Términos del Tratamiento de Datos de Google Ads

Google y la contraparte que acepta los presentes términos (el "**Cliente**") han suscrito un contrato de prestación de Servicios del Encargado del Tratamiento (con sus enmiendas puntuales, el "**Contrato**").

Los presentes Términos del Tratamiento de Datos de Google Ads (incluidos los apéndices, los "**Términos del Tratamiento de Datos**") se suscriben entre Google y el Cliente, y complementan al Contrato. Estos Términos del Tratamiento de Datos entrarán en vigor y sustituirán a todos los términos aplicables anteriormente relacionados con su objeto (incluidos cualquier adenda de tratamiento de datos o cualquier anexo de tratamiento de datos que estén relacionados con los Servicios del Encargado del Tratamiento) a partir de la Fecha de Entrada en Vigor de los Términos.

Si usted acepta estos Términos del Tratamiento de Datos en nombre del Cliente, usted garantiza que a) tiene plena autoridad legal para que estos Términos del Tratamiento de Datos sean vinculantes para el Cliente, b) ha leído y comprende estos Términos del Tratamiento de Datos y c) los acepta en nombre del Cliente. Si no tiene la autoridad legal para que estos Términos del Tratamiento de Datos sean vinculantes para el Cliente, no los acepte.

1. Introducción

Estos Términos del Tratamiento de Datos reflejan el acuerdo entre las partes con respecto a los términos que rigen el tratamiento de determinados datos en relación con la Legislación Europea de Protección de Datos y cierta Legislación No Europea de Protección de Datos.

2. Definiciones e interpretación

2.1 En estos Términos del Tratamiento de Datos:

"**Autoridad de Control**" hace referencia, según corresponda, a) a una "autoridad de control" según se define en el RGPD de la UE y/o b) al "Comisario" según se define en el RGPD del Reino Unido y/o la FDPA de Suiza.

"**Certificación ISO 27001**" hace referencia a la certificación ISO/IEC 27001:2013 o una certificación comparable para los Servicios del Encargado del Tratamiento.

"**Cláusulas Contractuales Tipo del Cliente**" hace referencia a las SCCs (Responsable del Tratamiento de Datos al Encargado del Tratamiento), las SCCs (Encargado del Tratamiento al Responsable del Tratamiento de Datos), y/o las SCCs (Encargado del Tratamiento al Encargado del Tratamiento), según corresponda.

"**Datos Personales del Cliente**" hace referencia a los datos personales tratados por Google en nombre del Cliente cuando Google proporciona Servicios del Encargado del Tratamiento.

"**Dirección de Correo Electrónico de Notificaciones**" hace referencia a la dirección de correo electrónico designada por el Cliente mediante la interfaz de usuario de los Servicios del Encargado del Tratamiento u otros medios proporcionados por Google para recibir determinadas notificaciones de Google relacionadas con estos Términos del Tratamiento de Datos.

"**Documentación de Seguridad**" hace referencia al certificado emitido para la certificación ISO 27001 y cualquier otra certificación o documentación de seguridad que Google pueda ofrecer en relación con los Servicios del Encargado del Tratamiento.

"**EEE**" hace referencia al Espacio Económico Europeo.

"**Entidad de Google**" hace referencia a Google LLC (anteriormente conocida como Google Inc.), Google Ireland Limited o cualquier otra entidad que, directa o indirectamente, controle a Google LLC, esté controlada por Google LLC o esté sujeta al mismo control que Google LLC.

"**FDPA de Suiza**" hace referencia a la Ley Federal de Protección de Datos del 19 de junio de 1992 (Suiza).

"**Fecha de Entrada en Vigor de los Términos**" hace referencia a lo siguiente, según corresponda:

(a) El 25 de mayo del 2018, si el Cliente hizo clic para aceptar o las partes acordaron estos Términos del Tratamiento de Datos en dicha fecha o antes de ella.

(b) La fecha en la que el Cliente haya hecho clic para aceptar o en la que las partes hayan acordado estos Términos del Tratamiento de Datos, si dicha fecha es posterior al 25 de mayo del 2018.

"**Google**" hace referencia a la Entidad de Google que sea parte del Contrato.

"**Herramienta del Interesado**" hace referencia a una herramienta (si la hubiera) que una Entidad de Google pone a disposición de los interesados y que permite a Google responder de manera directa estandarizada a determinadas solicitudes de los interesados en relación con los Datos Personales del Cliente (por ejemplo, en relación con las configuración de la publicidad online o con un complemento de inhabilitación para navegadores).

"**Incidente de Datos**" hace referencia a una quiebra de la seguridad de Google que provoque la destrucción, la pérdida, la alteración, la divulgación no autorizada o el acceso accidentales o ilegales a Datos Personales del Cliente en sistemas gestionados o controlados por Google. No se considerarán "Incidentes de Datos" los intentos fallidos ni las actividades que no pongan en riesgo la seguridad de los Datos Personales del Cliente, incluidos los intentos fallidos de inicio de sesión, los pings, las exploraciones de puertos, los ataques de denegación de servicio y otros ataques de red que se produzcan en cortafuegos o en sistemas en red.

"**Instrucciones**" tiene el significado que se le atribuye en la sección 5.2 (Instrucciones del Cliente).

"**Legislación Europea de Protección de Datos**" hace referencia, según corresponda, a) al RGPD y/o b) a la FDPA de Suiza.

"**Legislación No Europea de Protección de Datos**" hace referencia a las leyes de protección de datos o de privacidad que se encuentran en vigor fuera del EEE, Suiza y Reino Unido.

"**Leyes Europeas**" hace referencia, según corresponda, a) a la legislación de la UE o de un Estado miembro de la UE (si se aplica el RGPD de la UE al tratamiento de Datos Personales del Cliente) y b) a la legislación del Reino Unido o de una parte del Reino Unido (si se aplica el RGPD del Reino Unido al tratamiento de Datos

Personales del Cliente).

"**Medidas de Seguridad**" tiene el significado que se le atribuye en la sección 7.1.1 (Medidas de Seguridad de Google).

"**Nuevo Subencargado del Tratamiento**" tiene el significado que se le atribuye en la sección 11.1 (Consentimiento de contratación de un Subencargado del Tratamiento).

"**País Adecuado**" hace referencia a lo siguiente:

(a) En relación con los datos tratados sujetos al RGPD de la UE: el EEE o un país o territorio reconocido por garantizar una protección de datos adecuada de acuerdo con el RGPD de la UE.

(b) En relación con los datos tratados sujetos al RGPD del Reino Unido: el Reino Unido o un país o territorio reconocido por garantizar una protección de datos adecuada de acuerdo con el RGPD de Reino Unido;

(c) En relación con los datos tratados sujetos a la Ley Federal de Protección de Datos de Suiza (FDPA, por sus siglas en inglés): Suiza; un país o territorio que esté: i) incluido en la lista de estados cuya legislación asegure un nivel adecuado de protección de acuerdo con lo publicado por el Comisario Federal de Protección de Datos e Información de Suiza, o ii) reconocido por garantizar una protección de datos adecuada por el Consejo Federal suizo en virtud de la FDPA de Suiza,

en cada caso, aparte de basarse en un marco de protección de datos.

"**Producto Adicional**" hace referencia a un producto, servicio o aplicación proporcionado por Google o por un tercero que a) no forme parte de los Servicios del Encargado del Tratamiento y b) sea accesible para su uso dentro de la interfaz de usuario de los Servicios del Encargado del Tratamiento o esté integrado en ellos.

"**RGPD**" hace referencia, según corresponda, a) al RGPD de la UE y/o b) al RGPD del Reino Unido.

"**RGPD de la UE**" hace referencia al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo del 27 de abril del 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de esos datos, y por el que se deroga la Directiva 95/46/CE.

"**RGPD de Reino Unido**" hace referencia al RGPD de la UE tal y como se ha enmendado e incorporado a la legislación del Reino Unido en virtud de la ley del 2018 sobre la salida del Reino Unido de la Unión Europea, así como a la legislación secundaria aplicable que se haya creado en virtud de dicha ley.

"**SCCs**" hace referencia a las Cláusulas Contractuales Tipo del Cliente y/o las Cláusulas Contractuales Tipo (Encargado del Tratamiento de la UE al Encargado del Tratamiento, Exportador de Google), según corresponda.

"**SCCs (Encargado del Tratamiento al Encargado del Tratamiento)**" hace referencia a los términos incluidos en business.safety.google/adsprocessorterms/sccs/p2p.

"**SCCs (Encargado del Tratamiento al Encargado del Tratamiento, Exportador de Google)**" hace referencia a los términos incluidos en business.safety.google/adsprocessorterms/sccs/p2p-intra-group.

"**SCCs (Encargado del Tratamiento al Responsable del Tratamiento de Datos)**" hace referencia a los términos incluidos en business.safety.google/adsprocessorterms/sccs/p2c.

"**SCCs (Responsable del Tratamiento de Datos al Encargado del Tratamiento)**" hace referencia a los términos incluidos en business.safety.google/adsprocessorterms/sccs/c2p.

"**Servicios del Encargado del Tratamiento**" hace referencia a los servicios aplicables que se indican en business.safety.google/adsservices.

"**Solución Alternativa de Transferencia**" hace referencia a una solución, diferente a las Cláusulas Contractuales Tipo (SCC, por sus siglas en inglés), que permite la transferencia legítima de datos personales a un tercer país de acuerdo con la Legislación Europea de Protección de Datos, por ejemplo, un marco de protección de datos reconocido que garantice que las entidades participantes ofrecen una protección adecuada.

"**Subencargados del Tratamiento**" hace referencia a terceros autorizados en virtud de estos Términos del Tratamiento de Datos para tener acceso lógico a los Datos Personales del Cliente y tratarlos con la finalidad de prestar parte de los Servicios del Encargado del Tratamiento y cualquier asistencia técnica relacionada.

"**Términos Adicionales para Legislación No Europea de Protección de Datos**" hace referencia a los términos adicionales que se mencionan en el apéndice 3, que reflejan el acuerdo de las partes con respecto a los términos que rigen el tratamiento de determinados datos relacionados con alguna Legislación No Europea de Protección de Datos.

"**Vigencia**" hace referencia al periodo desde la Fecha de Entrada en Vigor de los Términos hasta el final de la prestación por parte de Google de los Servicios del Encargado del Tratamiento en virtud del Contrato.

2.2 Los términos "**responsable del tratamiento de datos**", "**interesado**", "**datos personales**", "**tratamiento**" y "**encargado del tratamiento**", tal y como se usan en estos Términos del Tratamiento de Datos, tienen los significados que se les atribuyen en el RGPD, y los términos "**importador de datos**" y "**exportador de datos**" tienen los significados que se les atribuyen en las SCCs correspondientes.

2.3 Las palabras "**incluir**" e "**incluidos**" significan "incluidos, entre otros". Todos los ejemplos que se incluyen en estos Términos del Tratamiento de Datos son ilustrativos y no pueden considerarse como únicos ejemplos de un concepto concreto.

2.4 Todas las referencias a un marco legal, estatuto u otra disposición legislativa es una referencia a la misma con sus ocasionales enmiendas o nuevas promulgaciones.

2.5 En caso de que alguna versión traducida de estos Términos del Tratamiento de Datos no coincida con la versión en inglés, prevalecerá la versión en inglés.

3. Duración de estos Términos del Tratamiento de Datos

Estos Términos del Tratamiento de Datos tendrán efecto a partir de la Fecha de Entrada en Vigor de los Términos. Independientemente de si el Contrato se ha resuelto o ha vencido, estos Términos del Tratamiento de Datos permanecerán en vigor hasta que Google elimine todos los Datos Personales del Cliente, momento en el que vencerán automáticamente los Términos del Tratamiento de Datos, tal y como se describe en dichos Términos.

4. Aplicación de estos Términos del Tratamiento de Datos

4.1 **Aplicación de la Legislación Europea de Protección de Datos**. Las secciones de la 5 (Tratamiento de datos) a la 12 (Ponerse en contacto con Google, registros de

tratamiento), ambas inclusive, solo se aplicarán en la medida en que la Legislación Europea de Protección de Datos se aplique al tratamiento de Datos Personales del Cliente, incluidos los siguientes casos:

(a) Si el tratamiento se realiza en el contexto de las actividades de un establecimiento del Cliente en el EEE o en Reino Unido.

(b) Si los Datos Personales del Cliente son datos personales relacionados con interesados que se encuentren en el EEE o en Reino Unido y el tratamiento está relacionado con la oferta de bienes o servicios a dichos interesados o con la supervisión de su comportamiento en el EEE o en Reino Unido.

4.2 **Aplicación de Servicios del Encargado del Tratamiento**. Los presentes Términos del Tratamiento de Datos solo serán aplicables a los Servicios del Encargado del Tratamiento para los que las partes hayan acordado estos Términos del Tratamiento de Datos. Por ejemplo, a) los Servicios del Encargado del Tratamiento para los cuales el Cliente haya hecho clic para aceptar estos Términos del Tratamiento de Datos o b) si el Contrato incorpora estos Términos del Tratamiento de Datos mediante referencia, los Servicios del Encargado del Tratamiento que son el objeto del Contrato.

4.3 **Incorporación de Términos Adicionales para Legislación No Europea de Protección de Datos**. Los Términos Adicionales para Legislación No Europea de Protección de Datos complementan los presentes Términos del Tratamiento de Datos.

5. Tratamiento de datos

5.1 **Roles y cumplimiento normativo; autorización**.

5.1.1 **Responsabilidades del Encargado del Tratamiento de Datos y del Responsable del Tratamiento de Datos**. Las partes reconocen y aceptan lo siguiente:

(a) El apéndice 1 describe la cuestión y los detalles del tratamiento de Datos Personales del Cliente.

(b) Google es un encargado del tratamiento de datos personales del Cliente en virtud de la Legislación Europea de Protección de Datos.

(c) El Cliente es un responsable del tratamiento de datos o un encargado del tratamiento, según corresponda, de los Datos Personales del Cliente en virtud de la Legislación Europea de Protección de Datos.

(d) Cada parte cumplirá las obligaciones que le correspondan en virtud de la Legislación Europea de Protección de Datos con respecto al tratamiento de Datos Personales del Cliente.

5.1.2 **Clientes Encargados del Tratamiento**. Si el Cliente es un encargado del tratamiento de datos:

(a) El Cliente garantiza de forma continua que el responsable del tratamiento de datos pertinente ha autorizado i) las Instrucciones, ii) la designación de Google por parte del Cliente como otro encargado del tratamiento y iii) la contratación por parte de Google de Subencargados del Tratamiento, tal y como se describe en la sección 11 (Subencargados del Tratamiento).

(b) El Cliente reenviará inmediatamente al responsable del tratamiento de datos pertinente cualquier aviso proporcionado por Google en virtud de las secciones 5.4 (Notificaciones de Instrucciones), 7.2.1 (Notificación de incidentes) u 11.4 (Oportunidad de oponerse a cambios del Subencargado del Tratamiento), o que haga referencia a cualquier SCC.

(c) El Cliente podrá poner a disposición del responsable del tratamiento de datos pertinente cualquier información que proporcione Google en virtud de las secciones 7.4 (Certificación de seguridad), 10.5 (Información de centros de datos) y 11.2 (Información sobre los Subencargados del Tratamiento).

5.2 **Instrucciones del Cliente**. Al suscribir los presentes Términos del Tratamiento de Datos, el Cliente indica a Google que trate los Datos Personales del Cliente únicamente de conformidad con la ley aplicable: a) para prestar los Servicios del Encargado del Tratamiento y cualquier asistencia técnica relacionada, b) tal y como se especifica más detalladamente a través del uso por parte del Cliente de los Servicios del Encargado del Tratamiento (incluidas la configuración y otras funciones de los Servicios del Encargado del Tratamiento) y cualquier asistencia técnica relacionada, c) según se documenta por medio del Contrato (incluidos estos Términos del Tratamiento de Datos) y d) tal y como se documenta más detalladamente en otras instrucciones proporcionadas por escrito por el Cliente y reconocidas por Google como instrucciones constitutivas para los propósitos de estos Términos del Tratamiento de Datos (en conjunto, las "**Instrucciones**").

5.3 **Cumplimiento de las Instrucciones por parte de Google**. Google cumplirá las Instrucciones a menos que lo prohíban las Leyes Europeas.

5.4 **Notificaciones de Instrucciones**. Google notificará inmediatamente al Cliente, a menos que dicha notificación esté prohibida por las Leyes Europeas, si, según la opinión de Google, a) las Leyes Europeas prohíben a Google cumplir una Instrucción, b) una Instrucción no cumple la Legislación Europea de Protección de Datos o c) Google no puede cumplir una Instrucción. Esta sección 5.4 (Notificaciones de Instrucciones) no reduce los derechos ni las obligaciones de ninguna de las partes que figuren en cualquier otra parte del Contrato.

5.5 **Productos Adicionales**. Si el Cliente usa cualquier Producto Adicional, los Servicios del Encargado del Tratamiento podrán permitir que dicho Producto Adicional acceda a los Datos Personales del Cliente según sea necesario para la interoperabilidad del Producto Adicional con los Servicios del Encargado del Tratamiento. Como aclaración, estos Términos del Tratamiento de Datos no se aplican al tratamiento de datos personales en relación con la provisión de ningún Producto Adicional usado por el Cliente, incluidos los datos personales transmitidos desde dicho Producto Adicional o hacia el mismo.

6. Eliminación de Datos

6.1 **Eliminación durante la Vigencia**.

6.1.1 **Servicios del Encargado del Tratamiento con funciones de eliminación**. Si, durante la Vigencia, se produce la siguiente situación:

(a) Las funciones de los Servicios del Encargado del Tratamiento incluyen la opción de que el Cliente elimine Datos Personales del Cliente,

(b) El cliente usa los Servicios del Encargado del Tratamiento para eliminar determinados Datos Personales del Cliente y

(c) El Cliente no puede recuperar Datos Personales del Cliente eliminados (por ejemplo, de la papelera),

Google eliminará de sus sistemas dichos Datos Personales del Cliente tan pronto como sea razonablemente posible y en un plazo máximo de 180 días, a menos que las Leyes Europeas exijan su almacenamiento.

6.1.2 **Servicios del Encargado del Tratamiento sin funciones de eliminación**. Durante la Vigencia, si las funciones de los Servicios del Encargado del Tratamiento no incluyen la opción de que el Cliente pueda eliminar Datos Personales del Cliente, Google cumplirá lo siguiente:

(a) Cualquier solicitud razonable del Cliente para facilitar dicha eliminación, en la medida en que eso sea posible teniendo en cuenta la naturaleza y la funcionalidad de los Servicios del Encargado del Tratamiento, a menos que las Leyes Europeas exijan su almacenamiento.

(b) Las prácticas de conservación de datos descritas en policies.google.com/technologies/ads.

Google puede cobrar una tarifa (basada en los costes razonables de Google) por cualquier eliminación de datos en virtud de la sección 6.1.2(a). Google proporcionará al Cliente más información sobre cualquier tarifa aplicable y le indicará la base de su cálculo antes de llevar a cabo cualquier eliminación de datos.

6.2 **Eliminación al vencimiento de la Vigencia**. El Cliente indica a Google que elimine todos los Datos Personales del Cliente restantes (incluidas las copias existentes) de los sistemas de Google cuando finalice la Vigencia según la ley aplicable. Google cumplirá esta instrucción tan pronto como sea razonablemente posible y dentro de un plazo máximo de 180 días, a menos que las Leyes Europeas exijan su almacenamiento.

7. Seguridad de los Datos

7.1 **Medidas de Seguridad y asistencia de Google**.

7.1.1 **Medidas de Seguridad de Google**. Google implementará y mantendrá medidas técnicas y organizativas para proteger los Datos Personales del Cliente frente a la destrucción accidental o ilícita, la pérdida, la alteración y la divulgación o el acceso no autorizados, tal y como se describe en el apéndice 2 (las "**Medidas de Seguridad**"). Tal y como se describe en el apéndice 2, las Medidas de Seguridad incluyen medidas a) para cifrar datos personales, b) para ayudar a asegurar la confidencialidad, la integridad, la disponibilidad y la resiliencia continuas de los sistemas y los servicios de Google, c) para ayudar a restaurar el acceso oportuno a los datos personales después de un incidente y d) para hacer pruebas periódicas de efectividad. Google podrá actualizar o modificar las Medidas de Seguridad ocasionalmente, siempre y cuando dichas actualizaciones y modificaciones no provoquen una degradación de la seguridad general de los Servicios del Encargado del Tratamiento.

7.1.2 **Acceso y cumplimiento**. Google a) autorizará a sus empleados, contratistas y Subencargados del Tratamiento a acceder a los Datos Personales del Cliente solo en la medida de lo estrictamente necesario para cumplir las Instrucciones, b) tomará las medidas adecuadas para asegurar el cumplimiento de las Medidas de Seguridad por parte de sus empleados, contratistas y Subencargados del Tratamiento en la medida en que sea aplicable a su ámbito de actuación y c) se asegurará de que todas las personas autorizadas para tratar los Datos Personales del Cliente se hayan comprometido a mantener la confidencialidad de estos datos o tengan una obligación legal pertinente de confidencialidad.

7.1.3 **Asistencia de Seguridad de Google**. Google (teniendo en cuenta la naturaleza del tratamiento de los Datos Personales del Cliente y la información que Google tenga a su disposición) ayudará al Cliente a asegurar el cumplimiento de las obligaciones del Cliente (o, si el Cliente es un encargado del tratamiento, del responsable pertinente del tratamiento de datos) con respecto a la seguridad de los datos personales y las brechas de seguridad de datos personales, incluidas las obligaciones del Cliente (o, si el Cliente es un encargado del tratamiento, del responsable pertinente del tratamiento de datos) en virtud de los artículos 32 al 34 (inclusive) del RGPD, haciendo lo siguiente:

(a) Implementar y mantener las Medidas de Seguridad de conformidad con la sección 7.1.1 (Medidas de Seguridad de Google).

(b) Cumplir los términos de la sección 7.2 (Incidentes de Datos).

(c) Proporcionar al Cliente la Documentación de Seguridad de conformidad con la sección 7.5.1 (Revisiones de la Documentación de Seguridad) y la información incluida en estos Términos del Tratamiento de Datos.

7.2 **Incidentes de Datos**.

7.2.1 **Notificación de incidentes**. Si Google tiene conocimiento de un Incidente de Datos, Google a) notificará al Cliente el Incidente de Datos a la mayor brevedad y sin retrasos indebidos, y b) tomará medidas razonables lo antes posible para minimizar los daños y proteger los Datos Personales del Cliente.

7.2.2 **Detalles de un Incidente de Datos**. Las notificaciones que se realicen en virtud de la sección 7.2.1 (Notificación de incidentes) deberán describir la naturaleza del Incidente de Datos (incluidos los recursos del Cliente que se hayan visto afectados), las medidas que Google haya tomado (o que planee tomar) para abordar el Incidente de Datos y mitigar sus riesgos potenciales, las medidas (si las hubiera) que Google recomiende al Cliente para abordar el Incidente de Datos y los datos de un punto de contacto en el que se pueda consultar más información. Si no es posible proporcionar toda esta información al mismo tiempo, la notificación inicial de Google incluirá la información disponible en ese momento y proporcionará más detalles sin retrasos indebidos en el momento en el que estén disponibles.

7.2.3 **Entrega de la notificación**. Google entregará su notificación de cualquier Incidente de Datos mediante la Dirección de Correo Electrónico de Notificaciones o, a discreción de Google (incluido el caso de que el Cliente no haya proporcionado ninguna Dirección de Correo Electrónico de Notificaciones), a través de otro medio de comunicación directa (por ejemplo, por teléfono o en una reunión presencial). El Cliente es el único responsable de proporcionar la Dirección de Correo Electrónico de Notificaciones y de asegurarse de que esté actualizada y sea válida.

7.2.4 **Notificaciones de terceros**. El Cliente es el único responsable de cumplir las leyes de notificación de incidentes aplicables al Cliente y de satisfacer cualquier obligación de notificación a terceros relacionada con cualquier Incidente de Datos.

7.2.5 **Ausencia de reconocimiento de culpa por parte de Google**. La notificación por parte de Google de un Incidente de Datos o la respuesta de Google a un Incidente de Datos en virtud de esta sección 7.2 (Incidentes de Datos) no deberá interpretarse como un reconocimiento por parte de Google de ninguna culpa ni responsabilidad con respecto al Incidente de Datos.

7.3 **Responsabilidades y evaluación de seguridad del Cliente**.

7.3.1 **Responsabilidades de seguridad del Cliente**. El Cliente acepta que, sin perjuicio de las obligaciones de Google en virtud de las secciones 7.1 (Medidas de Seguridad y asistencia de Google) y 7.2 (Incidentes de Datos):

(a) El Cliente es responsable del uso que haga de los Servicios del Encargado del Tratamiento, incluido lo siguiente:

(i) Hacer un uso adecuado de los Servicios del Encargado del Tratamiento para asegurar un nivel de seguridad adecuado al riesgo con respecto a los Datos Personales del Cliente.

(ii) Proteger las credenciales de autenticación de la cuenta, los sistemas y los dispositivos que use el Cliente para acceder a los Servicios del Encargado del Tratamiento.

(b) Google no tiene ninguna obligación de proteger los Datos Personales del Cliente que el Cliente decida almacenar o transferir fuera de los sistemas de Google y de los de sus Subencargados del Tratamiento.

7.3.2 **Evaluación de seguridad del Cliente**. El Cliente reconoce y acepta que las Medidas de Seguridad implementadas y mantenidas por Google según lo estipulado en la sección 7.1.1 (Medidas de Seguridad de Google) proporcionan un nivel de seguridad adecuado al riesgo con respecto a los Datos Personales del Cliente, teniendo en cuenta los últimos avances técnicos, los costes de implementación y la naturaleza, el alcance, el contexto y las finalidades del tratamiento de los Datos Personales del Cliente, así como los riesgos para las personas.

7.4 **Certificación de seguridad**. Para evaluar y ayudar a asegurar la eficacia continua de las Medidas de Seguridad, Google mantendrá la certificación ISO 27001.

7.5 **Revisiones y auditorías de cumplimiento**.

7.5.1 **Revisiones de la Documentación de Seguridad**. Para demostrar el cumplimiento por parte de Google de sus obligaciones en virtud de estos Términos del Tratamiento de Datos, Google pondrá a disposición del Cliente la Documentación de Seguridad para que la revise.

7.5.2 **Derechos de auditoría del Cliente**.

(a) Google permitirá al Cliente o a un auditor externo designado por el Cliente llevar a cabo auditorías (incluidas inspecciones) para verificar el cumplimiento de las obligaciones contraídas por Google en virtud de estos Términos del Tratamiento de Datos de conformidad con la sección 7.5.3 (Términos comerciales adicionales para auditorías). Durante una auditoría, Google pondrá a disposición toda la información necesaria para demostrar dicho cumplimiento y contribuir a las auditorías tal y como se describe en la sección 7.4 (Certificación de seguridad) y en esta sección 7.5 (Revisiones y auditorías de cumplimiento).

(b) Si se aplican las SCCs en virtud de la sección 10.2 (Transferencias Europeas Restringidas), Google permitirá que el Cliente (o un auditor externo designado por el Cliente) realice auditorías tal y como se describe en las SCCs y, durante la auditoría, pondrá a disposición toda la información requerida por las SCCs de conformidad con la sección 7.5.3 (Términos comerciales adicionales para auditorías).

(c) El Cliente también podrá realizar una auditoría para verificar que Google cumpla sus obligaciones en virtud de estos Términos del Tratamiento de Datos mediante la revisión del certificado emitido para la certificación ISO 27001 (que refleja el resultado de una auditoría realizada por un auditor externo).

7.5.3 **Términos comerciales adicionales para auditorías**.

(a) El Cliente enviará cualquier solicitud de auditoría conforme a la sección 7.5.2(a) o 7.5.2(b) a Google tal y como se describe en la sección 12.1 (Ponerse en contacto con Google).

(b) Después de que Google haya recibido una solicitud conforme a la sección 7.5.3(a), Google y el Cliente discutirán y acordarán por adelantado la fecha de inicio razonable, el alcance y la duración de la auditoría, así como los controles de seguridad y confidencialidad aplicables a la misma en virtud de la sección 7.5.2(a) o 7.5.2(b).

(c) Google puede cobrar una tarifa (basada en los costes razonables de Google) por cualquier auditoría en virtud de la sección 7.5.2(a) o 7.5.2(b). Google proporcionará al Cliente más información sobre cualquier tarifa aplicable y le indicará la base de su cálculo antes de llevar a cabo cualquier auditoría. El Cliente será responsable de todas las tarifas cobradas por cualquier auditor externo designado por el Cliente para realizar dicha auditoría.

(d) Google podrá oponerse a que cualquier auditor externo designado por el Cliente realice cualquier auditoría en virtud de la sección 7.5.2(a) o

7.5.2(b) si, en la opinión razonable de Google, el auditor no tiene la cualificación adecuada, no es independiente, es competidor de Google o es manifiestamente inadecuado. Cualquiera de dichas objeciones por parte de Google hará necesario que el Cliente designe a otro auditor o que realice la auditoría el propio Cliente.

(e) Nada de lo previsto en estos Términos del Tratamiento de los Datos requerirá que Google revele o permita al Cliente o a su auditor externo acceder a:

(i) Cualquier dato de cualquier otro cliente de una Entidad de Google.

(ii) La información contable o financiera interna de cualquier Entidad de Google.

(iii) Cualquier secreto comercial de una Entidad de Google.

(iv) Cualquier información que, en la opinión razonable de Google, pueda A) poner en riesgo la seguridad de cualquier sistema o instalación de una Entidad de Google o B) provocar que cualquier Entidad de Google incumpla sus obligaciones conforme a la Legislación Europea de Protección de Datos o sus obligaciones de seguridad y/o privacidad para con el Cliente o cualquier tercero.

(v) Cualquier información a la que quiera acceder el Cliente o su auditor externo por cualquier motivo que no sea el cumplimiento de buena fe de las obligaciones del Cliente conforme a la Legislación Europea de Protección de Datos.

8. Evaluaciones de impacto y consultas

Google (teniendo en cuenta la naturaleza del tratamiento y la información disponible para Google) ayudará al Cliente a asegurar el cumplimiento de las obligaciones del Cliente (o, si el Cliente es un encargado del tratamiento, de las obligaciones del responsable pertinente del tratamiento de datos) con respecto a las evaluaciones de impacto y consultas previas, incluidas (si corresponde) las obligaciones del Cliente o del responsable pertinente del tratamiento de datos en virtud de los artículos 35 y 36 del RGPD,:

(a) Proporcionando la Documentación de Seguridad de conformidad con la sección 7.5.1 (Revisiones de la Documentación de Seguridad).

(b) Proporcionando la información incluida en el Contrato (incluidos estos Términos del Tratamiento de Datos).

(c) Proporcionando o poniendo a disposición, de acuerdo con las prácticas estándar de Google, otros materiales relacionados con la naturaleza de los Servicios del Encargado del Tratamiento y el tratamiento de los Datos Personales del Cliente (por ejemplo, materiales del centro de ayuda).

9. Derechos de los interesados

9.1 **Respuestas a solicitudes de los interesados**. Si Google recibe una solicitud de un interesado en relación con los Datos Personales del Cliente, el Cliente autoriza a Google a hacer lo siguiente (y Google, por la presente, notifica al Cliente que lo hará):

(a) Responder directamente a la solicitud del interesado de acuerdo con la funcionalidad estándar de la Herramienta del Interesado (si la solicitud se realiza a

través de una Herramienta del Interesado).

(b) Informar al interesado para que envíe su solicitud al Cliente y el Cliente será responsable de responder a dicha solicitud (si la solicitud no se realiza a través de una Herramienta del Interesado).

9.2 **Asistencia de Google en relación con la solicitud del interesado**. Google ayudará al Cliente a cumplir sus obligaciones (o, si el Cliente es un encargado del tratamiento, las del responsable pertinente del tratamiento de datos) contraídas en virtud del capítulo III del RGPD para responder a solicitudes de ejercicio de los derechos del interesado, teniendo en cuenta en todos los casos la naturaleza del tratamiento de los Datos Personales del Cliente y, si corresponde, el artículo 11 del RGPD,:

(a) Proporcionando la funcionalidad de los Servicios del Encargado del Tratamiento.

(b) Cumpliendo los compromisos establecidos en la Sección 9.1 (Respuestas a solicitudes de los interesados).

(c) Si se aplica a los Servicios del Encargado del Tratamiento, poniendo a disposición Herramientas del Interesado.

9.3 **Rectificación**. Si el Cliente detecta que cualquier Dato Personal del Cliente es impreciso o está obsoleto, el Cliente será responsable de rectificar o eliminar ese dato si así lo exige la Legislación Europea de Protección de Datos, incluso (si estuviesen disponibles) mediante las funciones de los Servicios del Encargado del Tratamiento.

10. Transferencias de datos

10.1 **Almacenamiento de datos e instalaciones de tratamiento**. De conformidad con esta sección 10 (Transferencias de datos), Google podrá tratar Datos Personales del Cliente en cualquier país en el que Google o cualquiera de sus Subencargados del Tratamiento tenga instalaciones.

10.2 **Transferencias Europeas Restringidas**. Las partes reconocen que la Legislación Europea de Protección de Datos no exige SCCs ni una Solución Alternativa de Transferencia para tratar Datos Personales del Cliente en un País Adecuado ni para transferirlos a este. Si los Datos Personales del Cliente son transferidos a cualquier otro país y a esas transferencias se les aplica la Legislación Europea de Protección de Datos ("**Transferencias Europeas Restringidas**"), en ese caso:

(a) Si Google adopta una Solución Alternativa de Transferencia para cualquier Transferencia Europea Restringida, Google informará al Cliente de la solución relevante y se asegurará de que dichas Transferencias Europeas Restringidas se realicen de acuerdo con dicha Solución y/o

(b) Si Google no ha adoptado o ha informado al Cliente de que ya no va a adoptar ninguna Solución Alternativa de Transferencia para ninguna Transferencia Europea Restringida, en ese caso:

(i) Si la dirección de Google se encuentra en un País Adecuado:

(A) Se aplicarán las SCCs del Encargado del Tratamiento al Encargado del Tratamiento, Exportador de Google) con respecto a todas las Transferencias Europeas Restringidas de Google a los Subencargados del Tratamiento y.

(B) Además, si la dirección del Cliente no se encuentra en un País Adecuado, se aplicarán las SCCs (Encargado del Tratamiento al Responsable del Tratamiento de Datos) con respecto a las Transferencias Europeas Restringidas entre Google y el Cliente, independientemente de si el

Cliente es un responsable y/o un encargado del tratamiento o

(ii) Si la dirección de Google no se encuentra en un País Adecuado, Se aplicarán las SCCs del Responsable del Tratamiento de Datos al Encargado del Tratamiento y/o las SCCs (Encargado del Tratamiento al Encargado del Tratamiento), en función de si el Cliente es un responsable del tratamiento de datos y/o un encargado del tratamiento, con respecto a las Transferencias Europeas Restringidas entre el Cliente y Google.

10.3 **Medidas complementarias e información**. Google proporcionará al Cliente la información pertinente sobre las Transferencias Europeas Restringidas, incluida la información sobre medidas complementarias para proteger los Datos Personales del Cliente, tal y como se describe en la sección 7.5.1 (Revisiones de la Documentación de Seguridad), en el apéndice 2 (Medidas de Seguridad) y en otros materiales relacionados con la naturaleza de los Servicios del Encargado del Tratamiento y con el tratamiento de los Datos Personales del Cliente (por ejemplo, artículos del centro de ayuda).

10.4 **Resolución**. Si el Cliente concluye, según el uso que hace o pretende hacer de los Servicios del Encargado del Tratamiento, que la Solución Alternativa de Transferencia y/o las SCCs, según corresponda, no proporcionan la protección adecuada para los Datos Personales del Cliente, el Cliente podrá resolver inmediatamente el Contrato por conveniencia mediante una notificación por escrito a Google.

10.5 **Información de centros de datos**. La información sobre las ubicaciones de los centros de datos de Google está disponible en www.google.com/about/datacenters/locations/.

11. Subencargados del Tratamiento

11.1 **Consentimiento de contratación de un Subencargado del Tratamiento**. El Cliente autoriza específicamente la contratación como Subencargados del Tratamiento de las entidades que figuren, a partir de la Fecha de Entrada en Vigor de los Términos, en la URL especificada en la sección 11.2 (Información sobre los Subencargados del Tratamiento). Asimismo, y sin perjuicio de lo estipulado en la sección 11.4 (Oportunidad de oponerse a cambios del Subencargado del Tratamiento), el Cliente autoriza de forma general la contratación de cualquier otro tercero como Subencargado del Tratamiento ("**Nuevos Subencargados del Tratamiento**").

11.2 **Información sobre los Subencargados del Tratamiento**. La información sobre los Subencargados del Tratamiento está disponible en business.safety.google/adssubprocessors.

11.3 **Requisitos para la contratación de Subencargados del Tratamiento**. Al contratar a cualquier Subencargado del Tratamiento, Google:

(a) Se asegurará, por medio de un contrato escrito, de que:

(i) El Subencargado del Tratamiento solo use y acceda a los Datos Personales del Cliente en la medida en que los necesite para cumplir las obligaciones para las que se le ha subcontratado y lo haga de conformidad con el Contrato (incluidos estos Términos del Tratamiento de Datos).

(ii) Si el tratamiento de los Datos Personales del Cliente está sujeto a la Legislación Europea de Protección de Datos, se impongan las obligaciones de protección de datos de estos Términos del Tratamiento de Datos (tal y como se hace referencia a ellos en el artículo 28(3) del RGPD, si corresponde) al Subencargado del Tratamiento.

(b) Seguirá siendo plenamente responsable de todas las obligaciones para las que se ha subcontratado al Subencargado del Tratamiento y de todas las

acciones y omisiones de este.

11.4 **Oportunidad de oponerse a cambios del Subencargado del Tratamiento**.

(a) Cuando se contrate a un Nuevo Subencargado del Tratamiento durante la Vigencia, Google informará de la contratación (incluidos el nombre y la ubicación del subencargado del tratamiento, así como las actividades que realizará) al Cliente, al menos 30 días antes de que el Subencargado del Tratamiento trate cualquier Dato Personal del Cliente, mediante el envío de un correo a la Dirección de Correo Electrónico de Notificaciones.

(b) El Cliente podrá oponerse a cualquier Nuevo Subencargado del Tratamiento resolviendo el Contrato por conveniencia inmediatamente mediante aviso por escrito a Google, con la condición de que el Cliente proporcione dicho aviso en un plazo de 90 días desde el momento en el que se le haya informado de la contratación del Nuevo Subencargado del Tratamiento tal y como se describe en la sección 11.4(a).

12. Ponerse en contacto con Google y registros de tratamiento

12.1 **Ponerse en contacto con Google**. El Cliente podrá ponerse en contacto con Google en relación con el ejercicio de sus derechos en virtud de estos Términos del Tratamiento de Datos mediante los métodos descritos en privacy.google.com/businesses/processorsupport o a través de otros medios que pueda proporcionar Google ocasionalmente. Google proporcionará asistencia rápida y razonable en relación con las consultas del Cliente que Google reciba mediante dichos medios y que estén relacionadas con el tratamiento de los Datos Personales del Cliente en virtud del Contrato.

12.2 **Registros de tratamiento de Google**. Google mantendrá la documentación adecuada de sus actividades de tratamiento tal y como lo exige el RGPD. El Cliente reconoce que, de conformidad con el RGPD, Google tiene la obligación de a) recopilar y mantener registros de determinada información, incluidos i) el nombre y la información de contacto de cada encargado del tratamiento y/o responsable del tratamiento de datos en cuyo nombre actúa Google y (si corresponde) del representante local y del delegado de protección de datos de dicho encargado del tratamiento y/o responsable del tratamiento de datos, y ii) si corresponde en virtud de las SCCs del Cliente, la Autoridad de Control del Cliente, y b) poner dicha información a disposición de cualquier Autoridad de Control. En consecuencia, el Cliente proporcionará, cuando se le exija y según le corresponda, dicha información a Google a través de la interfaz de usuario de los Servicios del Encargado del Tratamiento o mediante otros medios que pueda proporcionar Google y usará dicha interfaz de usuario u otro medio para asegurarse de que toda la información sea precisa y esté actualizada.

12.3 **Solicitudes del Responsable del Tratamiento de Datos**. Si Google recibe una solicitud o una instrucción mediante los métodos descritos en la sección 12.1 (o cualquier otro método) de un tercero que afirme ser un responsable del tratamiento de los Datos Personales del Cliente, Google recomendará a dicho tercero que se ponga en contacto con el Cliente.

13. Responsabilidad

Si el Contrato se rige por las leyes de:

(a) Un estado de Estados Unidos de América: en ese caso, independientemente de cualquier otro contenido del Contrato, la responsabilidad absoluta de cualquiera de las partes para con la otra parte en virtud de estos Términos del Tratamiento de Datos o en relación con ellos estará limitada al máximo importe monetario o de

pago establecido como tope de la responsabilidad de esa parte en virtud del Contrato (y, por consiguiente, cualquier exclusión de demandas de indemnización de la limitación de responsabilidad del Contrato no será aplicable a demandas de indemnización en virtud del Contrato en relación con la Legislación Europea de Protección de Datos o la Legislación No Europea de Protección de Datos).

(b) Una jurisdicción que no sea un estado de Estados Unidos de América: en ese caso, la responsabilidad de las partes en virtud de los presentes Términos del Tratamiento de Datos, o en conexión con estos, estará sujeta a las exclusiones y limitaciones de responsabilidad que figuran en el Contrato.

14. Efectos de estos Términos del Tratamiento de Datos

14.1 **Orden de prioridad**. Si hay algún conflicto o discrepancia entre las SCCs del Cliente, los Términos Adicionales para Legislación No Europea de Protección de Datos, el resto de estos Términos del Tratamiento de Datos y/o el resto del Contrato, se aplicará el siguiente orden de prioridad:

(a) Las SCCs del Cliente (si corresponde).

(b) Los Términos Adicionales para Legislación No Europea de Protección de Datos (si corresponde).

(c) El resto de estos Términos del Tratamiento de Datos.

(d) El resto del Contrato.

Con sujeción a lo dispuesto en las enmiendas realizadas sobre estos Términos del Tratamiento de Datos, el Contrato seguirá siendo plenamente válido y eficaz.

14.2 **No modificación de las SCCs**. Ninguna de las disposiciones del Contrato (incluidos estos Términos del Tratamiento de Datos) tiene como finalidad modificar o contradecir ninguna SCC ni atentar contra los derechos fundamentales o las libertades de los interesados en virtud de la Legislación Europea de Protección de Datos.

14.3 Ausencia de efecto sobre los **Términos Aplicables a los Responsables del Tratamiento de Datos**. Estos Términos del Tratamiento de Datos no afectarán a ningún término independiente entre Google y el Cliente que refleje una relación entre responsables del tratamiento de datos para prestar un servicio diferente a los Servicios del Encargado del Tratamiento.

14.4 Las **Cláusulas Contractuales Tipo heredadas de Reino Unido**. A partir del 21 de Septiembre de 2022 o la fecha de entrada en vigor, lo que ocurra más tarde, se aplicarán las cláusulas complementarias de las SCCs para las transferencias del RGPD de Reino Unido y sustituirán y dejarán sin efecto cualquier cláusula contractual estándar aprobada en virtud del RGPD de Reino Unido y de la Ley de Protección de Datos de 2018 y suscrita previamente por el Cliente y Google (“SCC heredadas de Reino Unido”). Esta Sección 14.4 (SCC heredadas de Reino Unido) no afectará a los derechos de ninguna de las partes, ni a los derechos de ningún interesado, que pueda haber adquirido en virtud de las SCC heredadas de Reino Unido mientras se encontraban en vigor.

15. Cambios en estos Términos del Tratamiento de Datos

15.1 **Cambios en las URLs**. Ocasionalmente, Google puede cambiar cualquier URL a la que se haga referencia en estos Términos del Tratamiento de Datos y el contenido

de cualquiera de dichas URLs, con la salvedad de que Google solo podrá cambiar:

(a) Las SCCs de acuerdo con las secciones de la 15.2(b) a la 15.2(d) (Cambios en los Términos del Tratamiento de Datos) o para incorporar cualquier versión nueva de las SCCs que se haya podido adoptar en virtud de la Legislación Europea de Protección de Datos. En todos los casos, los cambios se deberán realizar de manera que no afecten a la validez de las SCCs de conformidad con la Legislación Europea de Protección de Datos.

(b) La lista de potenciales Servicios del Encargado del Tratamiento incluida en business.safety.google/adsservices: i) para reflejar un cambio en el nombre de un servicio, ii) para añadir un nuevo servicio o iii) para retirar un servicio (o una característica de un servicio) en caso de que x) todos los contratos sobre la prestación de dicho servicio se hayan resuelto; y) Google tenga el consentimiento del Cliente; o (z) el servicio, o una determinada característica del mismo haya sido recategorizado como servicio del responsable.

15.2 **Cambios en los Términos del Tratamiento de Datos**. Google podrá cambiar estos Términos del Tratamiento de Datos en los siguientes casos:

(a) Si el cambio está expresamente permitido por estos Términos del Tratamiento de Datos, incluido lo descrito en la sección 15.1 (Cambios en las URLs).

(b) Si el cambio refleja un cambio en el nombre o la forma de una entidad legal.

(c) Si el cambio es necesario para cumplir la legislación y la normativa aplicables, una orden judicial o una directriz publicada por un ente regulador o una agencia gubernamentales, o refleja la adopción por parte de Google de una Solución Alternativa de Transferencia.

(d) Si el cambio i) no provoca una degradación de la seguridad general de los Servicios del Encargado del Tratamiento, ii) no amplía el alcance de, ni elimina ninguna restricción sobre x) en el caso de los Términos Adicionales para Legislación No Europea de Protección de Datos, los derechos de Google para usar o tratar los datos en el ámbito de los Términos Adicionales para Legislación No Europea de Protección de Datos o, y) en el caso del resto de estos Términos del Tratamiento de Datos, el tratamiento que hace Google de los Datos Personales del Cliente, tal y como se describe en la sección 5.3 (Cumplimiento de las Instrucciones por parte de Google) y iii) no tiene un impacto material adverso en los derechos del Cliente en virtud de estos Términos del Tratamiento de Datos, según determine Google razonablemente.

15.3 **Notificación de los cambios**. Si Google tiene la intención de cambiar estos Términos del Tratamiento de Datos en virtud de la sección 15.2(c) o (d), informará al Cliente al menos 30 días (o el periodo más corto que se requiera para cumplir la legislación y la normativa aplicables, una orden judicial o una directriz publicada por un ente regulador o agencia gubernamentales) antes de que el cambio entre en vigor a) enviando un correo a la Dirección de Correo Electrónico de Notificaciones o b) alertando al Cliente a través de la interfaz de usuario de los Servicios del Encargado del Tratamiento. Si el Cliente se opone a alguno de esos cambios, podrá resolver inmediatamente el Contrato por conveniencia mediante un aviso por escrito a Google en un plazo de 90 días desde el momento en que Google le haya informado del cambio.

Apéndice 1: Objeto y detalles del tratamiento de datos

Objeto

La prestación por parte de Google de los Servicios del Encargado del Tratamiento y de cualquier soporte técnico relacionado al Cliente.

Duración del tratamiento

La Vigencia más el periodo desde el final de esta hasta la eliminación de todos los Datos Personales del Cliente por parte de Google de acuerdo con estos Términos del Tratamiento de Datos.

Naturaleza y finalidad del tratamiento

Google tratará (incluso, según corresponda a los Servicios del Encargado del Tratamiento y las Instrucciones, recogiendo, registrando, organizando, estructurando, almacenando, alterando, recuperando, utilizando, divulgando, combinando, borrando y destruyendo) los Datos Personales del Cliente con la finalidad de proporcionar los Servicios del Encargado del Tratamiento y cualquier soporte técnico relacionado al Cliente de acuerdo con los presentes Términos del Tratamiento de Datos.

Tipos de Datos Personales

Los Datos Personales del Cliente pueden incluir los tipos de datos personales descritos en business.safety.google/adsservices.

Categorías de Interesados

Los Datos Personales del Cliente afectarán a las siguientes categorías de interesados:

- Interesados sobre los que Google recopila datos personales al prestar sus Servicios del Encargado del Tratamiento.
- Interesados cuyos datos personales se transfieren a Google en relación con los Servicios del Encargado del Tratamiento por parte del Cliente, siguiendo las indicaciones del Cliente o en su nombre.

En función de la naturaleza de los Servicios del Encargado del Tratamiento, estos interesados pueden incluir individuos a) a quienes haya ido o vaya dirigida en un futuro la publicidad online, b) que hayan visitado sitios web o aplicaciones específicos con respecto a los cuales Google proporcione los Servicios del Encargado del Tratamiento y/o c) que sean clientes o usuarios de los productos o servicios del Cliente.

Apéndice 2: Medidas de Seguridad

A partir de la Fecha de Entrada en Vigor de los Términos, Google implementará y mantendrá las Medidas de Seguridad establecidas en el presente apéndice 2. Google podrá actualizar o modificar dichas Medidas de Seguridad ocasionalmente, siempre y cuando dichas actualizaciones y modificaciones no provoquen una degradación de la seguridad general de los Servicios del Encargado del Tratamiento.

1. **Centro de datos y seguridad de red**

   (a) **Centros de datos**.

   Infraestructura. Google mantiene centros de datos distribuidos geográficamente. Google almacena todos los datos de producción en centros de datos físicamente seguros.

   Redundancia. Los sistemas de infraestructura se han diseñado para eliminar los puntos únicos de fallo y minimizar el impacto de los riesgos ambientales previstos. Circuitos duales, conmutadores, redes u otros dispositivos necesarios ayudan a proporcionar esta redundancia. Los Servicios del Encargado del Tratamiento están diseñados para permitir a Google realizar ciertos tipos de mantenimiento preventivo y correctivo sin interrupciones. Todo el equipo y las instalaciones de

protección del medio ambiente han documentado los procedimientos de mantenimiento preventivo que detallan el proceso y la frecuencia de ejecución de acuerdo con las especificaciones del fabricante o las especificaciones internas. El mantenimiento preventivo y correctivo de los equipos del centro de datos se programa a través de un proceso estándar de acuerdo con procedimientos documentados.

Suministro eléctrico. Los sistemas de suministro eléctrico del centro de datos están diseñados para ser redundantes y poder mantenerse sin tener un gran impacto en el mantenimiento continuo de las operaciones, las 24 horas al día, los 7 días de la semana. En la mayoría de los casos, se proporciona una fuente de suministro eléctrico primaria, así como una fuente alternativa, cada una de ellas de igual capacidad, para los componentes críticos de la infraestructura del centro de datos. El suministro eléctrico de reserva se proporciona mediante diversos mecanismos, como, por ejemplo, baterías de sistemas de alimentación ininterrumpida (SAI), que proporcionan una protección del suministro eléctrico fiable y constante en caso de apagones parciales de las compañías eléctricas, apagones, sobretensión, baja tensión, y condiciones de frecuencia fuera de límites. Si se interrumpe el suministro eléctrico de la compañía eléctrica, el suministro eléctrico de reserva está diseñado para proporcionar energía transitoria al centro de datos, a plena capacidad, durante un máximo de 10 minutos hasta que el sistema de generadores de refuerzo tome el relevo. Los generadores de refuerzo son capaces de iniciarse automáticamente en cuestión de segundos para proporcionar suficiente suministro eléctrico de emergencia para que el centro de datos funcione a plena capacidad habitualmente durante varios días.

Sistemas operativos para servidores. Los servidores de Google usan sistemas operativos reforzados que se personalizan para las necesidades de servidor exclusivas de la empresa. Los datos se almacenan utilizando algoritmos patentados para aumentar la seguridad de los datos y la redundancia. Google emplea un proceso de revisión de código para aumentar la seguridad del código utilizado para prestar los Servicios del Encargado del Tratamiento y mejorar los productos de seguridad en entornos de producción.

Continuidad de la actividad. Google duplica datos a través de múltiples sistemas para ayudar a prevenir su destrucción o pérdida accidentales. Google ha diseñado y regularmente programa y pone a prueba sus programas de continuidad de la actividad/recuperación de desastres.

Tecnologías de cifrado. Las políticas de seguridad de Google exigen cifrado en reposo de todos los datos de usuarios, incluidos los datos personales. Los datos se suelen cifrar a varios niveles en pilas de almacenamiento de producción de los centros de datos de Google, incluido a nivel de hardware, y no requiere ninguna acción por parte de los clientes. Usar múltiples capas de cifradoañade protección de datos redundante y permite a Google seleccionar el enfoque óptimo en función de los requisitos de la aplicación. Todos los datos personales se cifran a nivel de almacenamiento, por lo general con el cifrado AES256. Google usa bibliotecas criptográficas comunes que incorporan el módulo validado FIPS 140-2 de Google para implementar el cifrado de manera uniforme en los Servicios del Encargado del Tratamiento.

(b) **Redes y transmisión**.

Transmisión de datos. Los centros de datos suelen estar conectados a través de enlaces privados de alta velocidad para proporcionar una transferencia de datos segura y rápida entre los centros de datos. Además, Google cifra los datos que se transmiten entre centros de datos. Esto se ha diseñado para evitar que los datos puedan ser leídos, copiados, alterados o eliminados sin autorización durante el transporte electrónico. Google transfiere datos a través de protocolos estándar de Internet.

Superficie de ataque externa. Google emplea múltiples capas de dispositivos de red y detección de intrusiones para proteger su superficie de ataque externa. Google considera posibles vectores de ataque e incorpora tecnologías apropiadas diseñadas especialmente en los sistemas orientados al exterior.

Detección de intrusiones. La detección de intrusiones tiene la finalidad de proporcionar información valiosa sobre las actividades de ataque en curso y ofrecer información adecuada para responder a los incidentes. La detección de intrusiones de Google implica lo siguiente:

1. El control firme del tamaño y la composición de la superficie de ataque de Google a través de medidas preventivas.

2. El empleo de controles de detección inteligentes en los puntos de entrada de datos.

3. El empleo de tecnologías que ponen remedio de forma automática a ciertas situaciones peligrosas.

Respuesta a incidentes. Google monitoriza diversos canales de comunicación para detectar incidentes de seguridad. El personal de seguridad de Google reaccionará rápidamente ante los incidentes conocidos.

Tecnologías de cifrado. Google utiliza el cifrado HTTPS (también conocido como conexión TLS) disponible. Los servidores de Google admiten el intercambio de claves criptográficas de Diffie Hellman de curva elíptica efímera firmado con RSA y ECDSA. Estos métodos de confidencialidad directa perfecta (perfect forward secrecy, PFS) ayudan a proteger el tráfico y minimizan el impacto de una clave vulnerada o una penetración criptográfica.

2. Acceso y controles en las instalaciones

(a) **Controles en las instalaciones**.

Operativo de seguridad en las instalaciones del centro de datos. Los centros de datos de Google mantienen un operativo de seguridad en las instalaciones responsable de todas las funciones de seguridad física del centro de datos las 24 horas del día, 7 días a la semana. El personal de operaciones de seguridad en las instalaciones controla las cámaras de circuito cerrado de televisión ("CCTV") y todos los sistemas de alarma. El personal del operativo de seguridad en las instalaciones realiza patrullas internas y externas del centro de datos con regularidad.

Procedimientos de acceso al centro de datos. Google mantiene procedimientos formales de acceso para permitir el acceso físico a los centros de datos. Los centros de datos están ubicados en instalaciones que requieren acceso con llave de tarjeta electrónica, con alarmas que están vinculadas al operativo de seguridad de las instalaciones. Todas las personas que accedan al centro de datos deben identificarse, así como mostrar un documento acreditativo al operativo de seguridad en las instalaciones. Solo se permite la entrada a los centros de datos a los empleados, contratistas y visitantes autorizados. Solo se les permite a los empleados y contratistas autorizados solicitar la tarjeta electrónica de llave de acceso a estas instalaciones. Las solicitudes de tarjeta electrónica de llave de acceso deben hacerse de antemano y por escrito, y requieren la aprobación del personal autorizado del centro de datos. Todas las demás personas que accedan temporalmente al centro de datos deben i) obtener la aprobación previa del personal autorizado del centro de datos para el centro de datos y las áreas internas específicos que deseen visitar, ii) firmar a requerimiento del operativo de seguridad en las instalaciones y iii) hacer referencia a un registro de accesos del centro de datos que identifique que el individuo cuenta con la debida aprobación.

Dispositivos de seguridad en las instalaciones del centro de datos. Los centros de datos de Google utilizan una llave de tarjeta electrónica y un sistema de control de acceso biométrico que están vinculados a un sistema de alarma. El sistema de control de acceso controla y registra la llave de tarjeta electrónica de cada individuo y cuándo acceden a las puertas del perímetro, la zona de envío y recepción, y otras áreas críticas. La actividad y los intentos de acceso no autorizados y fallidos se registran en el sistema de control de acceso y se investigan, según corresponda. El acceso autorizado a la zona de actividad comercial y los centros de datos se restringe por zonas y en función de las responsabilidades del puesto de trabajo de la persona en cuestión. Las puertas contra incendios de los centros de datos están dotadas de alarmas. Hay cámaras de CCTV en funcionamiento tanto dentro como fuera de los centros de datos. La ubicación de las cámaras ha sido diseñada para cubrir las áreas estratégicas que incluyen, entre otras, el perímetro, las puertas del edificio del centro de datos y la zona de envío/recepción. El personal del operativo de seguridad de las instalaciones se encarga del seguimiento, el registro y el control de los equipos de CCTV. Los equipos de CCTV están conectados con cables de seguridad por todos los centros de datos. Las cámaras graban en las instalaciones con grabadoras de vídeo digital las 24 horas del día, 7 días a la semana. Las grabaciones de vigilancia se conservan durante al menos 7 días en función de la actividad.

(b) **Control de accesos**.

Personal de seguridad de la infraestructura. Google tiene y mantiene una política de seguridad para su personal que requiere su capacitación en materia de seguridad como parte del paquete de capacitación de su personal. El personal de seguridad de la infraestructura de Google es responsable del control continuo de la infraestructura de seguridad de Google, de la revisión de los Servicios del Encargado del Tratamiento y de responder a los incidentes de seguridad.

Control de acceso y gestión de privilegios. Los administradores del Cliente y los usuarios deben autenticar su identidad a través de un sistema de autenticación central o por medio de un inicio de sesión único en el sistema para usar los Servicios del Encargado del Tratamiento.

Procesos y políticas de acceso a datos internos: política de acceso. Los procesos y las políticas de acceso a datos internos de Google están diseñados para evitar que personas y/o sistemas no autorizados tengan acceso a los sistemas utilizados para tratar datos personales. Google tiene como objetivo diseñar sus sistemas para i) que solo permitan a las personas autorizadas acceder a los datos a los que estén autorizados a acceder y ii) asegurarse de que los datos personales no puedan ser leídos, copiados, modificados ni retirados sin autorización durante su tratamiento y uso, ni después de su grabación. Los sistemas están diseñados para detectar cualquier acceso indebido. Google emplea un sistema de gestión de acceso centralizado para controlar el acceso del personal a los servidores de producción y solo permite el acceso a un número limitado de personal autorizado. LDAP, Kerberos y un sistema patentado que utiliza certificados digitales están diseñados para proporcionar a Google mecanismos de acceso seguros y flexibles. Estos mecanismos están diseñados para otorgar solo derechos de acceso aprobados a los hosts del sitio, los registros, los datos y la información de configuración. Google requiere el uso de IDs de usuario únicas, contraseñas seguras, autenticación de dos factores y listas de acceso cuidadosamente controladas para minimizar el posible uso no autorizado de cuentas. La concesión o modificación de derechos de acceso se basa en las responsabilidades del puesto de trabajo del personal autorizado, en los requisitos de las funciones laborales necesarios para realizar las tareas autorizadas y en función de necesidades concretas de información. La concesión o modificación de derechos de acceso debe estar en conformidad con las políticas y la capacitación de acceso a datos internos de Google. Se gestionan las aprobaciones con herramientas de flujo de trabajo que guardan registros de auditoría de todos los cambios. Se registra el acceso a los sistemas para crear un registro de auditoría con el fin de dirimir responsabilidades. Cuando se emplean contraseñas para la autenticación (por ejemplo, para acceder a las estaciones de trabajo), se implementan, al menos, políticas de contraseñas que siguen las prácticas estándar del sector. Estos estándares incluyen restricciones a la reutilización de contraseñas y requisitos mínimos de seguridad de la contraseña.

3. Datos

(a) **Almacenamiento de datos, aislamiento y autenticación**.

Google almacena los datos en un entorno multicliente en servidores propiedad de Google. Se replican los datos, la base de datos de los Servicios del Encargado del Tratamiento y la arquitectura de los sistemas de archivos entre múltiples centros de datos dispersos geográficamente. Google aísla lógicamente los datos de cada cliente. Se utiliza un sistema de autenticación central en todos los Servicios del Encargado del Tratamiento para aumentar la seguridad uniforme de los datos.

(b) **Discos Fuera de Servicio y Directrices de Destrucción de Discos**.

Algunos discos que contienen datos pueden experimentar problemas de rendimiento, errores o fallos del hardware que puede conducir a que sean retirados del servicio ("**Discos Fuera de Servicio**"). Cada Disco Fuera de Servicio se somete a una serie de procesos de destrucción de datos (las "**Directrices de Destrucción de Discos**") antes de salir de las instalaciones de Google, ya sea para su reutilización o su destrucción. Los Discos Fuera de Servicio se borran en un proceso de múltiples pasos y al menos dos validadores independientes verifican que se ha realizado al completo. Los resultados del borrado se registran por el número de serie del Disco Fuera de Servicio para su seguimiento. Finalmente, el Disco Fuera de Servicio borrado se entrega al inventario para su reutilización y su redistribución. Si,

debido a un fallo de hardware, el Disco Fuera de Servicio no puede borrarse, se almacena de forma segura hasta que pueda ser destruido. Cada instalación es auditada periódicamente para monitorizar el cumplimiento de las Directrices de Destrucción de Discos.

(c) **Datos seudónimos**.

Los datos de publicidad online se asocian generalmente con identificadores online que, por sí mismos, se consideran "seudónimos" (es decir, no se pueden atribuir a una persona concreta sin usar información adicional). Google ha implementado un robusto conjunto de políticas y controles técnicos y organizativos para asegurar la separación entre datos seudónimos e información personal identificable del usuario (es decir, información que se podría usar directamente para identificar, contactar o ubicar con precisión a un individuo), como los datos de la cuenta de Google de un usuario. Las políticas de Google solo permiten flujos de información entre datos seudónimos y datos personales identificables en circunstancias estrictamente limitadas.

(d) **Revisiones de lanzamiento**.

Google realiza revisiones de lanzamiento de productos y funciones nuevos antes de que se lancen. Ello incluye una revisión de la privacidad, llevada a cabo por ingenieros especialmente formados y especializados en privacidad. En las revisiones de privacidad, los ingenieros especializados en privacidad se aseguran de que se cumplan todas las políticas y directrices de Google aplicables, incluidas, entre otras, las políticas relacionadas con la seudonimización y la conservación y eliminación de datos.

4. Seguridad del personal

Se exige al personal de Google que se comporte de una manera coherente con las directrices de la empresa respecto a la confidencialidad, la ética empresarial, el uso adecuado y las normas profesionales. Google lleva a cabo comprobaciones razonables de sus antecedentes en la medida en que esté legalmente permitido y de conformidad con la legislación laboral y las disposiciones legales locales aplicables.

Se exige al personal que otorgue un acuerdo de confidencialidad y deben acusar recibo de las políticas de confidencialidad y privacidad de Google, así como cumplirlas. Se proporciona formación en seguridad al personal. Se exige al personal que trata los Datos Personales del Cliente que satisfaga requisitos adicionales en función de su puesto. El personal de Google no efectuará el tratamiento de los Datos Personales del Cliente sin autorización.

5. Seguridad de los Subencargados del Tratamiento

Antes de la contratación de Subencargados del Tratamiento, Google lleva a cabo una auditoría de las prácticas de seguridad y privacidad de los Subencargados del Tratamiento para asegurar que los Subencargados del Tratamiento proporcionen un nivel de seguridad y privacidad adecuado a su acceso a los datos y al alcance de los servicios para los que se les contrata. Una vez que Google ha evaluado los riesgos que representa el Subencargado del Tratamiento, se exige al Subencargado del Tratamiento que celebre un contrato con las condiciones contractuales adecuadas en materia de seguridad, confidencialidad y privacidad, con arreglo a los requisitos establecidos en la sección 11.3 (Requisitos para la contratación de Subencargados del Tratamiento)

Apéndice 3: Términos Adicionales para Legislación No Europea de Protección de Datos

Los siguientes Términos Adicionales para Legislación No Europea de Protección de Datos complementan los presentes Términos del Tratamiento de Datos:

- Anexo de la CCPA sobre proveedores de servicios disponible en business.safety.google/adsprocessorterms/ccpa/ (con fecha de 1 de enero del 2020)
- Anexo para Encargados del Tratamiento de la LGPD disponible en business.safety.google/adsprocessorterms/lgpd/ (con fecha de 16 de agosto del 2020)

Términos del Tratamiento de Datos de Google Ads, versión 4.0

21 de septiembre de 2022

Versiones anteriores

- 27 de septiembre de 2021
- 16 de agosto del 2020
- 12 de agosto del 2020
- 1 de enero del 2020
- 31 de octubre del 2019
- 12 de octubre del 2017