

Todos estos accesos quedan en el registro interno del Encargado, que el Cliente puede pedir.

Anexo I · Descripción del tratamiento

Elemento	Descripción
Objeto	Gestión y automatización de las comunicaciones comerciales y de atención del Cliente mediante agentes conversacionales de IA (Skailon).
Naturaleza y finalidad	Recepción, procesamiento y respuesta de mensajes y llamadas, de forma autónoma o con revisión humana; cualificación y seguimiento de los leads; agendado de citas; transcripción y análisis; gestión del embudo comercial; registro de auditoría; sincronización con los sistemas del Cliente; envío de conversiones a Meta cuando el Cliente lo activa.
Duración	Mientras dure el Servicio, conforme al Anexo III.
Interesados	Leads, contactos y clientes del Cliente, y los miembros de su equipo que usan la Plataforma.
Datos	Identificativos y de contacto (nombre, teléfono, usuario de red social, correo); identidades vinculadas entre canales; contenido de las conversaciones (texto, notas de voz, imágenes, vídeo, documentos y publicaciones compartidas) y sus transcripciones; SMS; llamadas y, si el Cliente las activa, sus grabaciones y transcripciones; metadatos de mensajería; datos derivados (etiquetas, cualificación, etapa del embudo, resúmenes); origen y atribución; citas; permisos de contacto y registros de consentimiento; registro de auditoría; tramos de conexión del equipo del Cliente.
Categorías especiales (artículo 9 del RGPD)	Solo si el Cliente decide tratarlas conforme a la cláusula 18, por ejemplo datos de salud facilitados por los interesados o consultados en sistemas del Cliente.

Anexo II · Subencargados autorizados

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

Subencargado	Qué trata	Dónde están los datos	Sede	Garantía
Supabase, Inc.	Base de datos y archivos	Alemania (Fráncfort)	EE. UU.	Cláusulas tipo, para el acceso desde EE. UU.
Render	Servidores, cola y caché	Alemania (Fráncfort)	EE. UU.	Cláusulas tipo, para el acceso desde EE. UU.
Anthropic, PBC	Texto que se envía a los modelos de IA	EE. UU. u otras regiones de su infraestructura	EE. UU.	Cláusulas tipo. Sin entrenamiento; borrado en un máximo de 30 días
Microsoft (Azure Speech)	Transcripción de voz	Irlanda (North Europe)	EE. UU.	Contrato de encargo de Microsoft, con cláusulas tipo y Marco de Privacidad para el acceso desde EE. UU.
Telnyx	Llamadas y SMS, solo si el Cliente usa esos canales	EE. UU.	EE. UU.	Cláusulas tipo y Marco de Privacidad
Resend	Correos del Servicio, que pueden incluir el nombre de un interesado	EE. UU. (envío desde Irlanda)	EE. UU.	Cláusulas tipo
Sentry	Registro de errores, que caduca a los 30 días	Alemania	EE. UU.	Cláusulas tipo, para el acceso desde EE. UU.
Vercel	Alojamiento del panel; solo registros de acceso	EE. UU.	EE. UU.	Cláusulas tipo y Marco de Privacidad

Subencargado	Qué trata	Dónde están los datos	Sede	Garantía
Hostinger International Ltd.	Buzón de soporte hola@skailon.com, que no es un canal para datos de los interesados (cláusula 20)	Espacio Económico Europeo, sin concretar el país; en el correo intervienen subencargados de Hostinger con sede en EE. UU.	Chipre (UE)	Contrato de encargo de Hostinger, con cláusulas tipo para lo que salga del EEE

«Cláusulas tipo» son las de la Decisión (UE) 2021/914. «Marco de Privacidad» es el Marco de Privacidad de Datos UE–EE. UU., cuando el proveedor está adherido.

Fuera de la UE tratan contenido Anthropic, Telnyx y Resend. Supabase, Render, Microsoft y Sentry alojan los datos en la UE, pero tienen sede en EE. UU. y pueden acceder a ellos desde allí para prestar soporte. Vercel solo trata registros de acceso al panel.

No son subencargados: Meta y las integraciones que el Cliente conecta con sus propias cuentas (cláusula 19). Tampoco Stripe, Cloudflare ni Google, que tratan datos de los que el Encargado es responsable (facturación, alta, inicio de sesión y correo de soporte), no datos de los interesados.

Anexo III · Medidas técnicas y organizativas

A. Control de acceso e identidad

- Autenticación individual; control de acceso por roles y mínimo privilegio; aislamiento de cada cliente en la base de datos.
- Verificación en dos pasos obligatoria para el acceso del personal del Encargado a su panel de administración.
- En las Cuentas que han declarado datos de salud, verificación en dos pasos obligatoria para todos sus Usuarios, sin inicio de sesión con Google (cláusula 18.3).
- El personal de soporte del Encargado accede a la Cuenta del Cliente mediante una sesión de soporte con motivo, límite de 2 horas y registro, con las excepciones y el historial de la cláusula 20.
- Registro y revisión de accesos; revocación inmediata al cesar la relación con el personal.

B. Cifrado

- En tránsito: TLS 1.2 o superior en todas las comunicaciones y con todos los subencargados.
- En reposo: en la base de datos, el almacenamiento y la cola de los proveedores de infraestructura del Anexo II. Las credenciales de canal se cifran además por el Encargado (AES-256-GCM).
- Gestión segura de secretos y credenciales.

C. Infraestructura y disponibilidad

- Alojamiento en la UE (Alemania, Fráncfort); transcripción en la UE (Azure North Europe, Irlanda).
- Copias de seguridad cifradas gestionadas por el proveedor de base de datos, que se sobrescriben en su ciclo de rotación.
- Vigilancia externa de disponibilidad, alertas de mensajes no recibidos y de consumo, y un resumen diario de incidencias.

D. Tratamiento por IA

- A cada tarea se envía el contexto necesario (resumen y mensajes recientes), no el historial completo.
- Compromiso contractual del proveedor de no entrenar sus modelos con los datos; borrado de entradas y salidas en un máximo de 30 días.
- Registro probatorio de los consentimientos y permisos de contacto (fecha y hora, texto y canal).

E. Medidas organizativas

- Compromiso de confidencialidad de toda persona con acceso a los datos.
- Registro de actividades de tratamiento (artículo 30 del RGPD).
- Procedimiento de gestión de violaciones de seguridad, con registro (artículo 33.5 del RGPD).
- Procedimiento de atención de los derechos de los interesados.

F. Conservación de los datos

Tipo de dato	Conservación
Datos de los interesados tratados en el Servicio: contactos, conversaciones, transcripciones, notas de voz, imágenes y demás archivos, notas y citas	Mientras dure el Servicio o hasta que el Cliente los suprima
Datos derivados: resúmenes, transcripciones y datos extraídos	Siguen al dato del que proceden
Registro de auditoría	Mientras dure el Servicio. Si se suprime a un interesado, se eliminan del registro sus datos personales. Quedan la constancia de la supresión y la secuencia de sucesos, con identificadores internos que ya no permiten identificarle. Un texto libre que le mencione sin identificarle no se puede localizar, y así lo indica el certificado
Permisos de contacto y registros de consentimiento	Mientras dure el Servicio. Se incluyen en la devolución de datos
Al terminar el Servicio	Al menos 30 días para pedir la devolución; después, supresión (cláusula 12)
Copias de seguridad	Se sobrescriben en su ciclo de rotación, en un máximo de 30 días

Los registros técnicos de errores, que pueden contener algún dato suelto de un interesado, caducan solos a los 30 días, y los del servidor, a los 7 días. Antes de escribirse, en esos registros se ocultan los teléfonos, los correos, los nombres y el texto de los mensajes; pueden quedar identificadores internos o de plataformas, direcciones IP y algún dato suelto dentro de un texto libre. Fuera de ese caso, el Encargado no suprime datos por el mero transcurso de un plazo durante el Servicio. Corresponde al Cliente, como responsable del tratamiento, fijar los plazos de conservación de los datos de sus interesados (artículo 5.1.e del RGPD) y suprimirlos cuando proceda, con las herramientas del Servicio o pidiéndolo al Encargado, que lo ejecutará conforme a la cláusula 8.