ANEXO SOBRE EL TRATAMIENTO DE DATOS DEL CLIENTE

Última actualización: septiembre de 2025

Si desea una copia firmada de este acuerdo, haga clic aquí.

Este Anexo sobre el Tratamiento de Datos del Cliente, incluyendo sus anexos y apéndices (el "Anexo"), se celebra entre HighLevel, Inc., una corporación constituida bajo las leyes de Dallas, Texas; ZenZales una corporación constituida bajo las leyes de Colombia y México y sus Afiliadas correspondientes ("HighLevel y ZenZales"), y la contraparte que acepta este Anexo ("Cliente") (cada una, una "Parte" y, colectivamente, las "Partes") en virtud de la firma y aceptación por parte del Cliente del Acuerdo de Términos de Servicio (el "Acuerdo"). A partir de la fecha de entrada en vigor del Acuerdo (la "Fecha de Entrada en Vigor"), los términos de este Anexo se incorporarán por referencia y formarán parte del Acuerdo. En caso de conflicto o inconsistencia con los términos del Acuerdo, este Anexo prevalecerá sobre los términos del Acuerdo en la medida de dicho conflicto o inconsistencia, y reemplazará cualquier Anexo anterior. Para mayor claridad, las Cláusulas Contractuales Estándar prevalecen sobre cualquier otro término del Anexo. Salvo que el contexto requiera lo contrario, las referencias en este Addendum al Acuerdo se refieren al Acuerdo modificado o complementado por, e incluyendo, este Addendum.

1. Definiciones

a. A los efectos de interpretar el presente Addendum, los siguientes términos (y sus cognados aplicables) tendrán los significados que se establecen a continuación:

1. " **Cuenta** " significa cualquier cuenta o instancia creada por, o en nombre de, el Cliente o sus Afiliados dentro de los Servicios.

2. " **Afiliado** " significa cualquier entidad dentro de un grupo controlado de empresas que directa o indirectamente, a través de uno o más intermediarios, controla, está controlada por o está bajo control común con una de las Partes.
3. " **Leyes de protección de datos aplicables** " significa todas las leyes y regulaciones aplicables al procesamiento de datos personales del cliente, incluidas, entre otras, las leyes y regulaciones identificadas en el **Anexo B** del presente, que pueden modificarse, enmendarse o complementarse de vez en cuando, según corresponda.
4. " **Procesador contratado** " significa cualquier tercero designado por o en nombre de HighLevel y ZenZales para procesar los datos personales del cliente en relación con los Servicios.
5. " **Datos Personales del Cliente** " se refiere a los Datos Personales contenidos en los Datos del Cliente que HighLevel y ZenZales procesan por o en nombre del Cliente para prestar los Servicios de conformidad con el Acuerdo. Los Datos Personales del Cliente no incluyen la información de su Cuenta.
6. " **Exportador de Datos** " e " **Importador de Datos** " tendrán los mismos significados que se les asignan en **la Parte A del Anexo** A.
7. " **RGPD** " significa el RGPD de la UE y el RGPD del Reino Unido tal como se definen esos términos en **el Anexo B** , según corresponda.
8. " **Términos Específicos de Jurisdicción** " se refiere a todos los términos aplicables al Tratamiento de Datos Personales que se aplican en la medida en que HighLevel y ZenZales Tratan Datos Personales de Clientes originados o protegidos por las Leyes de Protección de Datos Aplicables en una de las jurisdicciones identificadas en estos términos. Los Términos Específicos de Jurisdicción están disponibles actualmente como **Anexo B** de este Anexo y pueden publicarse en línea de acuerdo con la Sección 15 de este Anexo.

9. " **Transferencia restringida** " significa cualquier transferencia de Datos personales del cliente protegidos por las leyes de protección de datos aplicables a un tercer país o una organización internacional en un tercer país (incluido el almacenamiento de datos en servidores extranjeros).
10. Las " **SCCs** " o " **Cláusulas Contractuales Estándar** " son las cláusulas modelo para Transferencias Restringidas adoptadas de tiempo en tiempo por las autoridades pertinentes de las jurisdicciones indicadas en **el Anexo B** , en la medida en que su uso sea aprobado por las

autoridades pertinentes como un mecanismo o salvaguarda apropiado para Transferencias Restringidas.

11. " **Servicios** " se refiere a los servicios y otras actividades realizadas por o en nombre de HighLevel y ZenZales para el Cliente tras la creación de una Cuenta, ya sea mediante una prueba gratuita o una suscripción de pago. Para evitar cualquier duda, los Servicios excluyen los servicios que HighLevel y ZenZales realizan como Responsable del Tratamiento, como la gestión de las relaciones con los clientes, la administración de cuentas y la provisión de las áreas de su sitio web https://www.gohighlevel.com/ a las que se puede acceder sin crear una Cuenta.
12. « **Subencargado del Tratamiento** » se refiere al Encargado del Tratamiento directo de un Encargado. Para evitar cualquier duda, los Encargados del Tratamiento contratados son Subencargados del Tratamiento.

b. Los términos " **Responsable del tratamiento** ", " **Evaluación de la protección de datos** ", " **Sujeto de los datos** ", " **Estado miembro** ", " **Datos personales** ", " **Violación de datos personales** ", " **Procesamiento ", " Encargado** del tratamiento" , " **Derechos de los sujetos de los datos** ", " **Autoridad de control** " y " **Tercer país** " tendrán el mismo significado que en las Leyes de protección de datos aplicables, y sus términos afines y correspondientes se interpretarán en consecuencia.

c. Los términos en mayúsculas que se utilicen, pero no se definan en el presente documento, tendrán el significado que se les atribuye en el Acuerdo. Salvo las modificaciones o complementos mencionados anteriormente, las definiciones del Acuerdo mantendrán su plena vigencia.

2. Alcance y aplicabilidad.

a. Duración . Este Anexo entrará en vigor en la Fecha de Entrada en Vigencia y continuará vigente mientras HighLevel y ZenZales procesen los Datos Personales de conformidad con el Acuerdo.

b. Alcance . Este Anexo se aplicará al Tratamiento de todos los Datos Personales del Cliente, independientemente del país de origen, el lugar de Tratamiento, la ubicación de los Interesados o cualquier otro factor. El Tratamiento de Datos Personales que no constituyan Datos Personales del Cliente queda fuera del alcance de este Anexo.

c. Anexos y Apéndices . Este Anexo incluye los siguientes anexos y apéndices:

1. Anexo A – Detalles del procesamiento;
2. Apéndice I del Anexo A – Medidas de seguridad técnicas y organizativas;
3. Anexo B – Términos específicos de la jurisdicción; y
4. Apéndice I del Anexo B – Cláusulas complementarias a las cláusulas contractuales estándar.

3. Tratamiento de Datos Personales del Cliente.

a. HighLevel y ZenZales actuarán como Encargados del Tratamiento de los Datos Personales del Cliente. El Cliente actuará como Responsable del Tratamiento de los Datos Personales del Cliente. En la medida en que el Cliente actúe como Encargado del Tratamiento para otras partes al procesar sus Datos Personales, HighLevel y ZenZales actuarán como Subencargados del Tratamiento para el Cliente.

b. HighLevel y ZenZales deberán:

1. Cumplir con todas las Leyes de Protección de Datos Aplicables en el Procesamiento de Datos Personales del Cliente;
2. No procesar datos personales del cliente salvo según las instrucciones documentadas pertinentes del cliente, incluso para proporcionar y mejorar los servicios establecidos en el acuerdo (para mayor claridad, dichas instrucciones incluyen la autorización para anonimizar, desidentificar o agregar datos personales del cliente y para proporcionar las funciones de inteligencia artificial de HighLevel y ZenZales utilizadas para los servicios), a menos que dicho procesamiento esté permitido o requerido por las leyes de protección de datos aplicables; y
3. Informar inmediatamente al Cliente en caso de que, en la opinión razonable de HighLevel y ZenZales, una instrucción de Procesamiento dada por el Cliente pueda infringir las Leyes de Protección de Datos Aplicables.

c. Toda la información necesaria relativa a los detalles del Tratamiento se establece en **el Anexo A.**

d. El Cliente instruye a HighLevel y ZenZales (y autoriza a HighLevel y ZenZales a instruir a cada Procesador contratado que contrate) a Procesar los Datos Personales del Cliente y, en particular, a transferir los Datos Personales del Cliente a cualquier país o territorio, solo según sea razonablemente

necesario para la prestación de los Servicios y de conformidad con el Acuerdo y este Anexo.

4. Personal. HighLevel y ZenZales tomarán las medidas razonables para garantizar:

a. la confiabilidad de cualquier empleado, agente o contratista que pueda tener acceso a los Datos Personales del Cliente;
b. que el acceso a los Datos Personales del Cliente está estrictamente limitado a aquellas personas que necesitan conocerlos o acceder a ellos, según sea estrictamente necesario para cumplir con las instrucciones documentadas dadas a HighLevel y ZenZales por el Cliente o para cumplir con las Leyes de Protección de Datos Aplicables; y
c. que todas esas personas están sujetas a compromisos formales de confidencialidad, obligaciones profesionales de confidencialidad u obligaciones legales de confidencialidad.

5. Seguridad del Tratamiento. HighLevel y ZenZales implementarán y mantendrá las medidas de seguridad administrativas, técnicas y organizativas identificadas en el **Apéndice I del Anexo A** , que garanticen un nivel de seguridad adecuado al riesgo del Tratamiento y tengan en cuenta: el estado de la técnica, los costes de implementación, la naturaleza y los fines del Tratamiento; la probabilidad y gravedad variables de los riesgos para los derechos y libertades de las personas físicas; y los riesgos que presentan las actividades de Tratamiento, en particular los riesgos relacionados con las Violaciones de Datos Personales.

6. Encargados del Tratamiento contratados.

a. Autorización para procesadores contratados existentes: el cliente autoriza a HighLevel y ZenZales a continuar utilizando los procesadores contratados contratados a partir de la fecha de entrada en vigor y establecidos en el sitio web de HighLevel y ZenZales [https://www.gohighlevel.com/sub-processors], y además autoriza a HighLevel y ZenZales y sus procesadores contratados a designar procesadores contratados adicionales, siempre que se cumplan las obligaciones de esta Sección 6 (y las respectivas obligaciones del **Anexo B**).

b. Autorización para la designación de Encargados del Tratamiento : Para designar un Encargado del Tratamiento adicional, HighLevel y ZenZales notificarán por escrito al Cliente, incluyendo los detalles del Tratamiento que se realizará, tal como se describe en su sitio web. El Cliente puede suscribirse para recibir dichas notificaciones haciendo clic en " Haga clic aquí para recibir notificaciones sobre cualquier actualización de esta lista " en la siguiente dirección: https://www.gohighlevel.com/sub-processors .

c. Objeción a los Encargados del Tratamiento Contratados:

1. Se considerará que el Cliente ha dado su consentimiento para el Encargado del Tratamiento adicional si no se recibe ninguna objeción dentro de los treinta (30) días siguientes a la notificación de HighLevel y ZenZales. El Cliente puede oponerse al nombramiento de un Encargado del Tratamiento mediante una objeción por escrito, que incluirá el nombre del Encargado del Tratamiento objeto de la objeción y una declaración justificada de su objeción.
2. Si se recibe una objeción, las Partes colaborarán de buena fe para alcanzar una solución comercialmente razonable. Si no se llega a una solución mutuamente aceptable, el Cliente podrá rescindir el Acuerdo inmediatamente mediante notificación por escrito a HighLevel y ZenZales, sin que se abonen más cargos que los acumulados hasta la fecha de rescisión. Tras la notificación de rescisión, HighLevel y ZenZales dejarán de procesar los datos personales del Cliente.

d. Requisitos para la designación de procesadores contratados: Con respecto a cada procesador contratado, HighLevel y ZenZales deberán:

1. restringir el acceso del Procesador Contratado a los Datos Personales del Cliente únicamente a lo que sea necesario para ayudar a HighLevel y ZenZales a proporcionar los Servicios, y prohibir al Procesador Contratado acceder a los Datos Personales del Cliente para cualquier otro propósito, y
2. garantizar que el acuerdo entre HighLevel y ZenZales y el Procesador Contratado esté regido por un contrato escrito que incluya términos que ofrezcan al menos el mismo nivel de protección para los Datos Personales del Cliente que los establecidos en este Anexo, en la medida que sea aplicable a la naturaleza de los servicios prestados por dicho Procesador Contratado.

e. Cuando cualquier Procesador contratado no cumpla con sus obligaciones de protección de datos bajo dicho contrato escrito (o en ausencia del mismo, según sea el caso), HighLevel y ZenZales seguirán siendo completamente

responsables ante el Cliente por el cumplimiento de las obligaciones de protección de datos de los respectivos Procesadores contratados bajo dicho contrato y/o las Leyes de protección de datos aplicables.

7. Derechos de los Titulares de los Datos.

a. Teniendo en cuenta la naturaleza del Procesamiento, HighLevel y ZenZales asistirán al Cliente implementando medidas técnicas y organizativas apropiadas, en la medida de lo posible, para responder a solicitudes válidas para ejercer los Derechos de los Titulares de Datos bajo las Leyes de Protección de Datos Aplicables.

b. Con respecto a los Derechos de los Titulares de Datos en el ámbito de aplicación de esta Sección 7, HighLevel y ZenZales deberán:

1. notificar de inmediato al Cliente si él o alguno de sus Procesadores Contratados recibe una solicitud de un Titular de Datos con respecto a los Datos Personales del Cliente;
2. no responder a esa solicitud, excepto siguiendo las instrucciones documentadas del Cliente o según lo requieran las Leyes de Protección de Datos Aplicables, en cuyo caso HighLevel y ZenZales deberán, en la medida permitida por las Leyes de Protección de Datos Aplicables, informar al Cliente sobre dicho requisito antes de responder a la solicitud o indicar a sus Procesadores Contratados que respondan; y
3. cumplir con prontitud cualquier instrucción documentada del Cliente con respecto a responder a una solicitud para ejercer los Derechos de un Titular de Datos.

8. Violaciones de datos personales.

a. Respuesta ante Violaciones. Si HighLevel y ZenZales descubren, reciben notificación o tienen motivos para sospechar una Violación de Datos Personales que afecte a los Datos Personales del Cliente bajo su control o el de sus Encargados del Tratamiento contratados, HighLevel y ZenZales (i) implementarán inmediatamente medidas para detener el acceso no autorizado; (ii) protegerán los Datos Personales del Cliente; y (iii) notificarán al Cliente sin demora indebida y, en cualquier caso, dentro de las setenta y

dos (72) horas siguientes a la toma de conocimiento de dicha presunta Violación de Datos Personales.

b. Obligaciones en caso de violación de datos personales. Inmediatamente después de notificar una violación de datos personales, HighLevel y ZenZales deberán:

1. describir al Cliente con el mayor detalle posible: (i) la naturaleza de la violación de datos personales, (ii) cuando sea posible, las categorías y el número aproximado de sujetos de datos afectados y las categorías y el número aproximado de registros de datos personales afectados, (iii) el impacto de dicha violación de datos personales sobre el Cliente y los sujetos de datos afectados, y (iv) las medidas adoptadas o propuestas por HighLevel y ZenZales para abordar la violación de datos personales;
2. proporcionar y complementar notificaciones a medida que se disponga de información adicional;
3. ayudar al Cliente a cumplir con sus respectivas obligaciones de conformidad con las Leyes de Protección de Datos Aplicables, incluidas las obligaciones de notificar a las Autoridades de Supervisión o a los Titulares de Datos sobre una Violación de Datos Personales; y
4. utilizar esfuerzos comercialmente razonables para investigar, mitigar y remediar cada una de dichas violaciones de datos personales y evitar que vuelvan a ocurrir.

c. Sin reconocimiento de culpa. La notificación o respuesta de HighLevel y ZenZales ante una violación de datos personales en virtud de esta Sección no se interpretará como un reconocimiento por parte de HighLevel y ZenZales de cualquier culpa o responsabilidad con respecto a dicha violación.

9. Evaluación de Protección de Datos y Consulta Previa. HighLevel y ZenZales proporcionarán al Cliente la información y documentación pertinentes, y le ayudará a cumplir con sus obligaciones en relación con cualquier evaluación de protección de datos o consulta previa con las Autoridades de Control cuando así lo exija la Ley de Protección de Datos Aplicable, pero en cada caso únicamente en relación con los Datos Personales del Cliente Procesados por HighLevel y ZenZales y sus Encargados del Tratamiento, teniendo en cuenta la naturaleza del Procesamiento y la información disponible para ellos.

10. Eliminación o devolución de datos personales.

a. HighLevel y ZenZales proporcionarán al Cliente los medios técnicos, acorde con la forma en que se prestan los Servicios, para solicitar la eliminación de los Datos Personales del Cliente, con excepción de cualquier Dato Personal del Cliente que pueda conservarse de conformidad con las leyes aplicables.
b. Si el Cliente lo solicita y luego del cese de los Servicios, HighLevel y ZenZales eliminará o devolverá de inmediato todos los Datos Personales del Cliente (incluidas las copias) al Cliente, con excepción de cualquier Dato Personal del Cliente que pueda conservarse de conformidad con las leyes aplicables.
c. HighLevel y ZenZales también harán que todos los Procesadores Contratados que hayan recibido Datos Personales del Cliente eliminen o devuelvan, según corresponda, todos esos Datos Personales del Cliente, con excepción de cualquier Dato Personal del Cliente que pueda conservarse de conformidad con las leyes aplicables.
d. Esta Sección 10 no se aplica a los Datos Personales del Cliente que hayan sido archivados en sistemas de respaldo, que HighLevel y ZenZales o sus Procesadores Contratados, según corresponda, aislarán y protegerán de forma segura de cualquier Procesamiento adicional, excepto en la medida requerida por la ley aplicable.

11. Derechos de auditoría. HighLevel y ZenZales permitirán y contribuirá a las auditorías, incluidas las inspecciones remotas, realizadas por el Cliente o por un auditor designado por este (en su propio nombre o en el de sus clientes) en relación con el tratamiento de los datos personales del Cliente por parte de HighLevel y ZenZales y sus encargados del tratamiento contratados. En la medida legalmente permitida, el Cliente reembolsará a HighLevel y ZenZales el tiempo empleado en dichas auditorías, según las tarifas de servicios profesionales vigentes en ese momento, que se pondrán a disposición del Cliente si las solicita.

12. Términos específicos de la jurisdicción. En la medida en que HighLevel y ZenZales procese datos personales de clientes originados o protegidos por las leyes de protección de datos aplicables en una jurisdicción indicada en **el Anexo B** , se

aplicarán los términos y definiciones especificados en ~~el Anexo B~~ con respecto a la jurisdicción aplicable, además de los términos de este Anexo.

13. Transferencias restringidas.

a. Las transferencias restringidas de datos personales del cliente dentro del alcance de este Anexo se realizarán de conformidad con **el ~~Anexo B~~** y ~~las~~ leyes de protección de datos aplicables.

b. Si las autoridades pertinentes adoptan una nueva versión de las SCC como mecanismo legal para las Transferencias Restringidas en una jurisdicción que rige el procesamiento de Datos Personales del Cliente, se considerará que las Partes han acordado la ejecución de la nueva versión de las SCC al firmar este Anexo y, de ser necesario, HighLevel y ZenZales tendrán derecho a actualizar **el Anexo A** y **el Anexo B** (y s~~us apéndices~~) ~~en consecu~~encia.

c. Si HighLevel y ZenZales adoptan un mecanismo de transferencia alternativo, como las Normas corporativas vinculantes, durante el plazo del Acuerdo (un " **Mecanismo alternativo** "), y HighLevel y ZenZales notifican al Cliente que algunas o todas las Transferencias restringidas se pueden realizar de conformidad con las Leyes de protección de datos aplicables de conformidad con el Mecanismo alternativo, las Partes confiarán en el Mecanismo alternativo en lugar de los mecanismos de transferencia del **Anexo B** para Transferencias ~~restringid~~as a las que se aplica el Mecanismo alternativo.

d. Además, HighLevel y ZenZales cuentan con la certificación del Marco de Privacidad de Datos UE-EE. UU., la Extensión del Reino Unido al Marco de Privacidad de Datos UE-EE. UU. y el Marco de Privacidad de Datos Suiza-EE. UU. HighLevel y ZenZales se comprometen a notificar al Cliente si determina que ya no puede cumplir con su obligación de proporcionar el mismo nivel de protección que exigen los principios del Marco de Privacidad de Datos.

14. Prohibición de venta de datos personales del cliente. HighLevel y ZenZales reconocen y confirman que no reciben datos personales del cliente como contraprestación por los servicios u otros artículos que HighLevel y ZenZales le proporcionan. Entre el cliente y HighLevel y ZenZales, el cliente conserva todos los derechos e intereses sobre los datos personales del cliente. HighLevel y ZenZales se comprometen a abstenerse de realizar cualquier acción que pueda dar lugar a que

las transferencias de datos personales del cliente hacia o desde HighLevel y ZenZales se consideren venta de datos personales del cliente según la legislación aplicable en materia de protección de datos.

15. Enmienda y alojamiento en línea.

a. Sujeto a las condiciones especificadas en este Addendum, HighLevel y ZenZales pueden alojar el contenido de los anexos y apéndices de este Addendum en línea, y actualizar aún más el Addendum/dichos anexos y apéndices, siempre que se notifique previamente al Cliente.
    1. Si no se recibe ninguna objeción dentro de los catorce (14) días siguientes a la recepción de la notificación, se considerará que el Cliente ha dado su consentimiento a la actualización. Si el Cliente notifica su no aceptación, las Partes cooperarán y negociarán de buena fe respecto a cualquier actualización necesaria.
    2. Si no se llega a una solución mutuamente satisfactoria, el Cliente podrá rescindir el Acuerdo inmediatamente mediante notificación por escrito a HighLevel y ZenZales, sin que se le abonen más cargos que los acumulados hasta la fecha de rescisión. Tras la notificación de rescisión, HighLevel y ZenZales dejarán de procesar los datos personales en nombre del Cliente.
b. En la medida en que una Adenda/un anexo o apéndice esté alojado en línea, la última versión en línea tendrá prioridad sobre el anexo o apéndice pertinente dentro de esta Adenda.

16. Responsabilidad.

a. Sujeto a las Leyes de Protección de Datos Aplicables, la responsabilidad de cada Parte bajo este Anexo estará sujeta a las exclusiones y limitaciones de responsabilidad establecidas en el Acuerdo.

17. Condiciones Generales.

a. Aviso. Las Partes utilizarán el Contacto de Protección de Datos que se proporciona en **la Parte A del Anexo A** como punto de contacto para todos los asuntos relacionados con este Anexo, incluyendo la notificación de una

Violación de Datos Personales y las consultas de conformidad con los Derechos de los Titulares de los Datos.

b. Acuerdo Previo. Este Anexo sustituye y reemplaza todas las propuestas, declaraciones, materiales de venta o presentaciones, y acuerdos, tanto orales como escritos, anteriores y contemporáneos, relacionados con el objeto de este Anexo, incluyendo cualquier anexo previo sobre procesamiento de datos celebrado entre HighLevel y ZenZales y el Cliente en relación con el Acuerdo. No obstante, todas las cláusulas del Acuerdo que no se modifiquen o complementen explícitamente con las cláusulas de este Anexo permanecerán en pleno vigor y efecto, siempre que no contradigan los requisitos obligatorios de la Ley de Protección de Datos Aplicable.

c. Revisión anual. Cada Parte deberá revisar este Anexo (incluido **el Anexo A** y sus apéndices) periódicamente para garantizar que se mantenga preciso, actualizado y proporcione las garantías adecuadas para los Datos Personales. Cada Parte realizará estas revisiones cada vez que se produzca un cambio en los Datos Personales, los fines del Tratamiento, la información del Importador de Datos o cualquier evaluación de riesgos relacionada con el Tratamiento contemplado en este Anexo.

d. Conflictos . En caso de conflicto entre el Acuerdo (incluidos sus anexos, anexos y apéndices) y este Anexo, prevalecerán las disposiciones de este Anexo. En caso de conflicto o ambigüedad entre las Condiciones Específicas de la Jurisdicción y cualquier otro término de este Anexo, prevalecerán las Condiciones Específicas de la Jurisdicción aplicables.

e. Divisibilidad . Si alguna disposición de este Anexo se considera legalmente inválida o inaplicable, dicha disposición se considerará sustituida por una disposición válida y aplicable que se ajuste lo más posible a la intención de la disposición original, y el resto de este Anexo continuará vigente.

f. Incumplimiento . Si HighLevel y ZenZales determinan que ya no puede cumplir con alguna de sus obligaciones establecidas en este Anexo, la Ley de Protección de Datos Aplicable o las Cláusulas Contractuales de la UE (si corresponde), deberá (i) notificar de inmediato al Cliente dicha determinación y (ii) cesar el Tratamiento, si el Cliente lo solicita, o tomar de inmediato otras medidas razonables y apropiadas para remediar el incumplimiento.

g. Ambigüedad . HighLevel y ZenZales podrán modificar este Anexo sin previo aviso ni consentimiento del Cliente con el fin de a) subsanar cualquier ambigüedad, b) subsanar, corregir o complementar cualquier disposición defectuosa contenida en el presente, o c) establecer cualquier otra

disposición con respecto a asuntos o cuestiones que surjan en virtud de este Anexo; siempre que dicha acción no altere sustancialmente el Anexo.

h. Firma . Si acepta los términos de este Anexo en nombre de cualquiera de las Partes, declara y garantiza que tiene la autoridad para vincular a dicha Parte y a sus Afiliadas, cuando corresponda, a los términos y condiciones de este Anexo. Divulgación a las Autoridades de Supervisión . Las Partes reconocen que cualquiera de ellas podrá divulgar este Anexo y cualquier disposición de privacidad pertinente del Acuerdo a las Autoridades de Supervisión o a cualquier otro organismo judicial o regulador, a solicitud de estas.

Anexo A

Detalles del procesamiento

A. LISTA DE PARTES: **Nombre y dirección:**	**HighLevel:** HighLevel Inc. y sus afiliados relevantes 5473 Blair Rd Ste 100, PMB 383313, Dallas, Texas 75231-4227 **Cliente:** Nombre del cliente según se define en los Términos de servicio de HighLevel y sus afiliados relevantes Dirección del cliente según lo especificado en la Cuenta de plataforma del cliente.
Contacto de Protección de Datos:	**HighLevel:** Betsy Cantrell – legal@gohighlevel.com

	Cliente: Detalles de contacto del cliente, según lo especificado en la cuenta de plataforma del cliente.
Actividades relevantes para los datos transferidos:	Actividades de tratamiento relacionadas con la prestación de los Servicios, según lo establecido en el Acuerdo. El tratamiento implicará la recopilación, el almacenamiento, el registro, el contacto y la gestión de los Datos Personales del Cliente, en particular para la ejecución de campañas de marketing, la prestación de servicios de marketing y la gestión general del marketing.
Rol de control:	**El Cliente como Responsable del Tratamiento y HighLevel y ZenZales como Encargado del Tratamiento:** • En la medida en que el Cliente sea el Responsable del Tratamiento de sus Datos Personales, HighLevel y ZenZales será su Encargado del Tratamiento. **El Cliente como Encargado del Tratamiento y HighLevel y ZenZales como Subencargado del Tratamiento:** • En la medida en que el Cliente sea el Encargado del Tratamiento de sus Datos Personales, HighLevel y ZenZales serán su Subencargado del Tratamiento.
Rol de transferencia de datos:	**Alto nivel:** Importador de datos **Cliente:** Exportador de datos

B. DETALLES DEL TRATAMIENTO:

Objeto del Tratamiento:	El objeto del Tratamiento de los Datos Personales del Cliente está relacionado con la prestación de Servicios de conformidad con el Acuerdo.

Naturaleza y finalidad del tratamiento:	HighLevel y ZenZales procesarán los Datos Personales del Cliente según sea necesario para proporcionar los Servicios bajo el Acuerdo, para los fines especificados en el Acuerdo y este Anexo, y de acuerdo con las instrucciones del Cliente establecidas en este Anexo.
Criterios de retención (duración):	La duración del período en el que el Cliente accede y utiliza la plataforma HighLevel y ZenZales bajo el Acuerdo de Servicios.
Categorías de interesados:	El Cliente puede enviar Datos Personales según lo determine el Cliente, que pueden incluir, pero no se limitan a, Datos Personales relacionados con el Cliente, empresas y otras entidades que contratan con el Cliente, y usuarios de esas empresas y otras entidades.
Categorías de Datos Personales:	Según corresponda, cualquier dato personal del cliente que éste proporcione en los Servicios.
Categorías especiales de datos personales:	Las Partes no anticipan la transferencia de categorías especiales de datos, a menos que el Cliente notifique primero a HighLevel y ZenZales, en cuyo caso las Partes acuerdan aplicar restricciones y salvaguardas apropiadas teniendo en cuenta la naturaleza de los datos y los riesgos involucrados.
Frecuencia de la Transferencia:	Regular y repetitivo mientras el Cliente utilice los Servicios.
Objeto, naturaleza y duración de los encargados del tratamiento contratados:	Lo mismo que lo anterior en la medida en que dicha información se proporcione a los Procesadores Contratados a los efectos de proporcionar los Servicios.

Apéndice I del Anexo A

Medidas de seguridad técnicas y organizativas

Durante la vigencia del Acuerdo y mientras HighLevel y ZenZales tengan acceso a cualquier Dato Personal del Cliente, HighLevel y ZenZales implementarán y mantendrán al menos las siguientes (o superiores) medidas técnicas y organizativas de seguridad (" **TOMs** ") para salvaguardar dichos Datos Personales del Cliente:

Tipos de TOM	Descripción de los TOM
Medidas de seudonimización y cifrado de Datos Personales:	• Todos los datos personales en reposo están cifrados con: AES 256 CBC • Todos los datos personales en tránsito están cifrados con: TLS V1.2+.
Medidas para garantizar la confidencialidad, integridad, disponibilidad y resiliencia continuas de los sistemas y servicios de Tratamiento:	El procesador cuenta con protección de endpoints en los dispositivos de sus usuarios. El procesador cuenta con monitores de actividad para garantizar la disponibilidad y avisarle en caso de inactividad. El procesador ha implementado medidas de control de acceso, como el control de acceso basado en roles (RBAC) y la autenticación basada en subcuentas. El procesador utiliza servicios gestionados (AWS, GoogleCloud) para garantizar la integridad.
Medidas para garantizar la capacidad de restaurar la disponibilidad y el acceso a los Datos Personales de manera oportuna en caso de un incidente físico o técnico:	• Datos personales respaldados en AWS y GoogleCloud con granularidad de cinco minutos para permitir que el procesador restaure datos personales en caso de incidente.

Procesos para probar, evaluar y valorar periódicamente la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del Tratamiento:	• Análisis o auditorías de vulnerabilidades de terceros de dispositivos de infraestructura externos. • Pruebas de penetración anuales de terceros en sistemas que almacenan y procesan datos personales. • Mantener un proceso y una práctica estándar de gestión de parches para garantizar la protección de todos los dispositivos utilizados para acceder, procesar o almacenar datos personales.
Medidas de identificación y autorización de usuarios:	• El procesador utiliza tokens firmados cifrados y autorizaciones basadas en roles, así como protección con contraseña.
Medidas para la protección de Datos Personales durante la transmisión:	• Se utilizan certificados SSL y HTTPS durante la transmisión de datos personales. Protección con TLS v1.2+.
Medidas para la protección de Datos Personales durante el almacenamiento:	• Los datos personales se cifran en reposo con cifrado AES-256 CBC.
Medidas para garantizar la seguridad física de los lugares en los que se procesan datos personales:	El encargado del tratamiento utiliza servicios gestionados para garantizar la seguridad física de las ubicaciones de los servidores. Todos los datos personales se almacenan en AWS y GoogleCloud, con la seguridad física descrita en los Términos y Condiciones de AWS y GoogleCloud, respectivamente.
Medidas para garantizar el registro de eventos:	El procesador utiliza registros para todas las acciones de los usuarios y los registros de auditoría. En particular, utiliza Google Cloud Ops para la monitorización de aplicaciones e infraestructura. Además, utiliza Cloudwatch de AWS.

Medidas para garantizar la configuración del sistema, incluida la configuración predeterminada:	El procesador tiene configuraciones almacenadas en el control de versiones. Todos los contenedores se crean a partir de imágenes estandarizadas alojadas por AWS y GoogleCloud. Las actualizaciones se realizan automáticamente y son administradas por GoogleCloud. La corrección de cualquier vulnerabilidad es administrada por GoogleCloud, de acuerdo con sus políticas estándar.
Medidas para la gobernanza y gestión interna de TI y de la seguridad informática:	• El procesador cuenta con un equipo interno que gestiona TI y seguridad de TI y utiliza MSSP de terceros para supervisar el SOC.
Medidas para la certificación/aseguramiento de procesos y productos:	• El Grupo de Cumplimiento ha emitido al Procesador un Certificado de Sello de Cumplimiento HIPAA.
Medidas para garantizar la minimización de datos:	• Requisito mínimo de datos establecido por el Encargado del Tratamiento. Los usuarios pueden optar por no introducir datos personales en los campos opcionales.
Medidas para garantizar la calidad de los datos:	El procesador permite a los clientes actualizar sus datos personales relevantes a la fecha más reciente y utiliza autenticación de dos factores. La monitorización de aplicaciones se realiza mediante Google Cloud y monitores personalizados.
Medidas para garantizar la retención limitada de datos:	• El administrador del cliente puede configurar la retención de datos con respecto a personas específicas.
Medidas para garantizar la rendición de cuentas:	• El acceso del procesador a los datos personales está restringido según el rol.
Medidas para permitir la portabilidad de	Los clientes pueden descargar sus datos personales desde el Servicio. Pueden solicitar una copia o la eliminación de sus datos personales al finalizar la relación.

datos y garantizar el borrado:	El procesador utiliza tickets de soporte para garantizar lo anterior.
Otro:	Los clientes pueden descargar sus datos personales desde el Servicio. Los administradores de clientes pueden configurar la retención de datos para el personal despedido. Preguntas frecuentes y tickets de soporte para consultas específicas no abordadas en el material adicional del sitio web de soporte al cliente/producto del Encargado.
Información sobre los TOM de los Encargados del Tratamiento contratados:	Establecido en **la Parte B del Anexo A.**

Anexo B

Términosespecíficosdelajurisdicción

1. Australia. Cuando corresponda, el procesamiento de los datos personales del cliente se ajustará a los Principios de Privacidad de Australia, la Ley de Privacidad de Australia (1988) y cualquier otra ley, reglamento o decreto australiano aplicable relativo a la protección de dicha información.

2. Brasil. Siempre que el Tratamiento conforme a la Adenda se encuentre dentro del ámbito de aplicación de la Ley General de Protección de Datos de Brasil, la Ley n.º 13.709 del 14 de agosto de 2018 y cualquier otra ley, reglamento o decreto aplicable de Brasil relativo a la protección de dicha información (en conjunto, las «Leyes de Protección de Datos de Brasil»), las disposiciones de la Adenda y de esta Sección se aplicarán a dicho Tratamiento.

a. Transferencias Restringidas. En lo que respecta a cualquier Transferencia Restringida sujeta a la Ley de Protección de Datos de Brasil, se aplicará uno

de los siguientes mecanismos de transferencia, en el siguiente orden de precedencia:

1. Una decisión de adecuación válida adoptada por la Autoridad de Protección de Datos de Brasil ("ANDP") con base en la Resolución 19/2024;
2. Las Cláusulas Contractuales Estándar adoptadas por ANDP de tiempo en tiempo;
3. El reconocimiento de una Cláusula Contractual Estándar extranjera que proporcione un nivel de protección equivalente a las Cláusulas Contractuales Estándar brasileñas por la ANDP; o
4. Cualquier otro mecanismo lícito de transferencia de datos, conforme a lo establecido en las Leyes de Protección de Datos brasileñas, según el caso.

b. Cláusulas contractuales estándar.

1. La Adenda incorpora por referencia las Cláusulas Contractuales Tipo Brasileñas, incluida la Sección II en su totalidad. Se considera que las Partes han aceptado, ejecutado y firmado las Cláusulas Contractuales Tipo Brasileñas en su totalidad, cuando sea necesario.
2. Las Partes acuerdan que cualquier referencia a cláusulas y opciones dentro de las Cláusulas Contractuales Estándar Brasileñas se considerarán las mismas que las referencias cognadas y correspondientes dentro de cualquier Cláusula Contractual Estándar apropiada y actualizada que pueda aplicarse en ese momento de conformidad con la Adenda.
3. A los efectos de las Cláusulas Contractuales Tipo Brasileñas y cualquier Cláusula Contractual Tipo sustancialmente similar que puedan adoptar las autoridades pertinentes en el futuro, las Partes acuerdan aplicar lo siguiente:
    i. Cláusula 1: El contenido de la Cláusula 1 se establece en la **Sección A del Anexo A** del Anexo.
    ii. Cláusula 2: El contenido de la Cláusula 2 se establece en **la Sección B del Anexo A** del Anexo.
    iii. Cláusula 3: Las Partes eligen la Opción B. El proceso para la transferencia posterior se describe en la Sección 6 del Anexo.
    iv. Cláusula 4: Las Partes eligen la Opción A.
        A. Cláusula 4.1 (a): Las Partes eligen al Exportador.
        B. Cláusula 4.1 (b): Las Partes eligen al Exportador.
        C. Cláusula 4.1 (c): Las Partes eligen al Exportador.

v. Sección III: El contenido del Anexo II se establece en **el Apéndice I del Anexo A** de la Adenda.

4. En los casos en que se apliquen las Cláusulas Contractuales Tipo Brasileñas y haya un conflicto entre los términos del Addendum y los términos de las Cláusulas Contractuales Tipo Brasileñas, los términos de las Cláusulas Contractuales Tipo Brasileñas prevalecerán con respecto a la Transferencia Restringida en cuestión.

3. Canadá. Cuando corresponda, el procesamiento de los datos personales del cliente deberá cumplir con la Ley Federal Canadiense de Protección de la Información Personal y de Documentos Electrónicos, así como con cualquier otra ley, reglamento o decreto aplicable de Canadá relativo a la protección de dicha información.

4. Espacio Económico Europeo.

a. **Definiciones.**

1. " **EEE** " significa el Espacio Económico Europeo, formado por los Estados miembros de la UE, Islandia, Liechtenstein y Noruega.
2. " **Leyes de protección de datos del EEE"** significa el RGPD de la UE y todas las leyes y regulaciones de la UE y los países del EEE aplicables al procesamiento de datos personales del cliente.
3. " **Cláusulas contractuales estándar UE 2021** " significa las cláusulas contractuales adoptadas por la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, sobre cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
4. " **RGPD UE** " (tal como se utiliza en el Anexo) significa el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, con sus modificaciones posteriores.

b. **Transferencias restringidas.**

1. Con respecto a cualquier Transferencia Restringida sujeta a las Leyes de Protección de Datos del EEE entre las Partes, se aplicará uno de los siguientes mecanismos de transferencia, en el siguiente orden de precedencia:

i. una decisión de adecuación válida adoptada por la Comisión Europea sobre la base del artículo 45 del RGPD de la UE;
ii. las cláusulas contractuales estándar apropiadas adoptadas por la Comisión Europea en cada momento; o
iii. cualquier otro mecanismo legal de transferencia de datos, según lo establecido en las Leyes de Protección de Datos del EEE.

c. **Cláusulas contractuales estándar.**

1. El presente Anexo incorpora por referencia las CCC. Se considera que las Partes han aceptado, ejecutado y firmado las CCC, cuando sea necesario, en su totalidad (incluidos sus anexos).
2. Las Partes acuerdan que cualquier referencia a cláusulas, anexos, módulos y opciones dentro de esta Sección se considerarán iguales a las referencias correspondientes y afines dentro de cualquier SCC apropiado y actualizado que pueda aplicarse en ese momento de conformidad con el Addendum.
3. A los efectos de las CCT UE 2021 y de cualquier CCT sustancialmente similar que puedan adoptar las autoridades pertinentes en el futuro:
    i. Las Partes acuerdan aplicar el siguiente módulo:
        A. Módulo Dos con respecto a las Transferencias Restringidas de Controlador a Encargado del Tratamiento; y
        B. Módulo tres con respecto a las transferencias restringidas de procesador a subprocesador
    ii. Cláusula 7: Las Partes optan por incluir la cláusula de acoplamiento opcional;
    iii. Cláusula 9(a): Las Partes eligen la opción 2, “Autorización General por Escrito”, y el plazo establecido en la Sección 6.3 del Addendum (Los procedimientos para la designación y notificación de nuevos Procesadores Contratados se establecen con más detalle en la Sección 6 del Addendum);
    iv. Cláusula 11: Las Partes optan por no incluir el lenguaje opcional relativo al uso de un organismo independiente de resolución de disputas;
    v. Cláusula 13 (Anexo IC): La Autoridad de Control competente es el Comité Europeo de Protección de Datos;
    vi. Cláusula 17: Las CCE se regirán por las leyes de la República de Irlanda;

vii. Cláusula 18: Cualquier disputa que surja de las CCC se resolverá en los tribunales de la República de Irlanda;

viii. Anexo I(A y B): El contenido del Anexo I(A) y (B) se establece en el Anexo A;

ix. Anexo II: El contenido del Anexo II se establece en el Apéndice I del Anexo A.

4. Los términos contenidos en el Anexo C del Addendum complementan las CCE.
5. En los casos en que se apliquen las CSC y exista un conflicto entre los términos del Anexo y los términos de las CSC, prevalecerán los términos de las CSC con respecto a la Transferencia Restringida en cuestión.

5. Suiza.

a. **Definiciones.**

1. " **Cláusulas contractuales estándar UE 2021** " significa las cláusulas contractuales adoptadas por la Decisión de Ejecución (UE) 2021/914 de la Comisión, de 4 de junio de 2021, sobre cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.
2. " **FDPIC** " significa el Comisionado Federal Suizo de Protección de Datos e Información.
3. " **Leyes suizas de protección de datos** " incluye la Ley Federal de Protección de Datos del 19 de junio de 1992 ("FADP") y la Ordenanza de la Ley Federal de Protección de Datos.

b. **Transferencias restringidas.**

1. Con respecto a cualquier Transferencia Restringida sujeta a las Leyes Suizas de Protección de Datos entre las Partes, se aplicará uno de los siguientes mecanismos de transferencia, en el siguiente orden de precedencia:

i. una decisión de adecuación válida adoptada por el FDPIC sobre la base del artículo 6 del FADP;

ii. las cláusulas contractuales estándar (SCC) apropiadas adoptadas por el FDPIC de vez en cuando; o

iii. cualquier otro mecanismo de transferencia legal, según lo establecido en las leyes suizas de protección de datos.

c. **Cláusulas contractuales estándar.**

1. La Adenda incorpora por referencia las CCT UE 2021, adoptadas para su uso por el FDPIC con ciertas modificaciones. Se considera que las Partes han aceptado, ejecutado y firmado las CCT UE 2021, cuando sea necesario, en su totalidad (incluidos sus anexos).
2. Las Partes incorporan y adoptan las Condiciones Generales de Contratación de la UE 2021 para Transferencias Restringidas sujetas a las Leyes de Protección de Datos Suizas de la misma manera establecida en la Sección 7.3 de estos Términos Específicos de Jurisdicción, ~~sujeto a lo siguiente:~~
   i. Cláusula 13 (Anexo IC): La autoridad competente será el FDPIC. Nada de lo dispuesto en la designación de la Autoridad de Supervisión competente por las Partes se interpretará como impedimento para que los interesados en Suiza soliciten asist~~encia al FDPIC~~.
   ii. Cláusu~~la 17: Las CC~~C se regirán por las leyes de Suiza;
   iii. Cláusula 18: Cualquier controversia derivada de las CCC se resolverá en los tribunales de Suiza. La elección de foro por las Partes no podrá interpretarse como una prohibición a los Interesados con residencia habitual en Suiza de demandar sus derechos en Suiza.
   iv. las referencias al "Reglamento (UE) 2016/679" y a los artículos específicos del mismo se sustituirán por referencias al FADP y a los artículos o secciones equivalentes del mismo, en la medida en que existan Transferencias Restringidas sujetas a las Leyes Suizas de Protección de Datos; y
   v. Las SCC también protegen los datos de las personas jurídicas hasta la entrada en vigor de la FADP revisada.
3. En los casos en que se apliquen las CSC y exista un conflicto entre los términos del Anexo y los términos de las CSC, prevalecerán los términos de las CSC con respecto a la Transferencia Restringida en cuestión.

6. Reino Unido.

a. **Definiciones.**

1. " **Cláusulas contractuales estándar UE 2021** " significa las cláusulas contractuales adoptadas por la Decisión de Ejecución (UE) 2021/914 de

la Comisión, de 4 de junio de 2021, sobre cláusulas contractuales tipo para la transferencia de datos personales a terceros países de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo.

2. Las " **Leyes de protección de datos del Reino Unido** " incluyen la Ley de protección de datos de 2018 y el RGPD del Reino Unido.
3. " **RGPD del Reino Unido** " (tal como se utiliza en el Anexo) significa el Reglamento General de Protección de Datos del Reino Unido, tal como forma parte de la legislación de Inglaterra y Gales, Escocia e Irlanda del Norte en virtud de la sección 3 de la Ley de Retirada de la Unión Europea de 2018.
4. " **UK ICO** " significa la Oficina del Comisionado de Información del Reino Unido.
5. " **Anexo de Transferencia del Reino Unido** " (tal como se utiliza en esta Sección) significa el Anexo de Transferencia Internacional de Datos a las Cláusulas Contractuales Estándar de la Comisión Europea emitido de conformidad con la Sección 119A(1) de la Ley de Protección de Datos de 2018 y aprobado por el Parlamento del Reino Unido.]

b. **Transferencias restringidas.**
   1. Con respecto a cualquier Transferencia Restringida sujeta a las Leyes de Protección de Datos del Reino Unido entre las Partes, se aplicará uno de los siguientes mecanismos de transferencia, en el siguiente orden de precedencia:
      i. una decisión de adecuación válida adoptada de conformidad con el artículo 45 del RGPD del Reino Unido;
      ii. las SCC apropiadas adoptadas por la ICO del Reino Unido en ese momento (en la medida en que las actividades de procesamiento del importador de datos no estén sujetas al RGPD del Reino Unido en virtud de la aplicación del Artículo 3(2) del RGPD del Reino Unido); o
      iii. cualquier otro mecanismo legal de transferencia de datos, según lo establecido en las Leyes de Protección de Datos del Reino Unido.

c. Anexo sobre cláusulas contractuales subordinadas de la UE de 2021 y transferencias al Reino Unido.
   1. El presente Anexo incorpora por referencia las CCC UE 2021, adoptadas para su uso por la ICO del Reino Unido con ciertas modificaciones y la adición del Anexo de Transferencias del Reino

Unido. Se considera que las Partes han aceptado, ejecutado y firmado las CCC UE 2021, cuando sea necesario, en su totalidad (incluidos sus anexos).

2. A los efectos de las tablas del Anexo de Transferencia del Reino Unido:
   i. Tabla 1: El contenido de la Tabla 1 se establece en la Parte A del Anexo A;
   ii. Tabla 2: El contenido de la Tabla 2 se incorpora y adopta en lo que respecta a las Transferencias Restringidas sujetas a las Leyes de Protección de Datos del Reino Unido exactamente de la misma manera establecida en la Sección 7.3 de estos Términos Específicos de la Jurisdicción.
   iii. Tabla 3: El contenido de la Tabla 3 (Anexos 1A, 1B, II y III) se establece de la siguiente manera:
      - Anexo 1: El contenido del Anexo 1 se establece en el Anexo A;
      - Anexo II: El contenido del Anexo II se establece en el Apéndice I del Anexo A; y
   iv. Tabla 4: Las Partes acuerdan que ninguna de ellas podrá rescindir el Anexo de Transferencia del Reino Unido.
3. Las Partes incorporan y adoptan las Condiciones Generales de Contratación de la UE 2021 en lo que respecta a las Transferencias Restringidas sujetas a las Leyes de Protección de Datos del Reino Unido exactamente de la misma manera establecida en la Sección 7.3 de estos Términos Específicos de Jurisdicción, sujeto a lo siguiente:
   i. Cláusula 13 (Anexo IC): La autoridad competente será la ICO del Reino Unido;
   ii. Cláusula 17: Las CCE UE 2021, incluido el Anexo de Transferencia del Reino Unido incorporado, se regirán por las leyes de Inglaterra y Gales; y
   iii. Cláusula 18: Cualquier controversia derivada de las CCC o del Anexo de Transferencia del Reino Unido incorporado se resolverá en los tribunales de Inglaterra y Gales. El interesado también podrá interponer acciones legales contra el exportador o el importador de datos ante los tribunales de cualquier país del Reino Unido. Las partes acuerdan someterse a la jurisdicción de dichos tribunales.
4. Los términos contenidos en **el Anexo C** del Anexo complementan las CCE.

5. En los casos en que se apliquen las CCE, junto con el Anexo de Transferencia del Reino Unido, y exista un conflicto entre los términos del Anexo y los términos de las CCE o el Anexo de Transferencia del Reino Unido, prevalecerán los términos del Anexo de Transferencia del Reino Unido con respecto a la Transferencia Restringida en cuestión.

7. Reino Unido.

a. **Aplicabilidad.** Siempre que el Tratamiento conforme al Anexo se encuentre dentro del ámbito de aplicación de las Leyes de Protección de Datos de Estados Unidos (definidas a continuación), las disposiciones del Anexo y de esta Sección se aplicarán a dicho Tratamiento.

b. **Definiciones.**

1. Las " **Leyes de Protección de Datos de Estados Unidos** " incluyen, individual y colectivamente, las leyes, leyes y reglamentos estatales y federales promulgados en los Estados Unidos de América que se aplican al Tratamiento de Datos Personales, con sus modificaciones periódicas. Dichas leyes incluyen, entre otras:

i. la Ley de Privacidad del Consumidor de California de 2018, con sus modificaciones, incluidas las modificaciones realizadas por la Ley de Derechos de Privacidad de California de 2020 (Código Civil de California § 1798.100 y siguientes), y las Regulaciones de la Ley de Privacidad del Consumidor de California, junto con todas las regulaciones de implementación;

ii. Leyes de privacidad estatales similares, incluidas, entre otras, la Ley de Privacidad de Colorado, la Ley de Connecticut sobre Privacidad de Datos Personales y Monitoreo en Línea, la Ley de Privacidad de Datos Personales de Delaware, la Ley de Protección de Datos del Consumidor de Iowa, la Ley de Privacidad de Datos en Línea de Maryland, la Ley de Privacidad de Datos del Consumidor de Minnesota, la Ley de Privacidad de Datos del Consumidor de Montana, la Ley de Privacidad de Datos de Nebraska, la Ley de Privacidad de New Hampshire, el Proyecto de Ley 332 del Senado de Nueva Jersey, la Ley de Privacidad del Consumidor de Oregón, la Ley de Protección de la Información de Tennessee, la Ley de Privacidad y Seguridad de Datos de Texas, la Ley de Privacidad del Consumidor de Utah y la Ley de Protección de Datos del Consumidor de Virginia.

2. " **Violación de datos personales** " (tal como se utiliza en el Anexo) incluye "Violación de seguridad" y "Violación de la seguridad del sistema" según se define en las leyes de protección de datos aplicables de los Estados Unidos.
3. Los términos " **Propósito comercial** ", " **Propósito comercial** ", " **Vender** " y " **Compartir** " tendrán los mismos significados que en las Leyes de protección de datos aplicables de los Estados Unidos, y sus términos cognados y correspondientes se interpretarán en consecuencia.

c. Tratamiento de Datos Personales del Cliente.
1. El Cliente divulga sus Datos Personales a HighLevel y ZenZales únicamente para: (i) Fines Comerciales válidos; y (ii) para permitir que HighLevel y ZenZales presten los Servicios.
2. HighLevel y ZenZales no podrán: (i) vender ni compartir datos personales del cliente; (ii) conservar, utilizar ni divulgar datos personales del cliente, salvo para prestar los servicios especificados en el Acuerdo o según lo permitan las leyes de protección de datos de Estados Unidos; ni (iii) combinar datos personales del cliente con otra información que HighLevel y ZenZales procesen en nombre de otras personas o que HighLevel y ZenZales recopilen directamente del titular de los datos, salvo según lo permitan las leyes de protección de datos de Estados Unidos. HighLevel y ZenZales certifican que comprenden estas prohibiciones y se comprometen a cumplirlas.

d. **Terminación.** Tras la terminación del Acuerdo, HighLevel y ZenZales deberán, tan pronto como sea razonablemente posible, destruir todos los Datos Personales del Cliente que haya Procesado en nombre del Cliente tras la finalización de la prestación de los Servicios relacionados con el Procesamiento, así como todas las copias de dichos Datos Personales, a menos que la legislación aplicable exija o permita su almacenamiento.

Apéndice I del Anexo B

Cláusulas complementarias a las cláusulas contractuales tipo

Mediante este Anexo C (este "Anexo"), las Partes otorgan garantías y reparaciones adicionales a los Titulares de Datos cuyos Datos Personales se transfieren de

conformidad con las CCC. Este Anexo complementa y forma parte de las CCC que puedan aplicarse a la Transferencia Restringida, pero no las modifica ni las modifica.

1. Definiciones. A los efectos de la interpretación de este Anexo, los siguientes términos tendrán el significado que se establece a continuación:

a. " **EO 12333** " significa la Orden Ejecutiva 12333 de los EE. UU.
b. " **FISA** " significa Ley de Vigilancia de Inteligencia Extranjera de Estados Unidos.
c. " **Sentencia Schrems II** " significa la sentencia del Tribunal de Justicia de la Unión Europea en el asunto C-311/18, Comisionado de Protección de Datos contra Facebook Ireland Limited y Maximilian Schrems.

2. Aplicabilidad de las leyes de vigilancia.

a. El Importador de Datos declara y garantiza que, a la Fecha de Entrada en Vigencia, no ha recibido ninguna orden de seguridad nacional del tipo descrito en los Párrafos 150 a 202 de la sentencia Schrems II.
b. El Importador de Datos declara que cree razonablemente que no es elegible para que se le exija proporcionar información, instalaciones o asistencia de ningún tipo según la Sección 702 de la FISA porque:
    i. Ningún tribunal ha determinado que el Importador de Datos sea una entidad elegible para recibir un proceso legal emitido bajo la Sección 702 de la FISA: (i) un "proveedor de servicios de comunicación electrónica" dentro del significado de 50 USC § 1881(b)(4); o (ii) una entidad que pertenece a cualquiera de las categorías de entidades descritas dentro de esa definición; y
    ii. Si se determinara que el Importador de Datos es elegible para el proceso bajo la Sección 702 de FISA, lo cual cree que no es el caso, no es, sin embargo, el tipo de proveedor que es elegible para estar sujeto a la recopilación UPSTREAM de conformidad con la Sección 702 de FISA, como se describe en los párrafos 62 y 179 de la sentencia Schrems II.
c. La EO 12333 no otorga al gobierno de EE. UU. la capacidad de ordenar o exigir que el Importador de Datos brinde asistencia para la recopilación masiva de información y el Importador de Datos no tomará ninguna medida de conformidad con la EO 12333.

3. Puertas traseras.

a. El Importador de Datos certifica que:
   i. no ha creado deliberadamente puertas traseras o programación similar para agencias gubernamentales que podrían usarse para acceder a los sistemas del Importador de Datos o a los Datos Personales del Cliente sujetos a las SCC;
   ii. no ha creado ni cambiado intencionalmente sus procesos comerciales de una manera que facilite el acceso gubernamental a los Datos Personales o sistemas del Cliente; y
   iii. La legislación nacional o la política gubernamental no requieren que el Importador de Datos cree o mantenga puertas traseras o facilite el acceso a los Datos Personales o sistemas del Cliente.

b. El Exportador de Datos tendrá derecho a rescindir el contrato con poca antelación en los casos en que el Importador de Datos no revele la existencia de una puerta trasera o programación similar o procesos comerciales manipulados o cualquier requisito para implementar cualquiera de estos o no informe rápidamente al Exportador de Datos una vez que tenga conocimiento de su existencia.

4. Información sobre prohibiciones legales. El Importador de Datos proporcionará al Exportador de Datos información sobre las prohibiciones legales que le impiden proporcionar información en virtud de este Anexo. El Importador de Datos podrá elegir el medio para proporcionar esta información.

5. Medidas adicionales para prevenir el acceso. Sin perjuicio de la aplicación de las medidas de seguridad establecidas en el Anexo, el Importador de Datos implementará políticas internas que establezcan lo siguiente:

a. El Importador de Datos debe exigir un documento oficial firmado emitido de conformidad con las leyes aplicables del tercero solicitante antes de considerar una solicitud de acceso a los Datos Personales del Cliente transferidos;
b. El Importador de Datos será notificado al recibir cada solicitud o pedido de Datos Personales del Cliente transferidos;

c. El Importador de Datos examinará cada solicitud para verificar su validez legal y, como parte de ese procedimiento, rechazará cualquier solicitud que considere inválida; Si el Importador de Datos está legalmente obligado a
d. cumplir una orden, responderá de la forma más específica posible a la solicitud; y Si el Importador de Datos recibe una solicitud de las autoridades
e. públicas para cooperar de forma voluntaria, los Datos Personales del Cliente transmitidos en texto simple solo podrán proporcionarse a las autoridades públicas con el acuerdo expreso del Exportador de Datos.

6. Terminación. Este Anexo terminará automáticamente con respecto al Tratamiento de Datos Personales del Cliente transferidos al amparo de las Cláusulas Contractuales Si la Autoridad Supervisora o un regulador competente aprueba un mecanismo de transferencia diferente que sea aplicable a las Transferencias Restringidas amparadas por las Cláusulas Contractuales (y si dicho mecanismo se aplica solo a algunas de las transferencias de datos, este Anexo terminará únicamente con respecto a dichas transferencias) y que no requiera las garantías adicionales establecidas en este Anexo.