La versión original de este Acuerdo de Procesamiento de Datos fue redactada en inglés antes de ser traducida a otros idiomas. Estas traducciones realizadas internamente se proporcionan únicamente como cortesía y no tienen valor legal.

Acuerdo de Procesamiento de Datos

Acuerdo sobre el procesamiento de datos personales en nombre de un responsable conforme al Art. 28 del RGPD entre el cliente (en adelante, el "**Cliente**") y CA Customer Alliance GmbH, Ullsteinstr. 130, 12109 Berlín, Alemania (en adelante, el "**Proveedor**").

1. Objeto del Acuerdo

En el curso de la prestación de servicios según el acuerdo de servicios (en adelante, el "**Acuerdo Principal**"), es necesario que el Proveedor trate datos personales con respecto a los cuales el Cliente actúa como responsable en términos de la ley de protección de datos (en adelante, "**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

2.1. El Proveedor tratará los Datos del Cliente en nombre y de acuerdo con las instrucciones del Cliente en el sentido del Art. 28 del RGPD (Tratamiento por Cuenta Ajena). El Cliente sigue siendo el responsable en términos de la ley de protección de datos.

2.2. El tratamiento de los Datos del Cliente por parte del Proveedor se realiza de la manera y en el alcance y para el propósito determinado en el **Anexo 1** de este acuerdo; el tratamiento se refiere a los tipos de datos personales y categorías de interesados especificados en el mismo. La duración del tratamiento corresponde a la duración del Acuerdo Principal.

2.3. El tratamiento de los Datos del Cliente por parte del Proveedor se realizará, en principio, dentro de la Unión Europea o en otro estado contratante del Espacio Económico Europeo (EEE). No obstante, el Proveedor está autorizado a tratar los Datos del Cliente de acuerdo con las disposiciones de este acuerdo fuera del EEE si informa al Cliente con antelación sobre el lugar de tratamiento de datos y si se cumplen los requisitos de los Art. 44 a 48 del RGPD o si se aplica una excepción según el Art. 49 del RGPD.

3. Derecho del Cliente a emitir instrucciones

3.1. El Proveedor trata los Datos del Cliente de acuerdo con las instrucciones del Cliente, a menos que el Proveedor esté legalmente obligado a hacer lo contrario. En este último caso, el Proveedor informará al Cliente de dicho requisito legal antes del tratamiento, a menos que esa ley prohíba dicha información por razones importantes de interés público.

3.2. Las instrucciones del Cliente se estipulan y documentan en principio 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 se harán por escrito.

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

4. Responsabilidad legal del Cliente

4.1. El Cliente es el único responsable de la permisibilidad del tratamiento de los Datos del Cliente y de la protección de los derechos de los interesados en la relación entre las partes.

4.2. El Cliente es responsable de proporcionar al Proveedor los Datos del Cliente a tiempo para la prestación de servicios según el Acuerdo Principal y es responsable de la calidad de los Datos del Cliente. El Cliente deberá informar al Proveedor de inmediato y de manera completa si durante la revisión de los resultados del Proveedor encuentra errores o irregularidades con respecto a las disposiciones de protección de datos o sus instrucciones.

4.3. Si el Proveedor está obligado a proporcionar información a un organismo gubernamental o persona sobre el tratamiento de los Datos del Cliente o a cooperar con estos organismos de cualquier otra manera, el Cliente está obligado, a solicitud, a asistir al Proveedor en proporcionar dicha información y en cumplir otras obligaciones de cooperación.

5. Requisitos para el personal

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

6. Seguridad del tratamiento

6.1. El Proveedor tomará, según el Art. 32 del RGPD, las medidas técnicas y organizativas necesarias y apropiadas, teniendo en cuenta el estado de la técnica, los costos de implementación y la naturaleza, el alcance, las circunstancias y los fines de los Datos del Cliente, así como la diferente probabilidad 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 encuentran en el **Anexo 2**.

6.2. El Proveedor tendrá el derecho de modificar las medidas técnicas y organizativas durante la vigencia del acuerdo, siempre que sigan cumpliendo con los requisitos legales.

7. Contratación de otros procesadores

7.1. El Cliente otorga al Proveedor la autorización general para contratar otros procesadores con respecto al tratamiento de los Datos del Cliente. Los procesadores adicionales consultados en el momento de la conclusión del acuerdo se indican en el **Anexo 3**. En general, no se requiere autorización para las relaciones contractuales con proveedores de servicios que se ocupen del examen o mantenimiento de los procedimientos o sistemas de tratamiento de

datos por parte de terceros o que impliquen otros servicios adicionales, incluso si el acceso a los Datos del Cliente no puede excluirse, siempre que el Proveedor tome medidas razonables para proteger la confidencialidad de los Datos del Cliente.

7.2. El Proveedor deberá notificar al Cliente sobre cualquier cambio previsto en relación con la consulta o sustitución de otros procesadores. En casos individuales, el Cliente tiene el derecho de oponerse a la contratación de un posible procesador adicional. Una objeción solo podrá ser planteada por el Cliente por razones importantes que deberán ser demostradas al Proveedor. En la medida en que el Cliente no se oponga dentro de los 14 días posteriores a la recepción de la notificación, su derecho a oponerse a la correspondiente contratación caduca. Si el Cliente se opone, el Proveedor tiene derecho a rescindir el Acuerdo Principal y este acuerdo con un plazo de preaviso de tres (3) meses.

7.3. El acuerdo entre el Proveedor y el otro procesador debe imponer a este último las mismas obligaciones que las 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 se imponen al otro procesador las obligaciones establecidas en el Art. 28, párrafo 3 del RGPD.

8. Derechos de los interesados

8.1. El Proveedor apoyará al Cliente dentro de lo razonable mediante 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.

8.2. En la medida en que un interesado presente una solicitud para el ejercicio de sus derechos directamente al Proveedor, este deberá remitir dicha solicitud al Cliente de manera oportuna.

8.3. El Proveedor informará al Cliente sobre cualquier información relacionada con los Datos del Cliente almacenados, sobre los destinatarios de los Datos del Cliente a los que el Proveedor los divulgará de acuerdo con la instrucción y sobre el propósito del almacenamiento, en la medida en que el Cliente no tenga esta información a su disposición y en la medida en que no pueda obtenerla por sí mismo.

8.4. El Proveedor deberá, dentro de los límites de lo razonable y necesario, permitir al Cliente corregir, eliminar o restringir el tratamiento posterior de los Datos del Cliente, o a solicitud del Cliente corregir, bloquear o restringir el tratamiento posterior él mismo, si y en la medida en que esto sea imposible para el Cliente.

9. Obligaciones de notificación y apoyo del Proveedor

9.1. 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, conforme a los Art. 33, 34 del RGPD), el Proveedor informará al Cliente de manera oportuna sobre cualquier evento reportable en su área de responsabilidad. El Proveedor asistirá al Cliente en el cumplimiento de las obligaciones de notificación a solicitud de este en la medida razonable y necesaria.

9.2. El Proveedor asistirá al Cliente en la medida razonable y necesaria con las evaluaciones de impacto de protección de datos que deba realizar el Cliente y, si es necesario, con las consultas posteriores con la autoridad de control conforme a los Art. 35, 36 del RGPD.

10. Eliminación de Datos del Cliente

10.1. El Proveedor eliminará los Datos del Cliente al finalizar este acuerdo, a menos que el Proveedor esté legalmente obligado a seguir almacenando los Datos del Cliente.

10.2. El Proveedor puede conservar la documentación que sirva como prueba del tratamiento ordenado y preciso de los Datos del Cliente, incluso después de la finalización del acuerdo.

11. Pruebas y auditorías

11.1. El Proveedor proporcionará al Cliente, a solicitud de este, toda la información requerida y disponible para el Proveedor para demostrar el cumplimiento de sus obligaciones bajo este acuerdo.

11.2. 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.

11.3. Para llevar a cabo inspecciones conforme a la Sección 11.2, el Cliente tiene derecho a acceder a las instalaciones del Proveedor en las que se procesen Datos del Cliente dentro del horario comercial habitual (de lunes a viernes de 10 a.m. a 6 p.m.) después de notificar con antelación y de acuerdo con la Sección 11.5, a su propio costo, sin interrumpir el curso de los negocios y bajo estricta confidencialidad de los secretos comerciales y empresariales del Proveedor.

11.4. El Proveedor tiene derecho, a su propia discreción y teniendo en cuenta las obligaciones legales del Cliente, a no divulgar información que sea sensible con respecto a los negocios del Proveedor o si el Proveedor estuviera infringiendo disposiciones legales o contractuales al revelarla. 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 otro dato confidencial del Proveedor que no sea directamente relevante para los fines de auditoría acordados.

11.5. El Cliente deberá informar al Proveedor con suficiente antelación (generalmente al menos dos semanas antes) sobre todas las circunstancias relacionadas con la realización de la auditoría. El Cliente puede realizar una auditoría por año calendario. Las auditorías adicionales se llevarán a cabo contra el reembolso de los costos y tras la consulta con el Proveedor.

11.6. Si el Cliente encarga a un tercero la realización de la auditoría, el Cliente deberá obligar por escrito al tercero de la misma manera que el Cliente está obligado hacia el Proveedor según esta Sección 11 de este acuerdo. Además, el Cliente deberá obligar al tercero a mantener la confidencialidad, a menos que el tercero esté sujeto a una obligación profesional de secreto.

11.7. A discreción del Proveedor, la prueba de cumplimiento de las obligaciones bajo este

acuerdo puede proporcionarse, en lugar de una inspección, mediante la presentación de una opinión o informe adecuado y actual de una autoridad independiente (por ejemplo, auditor, departamento de auditoría, oficial de protección de datos, departamento de seguridad informática, auditores de protección de datos o auditores de calidad) o una certificación adecuada de seguridad informática o auditoría de protección de datos – por ejemplo, según "BSI-Grundschutz" – ("informe de auditoría"), si el informe de auditoría permite al Cliente convencerse de manera adecuada del cumplimiento de las obligaciones contractuales.

12. Duración y terminación del contrato

La duración y terminación de este acuerdo se regirán por las disposiciones de duración y terminación del Acuerdo Principal. La terminación del Acuerdo Principal resulta automáticamente en la cancelación de este acuerdo. Se excluye la terminación aislada de este contrato.

13. Responsabilidad

13.1. 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 presenten reclamaciones contra el Proveedor que sean causadas por el incumplimiento culpable del Cliente de este acuerdo o de una de sus obligaciones como responsable en términos de la ley de protección de datos, el Cliente indemnizará y mantendrá indemne al Proveedor de estas reclamaciones a primera solicitud.

13.2. 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

14.1. Las disputas derivadas de este contrato se regirán por la ley alemana. El lugar de cumplimiento y jurisdicción será la sede registrada del Proveedor. En caso de contradicciones en las dos versiones lingüísticas, prevalecerá la versión alemana.

14.2. En caso de que alguna disposición de este acuerdo sea o se vuelva ineficaz o contenga una laguna, las disposiciones restantes no se verán afectadas. Las partes se comprometen a reemplazar la disposición ineficaz por una disposición legalmente permitida que se acerque lo más posible al propósito de la disposición ineficaz y que cumpla con los requisitos del Art. 28 del RGPD.

14.3. En caso de conflictos entre este acuerdo y otros acuerdos entre las partes, en particular el Acuerdo Principal, prevalecerán las disposiciones de este acuerdo.

Anexos:

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

Anexo 2: Medidas técnicas y organizativas

Anexo 3: Otros procesadores

Anexo 1 – Finalidad, tipo y alcance del tratamiento de 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 de y en nombre del Cliente antes y durante la prestación de su servicio para obtener retroalimentación, mejorar, estandarizar y automatizar la comunicación entre el Cliente y sus clientes finales. Los resultados se procesan y evalúan en nombre del Cliente. Además, se utilizan evaluaciones de retroalimentación indirecta y derivada, como información de fuentes internas y/o públicas, 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, comparación y características de monitoreo de KPI relacionadas con la retroalimentación proporcionada por los clientes finales del Cliente.

2. Tipos de datos personales

a) Datos maestros (por ejemplo, nombre, género, idioma);
b) Datos de contacto (por ejemplo, dirección de correo electrónico, dirección, número de teléfono);
c) Datos de comunicación (por ejemplo, correspondencia por correo electrónico);
d) Datos contractuales (por ejemplo, duración del contrato, información sobre la prestación del servicio, como facturación o costos);
e) Si aplica, 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 el cliente final (opinión del cliente);
g) Análisis de satisfacción (por ejemplo, evaluaciones de texto, temas y expresiones).

3. Categorías de interesados

a) Personal del Cliente;
b) Clientes finales del Cliente;
c) Proveedores del Cliente.

Anexo 2 – Medidas técnicas y organizativas

Las siguientes medidas técnicas y organizativas se han tomado para proteger los datos personales:

1. Control de entrada

Se denegará el acceso a los equipos de procesamiento de datos a personas no autorizadas.

Asegurado por:

a) Definición de áreas de seguridad y personas autorizadas
b) Seguridad de la sala (llave, persiana, etc.)
c) Registro de asistencia
d) Seguridad exterior del edificio (vallado, puertas/ventanas de seguridad)
e) Cuidado en la selección de los guardias de seguridad
f) Cuidado en la selección de los servicios de limpieza
g) Videovigilancia de las entradas
h) Gestión de llaves / documentación de asignación de llaves
i) Sistema automático de control de acceso
j) Tarjetas de chip / sistemas de transpondedor
k) Sistema de cierre manual
l) Cerraduras de seguridad
m) Puertas con pomo (exterior)

2. Control de acceso (externo)

Debe evitarse que los sistemas de procesamiento de datos puedan ser utilizados por personas no autorizadas.

Asegurado por:

a) Capacidad de bloquear la estación de datos
b) Inicio de sesión con nombre de usuario y contraseña y especificaciones para cambiarla
c) Cifrado de contraseñas
d) Software antivirus en el servidor
e) Software antivirus en los 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/tabletas
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 y seguridad de datos

3. Control de acceso (interno)

Se debe garantizar que las personas autorizadas para utilizar un sistema de procesamiento de datos solo puedan acceder a los datos según 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) Gestión de derechos graduales específicos del usuario
b) Gestión de derechos de usuario por administradores
c) Número mínimo de administradores
d) Documentación de la gestión de derechos
e) Oscurecimiento de pantalla durante interrupciones del trabajo
f) Actualizaciones de seguridad regulares
g) Trituradora (mín. nivel 3, corte transversal)
h) Registro de acceso a aplicaciones, específicamente al ingresar, modificar y eliminar datos

4. Control de separaciónl

Asegurarse de que los datos recopilados para diferentes propósitos puedan ser procesados por separado.

Asegurado por:

a) Sistemas de software separados
b) Bases de datos y almacenamiento separados
c) Control a través del concepto de autorización
d) Separación a través de regulaciones de acceso
e) Configuración de derechos de la base de datos

5. Control de transferencia

Se debe asegurar que los datos personales no puedan ser leídos, copiados, alterados o eliminados sin autorización durante la transmisión electrónica o durante su transporte o almacenamiento en soportes de datos, y que sea posible verificar y establecer en qué puntos se proporciona 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 a transmitir, receptores de la transmisión y rutas de transmisión
c) Seguridad en el transporte de soportes de datos
d) W-LAN seguro
e) Regulaciones sobre la destrucción de soportes de datos
f) Cifrado

6. Control de entrada

Se debe asegurar que los datos personales procesados en nombre del cliente solo puedan ser procesados 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

7. Control de disponibilidad

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

Asegurado por:

a) Creación de copias de seguridad periódicas
b) Protección UPS en caso de fallo de energía
c) Protección contra virus/firewall
d) Plan de emergencia
e) Plan de recuperación
f) Protección DDoS permanentemente activa

8. Control del procesamiento de pedidos

Se debe asegurar que los datos personales procesados en nombre del cliente solo puedan ser procesados 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

Anexo 3 – Otros procesadores			
Empresa, Dirección	**Servicio / Tipo de Procesamiento**	**Cobertura Legal**	**Medidas para un nivel de protección comparable (solo en terceros países)**
ALL-INKL.COM - Neue Medien Münnich, Hauptstraße 68, 02742 Friedersdorf Germany	Web-Hosting	Acuerdo de Procesamiento de Datos	/
CHARGEBEE INC., 340 S. Lemon Avenue, Suite #1537, Walnut, CA 91789 USA	Facturación	Cláusula contractual estándar y evaluación individual a 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 de red, aplicación y operación; configuración de seguridad de AWS – múltiples certificaciones para centros de datos, incluyendo cumplimiento con ISO 27001, certificación PCI y
Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043 USA	Google Workspace Google Analytics	Cláusula contractual estándar y evaluación individual a 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 y Reportes.
Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen Germany	Hosting	Acuerdo de Procesamiento de Datos	/
HubSpot, Inc., 25 First Street, Cambridge, MA 02141 USA	Inbound-Marketing y Ventas	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Normas Corporativas Vinculantes; Centro de Datos (certificado ISO 27001 / auditoría SOC 2); cifrado HTTPs.

Intercom, Inc., 55 2nd Street, 4th Fl., San Francisco, CA 94105 USA	Live-Chat	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Auditorías externas, pruebas de penetración y recompensas por errores; auditoría SOC 2; certificado ISO 27001; auditoría HIPAA; configuración de seguridad de AWS; puntos finales de API y aplicaciones solo TLS/SSL; política de seguridad; formación en seguridad y concienciación.
Impala Travel Technology Ltd., 70 White Lion Street, London, N1 9PP UK	Extracción de datos de PMS (API)	Acuerdo de Procesamiento de Datos	Protección adecuada de datos personales en el Reino Unido – Decisión de Ejecución de la Comisión Europea del 28 de junio de 2021 – C(2021) 4800.
Mailgun Technologies, Inc., 548 Market Street, Suite 43099, San Francisco, CA 94101 USA	Proveedor de Email (API de correo electrónico)	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Escaneo de red externa y prueba de penetración; cifrado de datos; detección de intrusos; procedimiento de gestión de proveedores – control y auditoría frecuente de todos los subprocesadores.
Microsoft Corporation One Microsoft Way Redmond, WA 98052-6399 USA	Office 365	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Reportes de confianza y auditoría externos; certificados ISO 27001, 27017, 27018, 22301, 277701; política de prevención de pérdida de datos; cumplimiento con SSAE 18 SOC 1 Tipo II y SSAE 18 SOC 2 Tipo II.
OVH GmbH, St. Johanner Str. 41-43, 66111 Saarbrücken Germany	Hosting	Acuerdo de Procesamiento de Datos	/
Scaling Technologies GmbH, Pfarrer-Hillmann-Weg 1, 51069 Köln Germany	Operaciones Web	Acuerdo de Procesamiento de Datos	/

Stripe, Inc. 510 Townsend Street San Francisco, CA 94103 USA	Solución de Pago	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Cifrado de datos en reposo y en tránsito – HTTPS para todos los servicios utilizando TLS (SSL); todos los números de tarjetas están cifrados en reposo con AES-256; registros de auditoría; política de gestión de accesos; certificado de Proveedor de Servicios PCI Nivel 1.
SugarCRM, Inc., 10050 N Wolfe Road, SW2-130 Cupertino, CA 95014 USA	Gestión de Relación con el Cliente (CRM)	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Certificado SOC II; cifrado para todas las contraseñas, datos clave y copias de seguridad; todos los datos de producción y de clientes están cifrados en tránsito y en reposo; autenticación multifactor; herramientas de prevención de pérdida de datos; alojado en Irlanda (UE); configuración de seguridad de AWS – múltiples certificaciones para centros de datos, incluyendo cumplimiento con ISO 27001, certificación PCI y
Twilio, Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105 USA	Proveedor de Mensajes Cortos (SMS)	Cláusula contractual estándar y evaluación individual a un nivel de protección comparable al estándar dentro de la UE.	Normas Corporativas Vinculantes; marco de seguridad basado en ISO 27001; certificados ISO/IEC 27001, ISO/IEC 27017 y 27018, SOC 2 Tipo II, PCI DSS Nivel 1; configuración de seguridad de AWS – múltiples certificaciones para centros de datos, incluyendo cumplimiento con ISO 27001, certificación PCI y reporte SOC; bases de datos (datos del cliente) están cifradas usando el Estándar de Cifrado Avanzado y los datos del cliente están cifrados cuando están en tránsito entre la aplicación de software del cliente y los servicios usando TLS v1.2; pruebas de penetración; políticas y procedimientos de gestión de incidentes de seguridad de acuerdo con NIST SP 800-61.