Acuerdo de Tratamiento de Datos

Acuerdo sobre el tratamiento de datos personales por cuenta de un responsable del tratamiento de conformidad con el Art. 28 del RGPD

entre el cliente (en adelante denominado "Cliente") y CA Customer Alliance GmbH, Hausvogteipl. 12, 10117 Berlín, Alemania (en adelante denominado "Proveedor").

Por favor, envíe cualquier pregunta o comentario relacionado con este acuerdo de tratamiento de datos o la protección de datos en general a la siguiente dirección de correo electrónico: dataprotection@customer-alliance.com

1. **Objeto del Acuerdo**

En el curso de la prestación de servicios según el acuerdo de servicio (en adelante denominado "Acuerdo Principal"), es necesario que el Proveedor trate datos personales con respecto a los cuales el Cliente actúa como responsable del tratamiento en términos de la ley de protección de datos (en adelante denominados "Datos del Cliente"). Este acuerdo especifica las obligaciones y derechos de protección de datos de las partes en relación con el uso de los Datos del Cliente por parte del Proveedor para prestar los servicios bajo el Acuerdo Principal.

2. **Alcance del encargo**
    1. **El Proveedor tratará los Datos del Cliente por cuenta y de acuerdo con las instrucciones del Cliente en el sentido del Art. 28 del RGPD (Tratamiento por Encargo). El Cliente sigue siendo el responsable del tratamiento en términos de la ley de protección de datos.**
    2. **El tratamiento de los Datos del Cliente por parte del Proveedor se realiza de la manera y en el alcance y para la finalidad determinada en el Anexo 1 de este acuerdo; el tratamiento se refiere a los tipos de datos personales y categorías de interesados especificados allí. La duración del tratamiento corresponde al plazo del Acuerdo Principal.**
    3. **El tratamiento de los Datos del Cliente por parte del Proveedor se llevará a cabo en principio dentro de la Unión Europea o de otro estado contratante del Espacio Económico Europeo (EEE). No obstante, se permite al Proveedor tratar los Datos del Cliente de acuerdo con las disposiciones de este acuerdo fuera del EEE si informa con antelación al Cliente sobre el lugar de tratamiento de datos y si se cumplen los requisitos de los Arts. 44 a 48 del RGPD o si se aplica una excepción según el Art. 49 del RGPD.**
3. **Derecho del Cliente a dar instrucciones**
    1. **El Proveedor trata los Datos del Cliente de acuerdo con las instrucciones del Cliente, a menos que el Proveedor esté legalmente obligado a actuar de otro modo. En este último caso, el Proveedor informará al Cliente de ese requisito legal antes del tratamiento, a menos que esa ley prohíba tal información por razones importantes de interés público.**
    2. **Las instrucciones del Cliente están en principio estipuladas y documentadas de manera concluyente en las disposiciones de este acuerdo. Las instrucciones individuales que se desvíen de las estipulaciones de este acuerdo o que impongan requisitos adicionales requieren un acuerdo mutuo y deberán hacerse por escrito.**

3. **El Proveedor se asegurará de que los Datos del Cliente se traten de acuerdo con las instrucciones dadas por el Cliente. Si el Proveedor opina que una instrucción dada por el Cliente infringe este acuerdo o la ley de protección de datos aplicable, tiene derecho, después de informar correspondientemente al Cliente, a suspender la ejecución de la instrucción hasta que el Cliente confirme la instrucción.**

4. **Responsabilidad Legal del Cliente**
    1. **El Cliente es el único responsable de la permisibilidad del tratamiento de los Datos del Cliente y de salvaguardar los derechos de los interesados en la relación entre las partes.**
    2. **El Cliente es responsable de proporcionar al Proveedor los Datos del Cliente a tiempo para la prestación de servicios de acuerdo con el Acuerdo Principal y es responsable de la calidad de los Datos del Cliente. El Cliente informará al Proveedor inmediata y completamente si durante el examen de los resultados del Proveedor encuentra errores o irregularidades con respecto a las disposiciones de protección de datos o sus instrucciones.**
    3. **Si se requiere que el Proveedor proporcione información a un organismo gubernamental o persona sobre el tratamiento de los Datos del Cliente o que coopere con estos organismos de cualquier otra forma, el Cliente está obligado, a primera solicitud, a asistir al Proveedor en la provisión de tal información y en el cumplimiento de otras obligaciones de cooperación.**
5. **Requisitos para el personal**

El Proveedor comprometerá a todas las personas involucradas en el tratamiento de los Datos del Cliente a la confidencialidad con respecto al tratamiento de los Datos del Cliente.

6. **Seguridad del tratamiento**
    1. **El Proveedor toma, según el Art. 32 del RGPD, las medidas técnicas y organizativas necesarias y apropiadas, teniendo en cuenta el estado de la técnica, los costes de implementación y la naturaleza, alcance, circunstancias y finalidades de los Datos del Cliente, así como las diferentes probabilidades y gravedad del riesgo para los derechos y libertades de los interesados, con el fin de garantizar un nivel de protección de los Datos del Cliente adecuado al riesgo. Las medidas actuales se pueden encontrar en el Anexo 2.**
    2. **El Proveedor tendrá derecho a modificar las medidas técnicas y organizativas durante el plazo del acuerdo, siempre que continúen cumpliendo con los requisitos legales.**
7. **Contratación de otros encargados del tratamiento**
    1. El Cliente otorga al Proveedor la autorización general para contratar a otros encargados del tratamiento con respecto al tratamiento de los Datos del Cliente. Otros encargados consultados en el momento de la conclusión del acuerdo resultan del Anexo 3. En general, no se requiere autorización para las relaciones contractuales con proveedores de servicios que se ocupan del examen o mantenimiento de procedimientos o sistemas de tratamiento de datos por parte de terceros o que involucran otros servicios adicionales, incluso si no se puede excluir el acceso a los Datos del Cliente, siempre que el Proveedor tome medidas razonables para proteger la confidencialidad de los Datos del Cliente.
    2. El Proveedor notificará al Cliente cualquier cambio previsto en relación con la consulta o sustitución de otros encargados. En casos individuales, el Cliente tiene derecho a objetar la contratación de un potencial encargado adicional. Una objeción solo puede ser planteada por el Cliente por razones importantes que

deben ser demostradas al Proveedor. En la medida en que el Cliente no objete dentro de los 14 días posteriores a la recepción de la notificación, su derecho a objetar la contratación correspondiente caduca. Si el Cliente objeta, el Proveedor tiene derecho a terminar el Acuerdo Principal y este acuerdo con un período de notificación de tres (3) meses.

3. El acuerdo entre el Proveedor y el otro encargado debe imponer a este último las mismas obligaciones que incumben al Proveedor en virtud de este acuerdo. Las partes acuerdan que este requisito se cumple si el contrato tiene un nivel de protección correspondiente a este acuerdo, respectivamente si las obligaciones establecidas en el Art. 28 párr. 3 del RGPD se imponen al otro encargado.

8. **Derechos de los interesados**
    1. **El Proveedor apoyará al Cliente dentro de lo razonable en virtud de medidas técnicas y organizativas en el cumplimiento de la obligación de este último de responder a las solicitudes de ejercicio de los derechos de los interesados.**
    2. **En la medida en que un interesado presente una solicitud para el ejercicio de sus derechos directamente al Proveedor, este reenviará esta solicitud al Cliente en tiempo oportuno.**
    3. **El Proveedor informará al Cliente de cualquier información relacionada con los Datos del Cliente almacenados, sobre los destinatarios de los Datos del Cliente a los que el Proveedor deberá divulgarlos de acuerdo con la instrucción y sobre la finalidad del almacenamiento, en la medida en que el Cliente no disponga de esta información y en la medida en que no sea capaz de recopilarla él mismo.**
    4. **El Proveedor, dentro de los límites de lo razonable y necesario, permitirá al Cliente corregir, eliminar o restringir el procesamiento adicional de los Datos del Cliente, o por instrucción del Cliente corregirá, bloqueará o restringirá el procesamiento adicional él mismo, si y en la medida en que esto sea imposible para el Cliente.**
9. **Obligaciones de notificación y apoyo del Proveedor**
    1. **En la medida en que el Cliente esté sujeto a una obligación legal de notificación debido a una violación de la seguridad de los Datos del Cliente (en particular de conformidad con los Arts. 33, 34 del RGPD), el Proveedor informará al Cliente en tiempo oportuno de cualquier evento reportable en su área de responsabilidad. El Proveedor asistirá al Cliente en el cumplimiento de las obligaciones de notificación a petición de este último en la medida razonable y necesaria.**
    2. **El Proveedor asistirá al Cliente en la medida razonable y necesaria con las evaluaciones de impacto de protección de datos a realizar por el Cliente y, si es necesario, consultas posteriores con la autoridad de control de conformidad con los Arts. 35, 36 del RGPD.**
10. **Eliminación de los Datos del Cliente**
    1. **El Proveedor eliminará los Datos del Cliente tras la terminación de este acuerdo, a menos que el Proveedor esté obligado por ley a seguir almacenando los Datos del Cliente.**
    2. **El Proveedor puede conservar documentación que sirva como prueba del tratamiento ordenado y preciso de los Datos del Cliente, incluso después de la terminación del acuerdo.**
11. **Evidencia y auditorías**
    1. **El Proveedor proporcionará al Cliente, a petición de este último, toda la información requerida y disponible para el Proveedor para demostrar el**

cumplimiento de sus obligaciones bajo este acuerdo.

2. **El Cliente tendrá derecho a auditar al Proveedor con respecto al cumplimiento de las disposiciones de este acuerdo, en particular la implementación de las medidas técnicas y organizativas; incluyendo inspecciones.**
3. **Para llevar a cabo inspecciones de acuerdo con la Sección 11.2, el Cliente tiene derecho a acceder a las instalaciones comerciales del Proveedor en las que se tratan los Datos del Cliente dentro del horario comercial habitual (de lunes a viernes de 10 a.m. a 6 p.m.) tras notificación previa oportuna de acuerdo con la Sección 11.5. a su propio costo, sin interrumpir el curso de los negocios y bajo estricto secreto de los secretos comerciales del Proveedor.**
4. **El Proveedor tiene derecho, a su discreción y teniendo en cuenta las obligaciones legales del Cliente, a no revelar información que sea sensible con respecto al negocio del Proveedor o si el Proveedor estaría en incumplimiento de disposiciones legales o otras disposiciones contractuales como resultado de su divulgación. El Cliente no tiene derecho a acceder a datos o información sobre otros clientes del Proveedor, información de costos, informes de control de calidad y gestión de contratos, o cualquier otra información confidencial del Proveedor que no sea directamente relevante para los propósitos de auditoría acordados.**
5. **El Cliente informará al Proveedor con suficiente antelación (normalmente al menos dos semanas de antelación) de todas las circunstancias relacionadas con la realización de la auditoría. El Cliente puede realizar una auditoría por año calendario. Auditorías adicionales se llevan a cabo contra reembolso de los costos y después de consultar con el Proveedor.**
6. **Si el Cliente encarga a un tercero la realización de la auditoría, el Cliente obligará al tercero por escrito de la misma manera que el Cliente está obligado frente al Proveedor según esta Sección 11 de este acuerdo. Además, el Cliente obligará al tercero a mantener el secreto y confidencialidad, a menos que el tercero esté sujeto a una obligación profesional de secreto.**
7. **A discreción del Proveedor, la prueba del cumplimiento de las obligaciones bajo este acuerdo puede ser proporcionada, en lugar de una inspección, mediante la presentación de una opinión o informe apropiado y actual de una autoridad independiente (por ejemplo, auditor, departamento de auditoría, delegado de protección de datos, departamento de seguridad de TI, auditores de protección de datos o auditores de calidad) o una certificación adecuada mediante auditoría de seguridad de TI o protección de datos -- por ejemplo, según "BSI-Grundschutz" -- ("informe de auditoría"), si el informe de auditoría permite al Cliente de manera apropiada convencerse del cumplimiento de las obligaciones contractuales.**

12. **Plazo del contrato y terminación**

El plazo y la terminación de este acuerdo se regirán por las disposiciones de plazo y terminación del Acuerdo Principal. Una terminación del Acuerdo Principal resulta automáticamente en una cancelación de este acuerdo. Se excluye una terminación aislada de este contrato.

13. **Responsabilidad**
    1. **La responsabilidad del Proveedor bajo este acuerdo se regirá por las limitaciones de responsabilidad previstas en el Acuerdo Principal. En la medida en que terceros hagan valer reclamaciones contra el Proveedor que sean causadas por el incumplimiento culpable de este acuerdo o de una de**

sus obligaciones como responsable del tratamiento en términos de ley de protección de datos que le afecte, el Cliente deberá, a primera solicitud, indemnizar y mantener indemne al Proveedor de estas reclamaciones.

2. **El Cliente se compromete a indemnizar al Proveedor a primera solicitud contra todas las posibles multas impuestas al Proveedor correspondientes a la parte de responsabilidad del Cliente por la infracción sancionada por la multa.**

14. **Disposiciones finales**
    1. **Las disputas que surjan de este contrato se regirán por la ley alemana. El lugar de cumplimiento y jurisdicción será el domicilio social del Contratista. En caso de contradicciones en las dos versiones lingüísticas, prevalecerá la versión alemana.**
    2. **En caso de que disposiciones individuales de este acuerdo sean ineficaces o se vuelvan ineficaces o contengan un vacío, las disposiciones restantes permanecerán sin afectar. Las partes se comprometen a reemplazar la disposición ineficaz por una disposición legalmente permisible que se acerque más al propósito de la disposición ineficaz y que con ello satisfaga los requisitos del Art. 28 del RGPD.**
    3. **En caso de conflictos entre este acuerdo y otros arreglos entre las partes, en particular el Acuerdo Principal, prevalecerán las disposiciones de este acuerdo.**

Anexo:

Anexo 1: Finalidad, tipo y alcance del tratamiento de los Datos del Cliente, tipos de datos personales y categorías de interesados

Anexo 2: Medidas técnicas y organizativas

Anexo 3: Otros Encargados del Tratamiento

Anexo 1 - Finalidad, tipo y alcance del tratamiento de los Datos del Cliente, tipos de datos personales y categorías de interesados

1. **Finalidad del tratamiento de datos**

El Proveedor envía mensajes a los clientes finales del Cliente y en nombre del Cliente antes y durante la prestación de su servicio para obtener feedback, mejorar, estandarizar y automatizar la comunicación entre el Cliente y sus clientes finales. Los resultados se procesan y evalúan por cuenta del Cliente. Además, las evaluaciones de feedback indirecto y derivado, como información de fuentes internas y/o públicas, se utilizan para representar completamente la voz del cliente final. El Proveedor agrega y, por lo tanto, anonimiza los datos del Cliente recopilados a través de la plataforma para ofrecer al Cliente servicios adicionales como informes, benchmarking y funciones de monitoreo de KPI relacionadas con el feedback dado por los clientes finales del Cliente.

2. **Tipos de datos personales a. Datos maestros (p. ej., nombre, género, idioma); b. Datos de contacto (p. ej., dirección de correo electrónico, dirección, n.º de teléfono); c. Datos de comunicación (p. ej., correspondencia por correo electrónico); d. Datos contractuales (p. ej., duración del contrato, información sobre la prestación del servicio como facturación o costos); e. Si corresponde, datos de segmentación**

individual existentes del Cliente para sus clientes finales, como forma de conclusión del contrato (internet, teléfono, etc.), país de origen, categoría de servicio o grupo de edad; f. Evaluación del Cliente por parte del cliente final (reseña del cliente); g. Análisis de satisfacción (p. ej., evaluaciones de texto, tema y expresión).

3. **Categorías de interesados a. Personal del Cliente; b. Clientes finales del Cliente; c. Proveedores del Cliente.**

Anexo 2 -- Medidas técnicas y organizativas

Se han tomado las siguientes medidas técnicas y organizativas para proteger los datos personales:

- **1. Control de entrada**

Se debe denegar a las personas no autorizadas el acceso a los equipos de procesamiento de datos con los que se procesan y utilizan los datos personales.

Asegurado por:

a. Definición de áreas de seguridad y personas autorizadas

b. Seguridad de las habitaciones (llave, persiana, etc.)

c. Registro de asistencia

d. Seguridad exterior del edificio (vallas, puertas/ventanas de seguridad)

e. Cuidado en la selección de guardias de seguridad

f. Cuidado en la selección de servicios de limpieza

g. Videovigilancia de las entradas

h. Gestión de llaves / regulación (bloqueo y desbloqueo) / documentación de asignación de llaves

i. Sistema de control de acceso automático

j. Tarjetas con chip / sistemas de transpondedor

k. Sistema de bloqueo manual

l. Cerraduras de seguridad

m. Puertas con pomo (exterior)

n. Derechos de acceso altamente restringidos a la sala del servidor

o. Servidores en armarios de servidores bloqueables, llave en el departamento de TI

2. **Control de acceso (externo)**

Debe evitarse que los sistemas de procesamiento de datos puedan ser utilizados por

personas no autorizadas.

Asegurado por:

a. Posibilidad de bloqueo de la estación de datos

b. Inicio de sesión con nombre de usuario y contraseña y especificaciones para cambiarlos (período de validación máx. 1 año)

c. Cifrado de contraseñas

d. Software antivirus para servidor

e. Software antivirus para clientes

f. Firewall

g. Gestión de dispositivos móviles

h. Uso de túneles VPN para acceso remoto

i. Bloqueo de interfaces externas (USB)

j. Cifrado de portátiles / tablets

k. Gestión de permisos de usuario

l. Creación de perfiles de usuario

m. Asignación centralizada de contraseñas

n. Política de contraseñas seguras

o. Política de eliminación / destrucción

p. Política de protección de datos y seguridad

3. **Control de acceso (interno)**

Se debe tener cuidado para garantizar que aquellos autorizados a usar un sistema de procesamiento de datos solo puedan acceder a los datos sujetos a su autorización de acceso y que los datos personales no puedan ser leídos, copiados, modificados o eliminados sin autorización durante el procesamiento, uso y después del almacenamiento.

Asegurado por:

a. Autenticación con usuarios + contraseñas

b. Gestión de derechos graduada específica de usuario / definición de roles

c. Gestión de derechos de usuario por administradores

d. Número mínimo de administradores

e. Documentación de la gestión de derechos

f. Oscurecimiento de pantalla durante la interrupción del trabajo

g. Actualizaciones de seguridad regulares

h. Trituradora (nivel mín. 3, corte cruzado)

i. Registro de acceso a aplicaciones, específicamente al ingresar, cambiar y eliminar datos

j. Política de contraseñas seguras

k. Política de eliminación / destrucción

l. Política de protección de datos y seguridad

4. **Control de separación**

Garantizar que los datos recopilados para diferentes propósitos puedan procesarse por separado.

Asegurado por:

a. Sistemas de software separados

b. Bases de datos y almacenamiento separados

c. Control mediante concepto de autorización

d. Separación mediante regulaciones de acceso

e. Configuración de derechos de base de datos

5. **Control de transferencia**

Se debe garantizar que los datos personales no puedan leerse, copiarse, alterarse o eliminarse sin autorización durante la transmisión electrónica o durante su transporte o almacenamiento en portadores de datos, y que sea posible verificar y establecer en qué puntos se prevé una transmisión de datos personales mediante equipos de transmisión de datos.

Asegurado por:

a. Determinación de poderes para el procesamiento de datos

b. Determinación de las partes autorizadas para transmitir, los destinatarios de la transmisión y las rutas de transmisión

c. Seguridad de transporte de portadores de datos

d. W-LAN asegurado

e. Regulaciones sobre la destrucción de portadores de datos

f. Cifrado de correo electrónico (S/MIME, PGP, REDDCRYPT)

g. Política de seguridad de TI

6. **Control de entrada**

Se debe tener cuidado para garantizar que sea posible verificar y establecer retrospectivamente si y por quién se han introducido, alterado o eliminado datos personales en sistemas de procesamiento de datos.

Asegurado por:

a. Gestión de acceso de lectura / escritura

b. Registro de accesos de lectura/escritura y llamadas a programas

c. Marcado de documentos de entrada de datos con nombre y fecha después de la entrada

d. Disposiciones sobre el cambio de derechos de acceso y responsabilidad de datos

e. Responsabilidades estrictas para eliminaciones

7. **Control de disponibilidad**

Se debe tener cuidado para garantizar que los datos personales estén protegidos contra la destrucción o pérdida accidental.

Asegurado por:

a. Creación de copias de respaldo periódicas

b. Protección UPS en caso de fallo de energía

c. Protección antivirus/firewall

d. Plan de emergencia

e. Plan de recuperación

f. Protección DDoS permanentemente activa

8. **Control de procesamiento de pedidos**

Debe garantizarse que los datos personales procesados en nombre del cliente solo puedan procesarse de acuerdo con las instrucciones del cliente.

Asegurado por:

a. Determinación de derechos y obligaciones del contratista

b. Contrato para el procesamiento de datos por encargo

c. Capacitación de todos los empleados con derechos de acceso

d. Auditorías regulares de protección de datos

e. Acuerdo sobre derechos de control y auditoría

f. El contratista nombra a un delegado de protección de datos o persona responsable

Anexo 3 -- Otros Encargados del Tratamiento

Empresa, Dirección	Servicio / Tipo de Tratamiento	Cobertura Legal	Medidas para un nivel de protección comparable (sólo en terceros países)
TODO-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Alemania	Alojamiento web	Acuerdo de procesamiento de datos	/
Apolo 415 Misión St, Piso 37, San Francisco, California 94105, EE.UU	Enriquecimiento de datos	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Certificado ISO (27001) y cumplimiento SOC-2 certificado por A-LIGN.
char desarrollo de sistemas s.l.u. Parque Empresarial Arboreto – Avda. de la Fama, 16-20, 3ª planta 08940 Cornellà de Llobregat – Barcelona – España	Proveedor de sistemas de gestión de propiedades	Acuerdo de procesamiento de datos	Cifrado de datos en reposo y para datos en tránsito: HTTPS para todos los servicios que utilizan TLS (SSL) y cumple totalmente con el RGPD

CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Nogal, CA 91789 EE. UU.	Facturación	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Certificaciones y auditorías de terceros; Certificado ISO 27001; Estándares SOC 1/SOC 2 y MFA; políticas de seguridad a nivel operativo, de aplicaciones y de red; Configuración de seguridad de AWS: múltiples certificaciones para centros de datos, incluido el cumplimiento de ISO 27001, certificación PCI e informes SOC.
google llc, 1600 Amphitheatre Parkway, vista a la montaña, CA 94043 EE. UU.	Espacio de trabajo de Google Google Analytics	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Certificados ISO (ISO 27001, 27017, 27018); Directriz de Protección de Datos; Centro de cumplimiento e informes.
Ayuda Scout PBC 177 Huntington Ave, Boston, MA 02115, EE. UU.	Servicio de asistencia técnica	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Help Scout tiene certificación SOC2 Tipo 2 para seguridad y disponibilidad. Leyes de protección de datos de la UE, incluido el Reglamento general de protección de datos de la UE (“RGPD de la UE”) Configuración de seguridad de AWS

Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Alemania	Alojamiento	Acuerdo de procesamiento de datos	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 EE. UU.	Inbound Marketing, Ventas, Éxito del Cliente y Gestión de Relaciones con el Cliente	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Normas corporativas vinculantes; Centro de Datos (certificado ISO 27001 / auditoría SOC 2); Cifrado HTTP.
Luzmo NV Tiensevest 102 caja 201, B-3000 Lovaina, Bélgica	Análisis conversacional	#VALUE!	Cumple con AICPA SOC 2 Tipo II
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 EE. UU.	Proveedor de correo electrónico (API de correo electrónico)	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Escaneo de red externa y prueba de penetración; cifrado de datos; detección de intrusiones; Procedimiento de gestión de proveedores: control y auditoría frecuente de todos los subencargados.

Corporación Microsoft Una manera de Microsoft Redmond, WA 98052-6399 EE.UU	Oficina 365	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Informes de auditoría y confianza externa; Normas ISO 27001, 27017, 27018, 22301, 277701 certificados; política de prevención de pérdida de datos; Cumple con SSAE 18 SOC 1 Tipo II y SSAE 18 SOC 2 Tipo II.
Nonio Rua Eng.º Frederico Ulrich, 2650 4470-605 Moreira de Maia Portugal	Proveedor de sistemas de gestión de propiedades	Acuerdo de procesamiento de datos	Cifrado de datos en reposo y para datos en tránsito: HTTPS para todos los servicios que utilizan TLS (SSL) y cumple totalmente con el RGPD
OpenAI OpCo, LLC 3180 18th Street, San Francisco, CA 94110	Información, informes, análisis	Acuerdo de procesamiento de datos	/
OVH GmbH, St. Johanner Str. 41-43, 66111 Sarrebruck Alemania	Alojamiento	Acuerdo de procesamiento de datos	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Colonia Alemania	Operaciones web	Acuerdo de procesamiento de datos	/

raya, inc. 510 Townsend Street San Francisco, CA 94103 EE. UU.	Solución de pago	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Cifrado de datos en reposo y para datos en tránsito: HTTPS para todos los servicios que utilizan TLS (SSL); todos los números de tarjetas están cifrados en reposo con AES-256; registros de auditoría; política de gestión de acceso; Certificado de Proveedor de Servicios PCI Nivel 1.

Twilio, Inc., 375 calle Beale, suite 300, San Francisco, CA 94105 EE. UU.	Proveedor de mensajes cortos (SMS)	Cláusula contractual estándar y evaluación individual hasta un nivel de protección comparable al estándar dentro de la UE.	Normas corporativas vinculantes; marco de seguridad basado en ISO 27001; ISO/IEC 27001, ISO/IEC 27017 y 27018, SOC 2 tipo II, PCI DSS nivel 1 certificados; Configuración de seguridad de AWS: múltiples certificaciones para centros de datos, incluido el cumplimiento de ISO 27001, certificación PCI e informe SOC; las bases de datos (datos del cliente) se cifran utilizando el Estándar de cifrado avanzado y los datos del cliente se cifran cuando están en tránsito entre la aplicación de software del cliente y los servicios utilizando TLS v1.2; pruebas de penetración; Políticas y procedimientos de gestión de incidentes de seguridad de acuerdo con NIST SP 800-61.