

Condiciones para el tratamiento de datos de Google Ads

Google y la contraparte que acepta las presentes Condiciones (el **"Cliente"**), han celebrado un contrato para la prestación de los Servicios del encargado del tratamiento (con sus enmiendas puntuales, el **"Contrato"**).

Las presentes Condiciones del tratamiento de datos de los anuncios de Google, (las **"Condiciones del tratamiento de datos"**) se suscriben por Google y el Cliente y complementan al Contrato. Las presentes Condiciones del tratamiento de datos entrarán en vigor y reemplazarán cualquier condición previamente aplicable relacionado con el objeto de las mismas (incluida cualquier enmienda de tratamiento de datos o adición de tratamiento de datos relacionada con los Servicios del encargado del tratamiento), a partir de la Fecha de entrada en vigor de las condiciones.

Si usted acepta las presentes Condiciones del tratamiento de datos en nombre del Cliente, usted garantiza que: (a) tiene plena autoridad legal para que las presentes Condiciones del tratamiento de datos sean vinculantes para el Cliente; (b) ha leído y comprende las presentes Condiciones del tratamiento de datos; y que (c) acepta, en nombre del Cliente, las presentes Condiciones del tratamiento de datos. Si no cuenta con la autoridad legal pertinente para que sean vinculantes para el Cliente, no acepte las presentes Condiciones del tratamiento de datos.

1. Introducción

Las presentes Condiciones del tratamiento de datos reflejan el acuerdo de las partes sobre las condiciones que rigen el tratamiento de determinados datos personales en relación con la Legislación europea de protección de datos y con determinada Legislación no europea de protección de datos.

2. Definiciones e interpretación

2.1 En las presentes Condiciones del tratamiento de datos:

"Producto adicional": un producto, servicio o aplicación proporcionada por Google o un tercero que: (a) no sea 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 de otra manera con los Servicios del encargado del tratamiento.

"Términos adicionales para Legislación no europea de protección de datos": los términos adicionales a los que se hace referencia en el Apéndice 3, que reflejan el acuerdo de las partes respecto de los términos que son de aplicación al tratamiento de determinados datos en relación con determinada Legislación no europea de protección de datos.

"Filial": cualquier entidad que, directa o indirectamente, controle, esté controlada o esté bajo control común de una parte.

“Datos personales del cliente”: los datos personales tratados por Google en nombre del Cliente en la prestación de los Servicios del encargado del tratamiento por parte de Google.

“Incidente de datos”: cualquier violación de la seguridad de Google que resulte en la destrucción, pérdida, alteración, divulgación no autorizada de Datos personales del cliente, o acceso a los mismos, de forma accidental o ilegal en sistemas administrados o controlados de otro modo por Google. “Incidente de datos” no incluirá los intentos fallidos o actividades que no comprometan la seguridad de los Datos personales del cliente, incluidos los intentos fallidos de inicio de sesión, pings, exploraciones de puertos, ataques de denegación de servicio y otros ataques de red a los cortafuegos o sistemas en red.

“Herramienta del interesado”: cualquier herramienta (si la hubiera) que una entidad de Google ponga a disposición de los interesados que permita a Google responder de manera estandarizada a determinadas solicitudes de los interesados en relación con los Datos personales del cliente (por ejemplo, configuración de la publicidad en línea o un complemento del navegador de exclusión voluntaria).

“EEE”: el Espacio Económico Europeo.

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

“Legislación europea de protección de datos”: según corresponda: (a) el RGPD; y/o (b) la Ley Federal de Protección de Datos de 19 de junio de 1992 (Suiza).

“Leyes Europeas o Nacionales”: según corresponda: (a) las leyes de la UE o sus Estados Miembros (si el RGPD UE aplica al tratamiento de Datos Personales del Cliente); y/o (b) la ley de Reino Unido o una parte de Reino Unido (si el RGPD de Reino Unido aplica al tratamiento de Datos Personales del Cliente).

“RGPD”: según corresponda: (a) el RGPD UE; y/o (b) el RGPD de Reino Unido.

“Google”: la Entidad de Google que sea parte del Contrato.

“Subencargados del tratamiento de datos de filiales de Google” tiene el significado dado en la Sección 11.1 (Consentimiento para la contratación del Subencargado del tratamiento de datos).

“Entidad de Google”: Google LLC (anteriormente conocido como Google Inc.), Google Ireland Limited o cualquier otra Filial de Google LLC.

“Certificación ISO 27001”: Certificación ISO/IEC 27001:2013 o una certificación comparable para los Servicios del encargado del tratamiento.

“Cláusulas del Contrato Tipo”: términos que figuran en <https://privacy.google.com/businesses/processorterms/mccs>, y que son cláusulas estándar de protección de datos para la transferencia de datos personales a los encargados del tratamiento establecidos en terceros países que no garanticen un

nivel adecuado de protección de los datos, como se describe en el artículo 46 del RGPD UE.

“Legislación no europea de protección de datos”: legislación vigente sobre protección de datos o sobre privacidad fuera del Espacio Económico Europeo, Suiza y el Reino Unido.

“Dirección de correo electrónico a efectos de notificaciones”: la dirección de correo (si la hubiera) que el Cliente haya designado en la Interfaz de usuario de los Servicios del encargado del tratamiento u otros medios proporcionados por Google, para recibir ciertas notificaciones de Google relacionadas con las presentes Condiciones del tratamiento de datos.

“Servicios del encargado del tratamiento”: los servicios aplicables que se enumeran en privacy.google.com/businesses/adsservices.

“Documentación de seguridad”: el certificado emitido para la Certificación ISO 27001 y cualquier otra certificación de seguridad o documentación que Google pueda poner a disposición con respecto a los Servicios del encargado del tratamiento.

“Medidas de seguridad” tiene el significado que se le da en la Sección 7.1.1 (Medidas de seguridad de Google).

“Subencargados del tratamiento de datos”: terceros autorizados con arreglo a las presentes Condiciones del tratamiento de datos para tener acceso lógico y tratar Datos personales del cliente para proporcionar partes de los Servicios del encargado del tratamiento y cualquier soporte técnico relacionado con los mismos.

“Autoridad de Control”: según corresponda: (a) una “autoridad de control” tal y como está definida en el RGPD EU; y/o (b) el “Commissioner” tal y como está definido en el RGPD de Reino Unido.

“Vigencia”: el período desde la Fecha de entrada en vigor de las condiciones hasta el final de la prestación por parte de Google de los Servicios del encargado del tratamiento en virtud del Contrato.

“Fecha de entrada en vigor de las condiciones”: según corresponda:

- (a) 25 de mayo de 2018, si el Cliente hizo clic para aceptar o las partes acordaron de otro modo las presentes Condiciones del tratamiento de datos antes de o en esa fecha; o
- (b) la fecha en la que el Cliente haya hecho clic para aceptar o las partes acordaron de otro modo las presentes Condiciones del tratamiento de datos, si tal fecha es posterior al 25 de mayo de 2018.

“Subencargados del tratamiento de datos terceros” tiene el significado dado en la Sección 11.1 (Consentimiento para la contratación del Subencargado del tratamiento de datos).

“RGPD de Reino Unido”: el RGPD UE tal y como ha sido modificado e incorporado en la legislación de Reino Unido en virtud de la “European Union (Withdrawal) Act

2018”, si la misma está vigente.

- 2.2 Los términos **“responsable del tratamiento”, “interesado”, “datos personales”, “tratamiento”** y **“encargado del tratamiento”** tal y como se utilizan en las presentes Condiciones de responsables del tratamiento tienen los significados dados en el RGPD, y los términos **“importador de datos”** y **“exportador de datos”** tienen los significados que se dan en las Cláusulas Contractuales Tipo.
- 2.3 Las expresiones **“incluido”** o **“incluyendo”** significan **“incluyendo, pero no limitado a”**. Cualesquiera ejemplos en las presentes Condiciones de tratamiento de datos son solamente ilustrativos y no los ejemplos exclusivos de un concepto particular.
- 2.4 Cualquier referencia a un marco legal, ley u otra disposición legislativa es una referencia a la misma con sus periódicas modificaciones o nuevas promulgaciones.
- 2.5 En caso de que estas Condiciones del tratamiento de datos fuesen traducidas a cualquier otro idioma y se diese alguna discrepancia entre la versión en inglés y el texto traducido, la versión en inglés será la aplicable.

3. Duración de las presentes Condiciones de tratamiento de datos

Las presentes Condiciones del tratamiento de datos entrarán en vigor en la Fecha de entrada en vigor de las condiciones y, a pesar del vencimiento de su Vigencia, permanecerán en vigor hasta la eliminación por parte de Google de todos los Datos personales del cliente tal y como se describe en las presentes Condiciones del tratamiento de datos, y cesarán automáticamente cuando se produzca.

4. Aplicación de las presentes Condiciones de tratamiento de datos

- 4.1 **Aplicación de la Legislación europea de protección de datos.** Los Apartados de 5 (Tratamiento de datos) a 12 (Ponerse en contacto con Google; registros del tratamiento), inclusive, solo serán aplicables en la medida en que la Legislación europea de protección de datos sea aplicable al tratamiento de los Datos personales del cliente, incluyendo si:
- (a) el tratamiento se realiza en el contexto de las actividades de un establecimiento del Cliente en el EEE o el Reino Unido; y/o
 - (b) Los Datos personales del cliente son datos personales relacionados con los interesados que se encuentren en el EEE o el Reino Unido y el tratamiento se relaciona con la oferta de bienes o servicios o la supervisión de su comportamiento en el EEE o el Reino Unido.
- 4.2 **Aplicación a los Servicios del encargado del tratamiento.** Las presentes Condiciones del tratamiento de datos solo serán aplicables a los Servicios del encargado del tratamiento para los cuales las partes hayan acordado las presentes Condiciones del tratamiento de datos (por ejemplo: (a) los Servicios del

encargado del tratamiento en los cuales el Cliente haya hecho clic para aceptar las presentes Condiciones del tratamiento de datos; (b) si el Contrato incorpora las presentes Condiciones del tratamiento de datos por referencia, los Servicios del encargado del tratamiento que sean el objeto del Contrato).

- 4.3 **Incorporación de los Términos adicionales para Legislación no europea de protección de datos.** Los Términos adicionales para Legislación no europea de protección de datos son complementarios a estas Condiciones del tratamiento de datos.

5. Tratamiento de datos

5.1 Roles y cumplimiento normativo; autorización.

5.1.1 Responsabilidades del encargado del tratamiento y del responsable del tratamiento.

Las partes reconocen y aceptan que:

- (a) El Apéndice 1 describe el objeto y los detalles del tratamiento de los Datos personales del cliente;
- (b) Google es un encargado del tratamiento de Datos personales del cliente con arreglo a la Legislación europea de protección de datos;
- (c) El Cliente es un responsable del tratamiento o encargado del tratamiento, según corresponda, de Datos personales del cliente con arreglo a la Legislación europea de protección de datos; y
- (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 Autorización de un responsable del tratamiento tercero.

Si el Cliente es un encargado del tratamiento, el Cliente garantiza a Google que las instrucciones y acciones del Cliente con respecto a los Datos personales del cliente, incluida la designación de Google por su parte como otro encargado del tratamiento, han sido autorizadas por el responsable del tratamiento correspondiente.

- 5.2 **Instrucciones del cliente.** Al celebrar las presentes Condiciones del tratamiento de datos, el Cliente instruye a Google para que efectúe el tratamiento de los Datos personales del cliente solo de acuerdo con la legislación aplicable: (a) para proporcionar los Servicios del encargado del tratamiento y cualquier soporte técnico relacionado; (b) tal y como se especifica más a través del uso por parte del Cliente de los Servicios del encargado del tratamiento (incluida la configuración y otras funcionalidades de los Servicios del encargado del tratamiento) y cualquier soporte técnico relacionado; (c) según se documenta por medio del Contrato, incluidas las presentes Condiciones del tratamiento de datos; y (d) tal y como se documenta en otras instrucciones proporcionadas por escrito por el Cliente y reconocidas por Google como instrucciones constitutivas para los propósitos de las presentes Condiciones del tratamiento de datos.

- 5.3 **Cumplimiento de las instrucciones por parte de Google.** Google cumplirá las instrucciones descritas en la Sección 5.2 (Instrucciones del cliente) (incluidas las relativas a transferencias de datos), a menos que las Leyes Europeas o Nacionales a las que está sujeta Google requiera otro tratamiento de datos personales por parte de Google, en cuyo caso Google informará al Cliente (a menos que alguna de dichas leyes prohíba a Google hacerlo por motivos importantes de interés público).
- 5.4 **Productos adicionales.** Si el Cliente utiliza un Producto adicional, los Servicios del encargado del tratamiento pueden permitir que ese Producto adicional acceda a los Datos personales del cliente según sea necesario para la interoperación del Producto adicional con los Servicios del encargado del tratamiento. Para mayor claridad, las presentes Condiciones del tratamiento de datos no se aplican al tratamiento de datos personales en relación con la provisión de ningún Producto adicional utilizado por el Cliente, incluidos los datos personales transmitidos desde ese 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 una funcionalidad de eliminación.

Durante la Vigencia, si:

- (a) la funcionalidad de los Servicios del encargado del tratamiento incluye la opción de que el Cliente elimine los Datos personales del cliente;
- (b) el Cliente utiliza los Servicios del encargado del tratamiento para eliminar ciertos Datos personales del cliente; y
- (c) el Cliente no puede recuperar los Datos personales del cliente eliminados (por ejemplo, de la “papelera”),

entonces, Google eliminará esos Datos personales del cliente de sus sistemas tan pronto como sea razonablemente posible y dentro de un período máximo de 180 días, salvo que las Leyes Europeas o Nacionales exijan su almacenamiento.

6.1.2 Servicios del encargado del tratamiento sin una funcionalidad de eliminación.

Durante la Vigencia, si la funcionalidad de los Servicios del encargado del tratamiento no incluye la opción de que el Cliente elimine los Datos personales del cliente, entonces Google cumplirá:

- (a) cualquier solicitud razonable del Cliente para facilitar dicha eliminación, en la medida en que esto sea posible teniendo en cuenta la naturaleza y la funcionalidad de los Servicios del encargado del tratamiento salvo que las Leyes Europeas o Nacionales exijan su almacenamiento; y
- (b) las prácticas de conservación de datos descritas en policies.google.com/technologies/ads.

Google puede cobrar un importe (basado 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 detalles de cualquier importe aplicable y la base de su cálculo, antes de cualquier eliminación de datos.

- 6.2 **Eliminación al vencimiento del periodo de vigencia.** Al vencimiento del periodo de vigencia, el Cliente le da instrucciones a Google de que elimine todos los Datos personales del cliente (incluidas las copias existentes) de los sistemas de Google de acuerdo con la legislación aplicable. Google cumplirá las presentes instrucciones tan pronto como sea razonablemente posible y dentro de un período máximo de 180 días, salvo que las Leyes Europeas o Nacionales exijan su almacenamiento.

7. Seguridad de datos

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

- 7.1.1 **Medidas de seguridad de Google.** Google implementará medidas técnicas y organizativas para proteger los Datos personales del cliente frente a la destrucción accidental o ilícita o pérdida, alteración [o] divulgación o acceso no autorizado tal y como se describe en el Apéndice 2 (las "**Medidas de seguridad**"). En línea con lo descrito en el Apéndice 2, las Medidas de seguridad incluyen medidas: (a) para cifrar datos personales; (b) para ayudar a garantizar la confidencialidad, integridad, disponibilidad y capacidad de recuperación actuales de los sistemas y servicios de Google; (c) para ayudar a restablecer el acceso oportuno a los datos personales después de un incidente; y (d) para pruebas regulares de efectividad. Google puede actualizar o modificar las medidas de seguridad periódicamente siempre que dichas actualizaciones y modificaciones no den lugar a una degradación de la seguridad general de los Servicios del encargado del tratamiento.
- 7.1.2 **Cumplimiento de las medidas de seguridad por parte del personal de Google.** Google tomará las medidas adecuadas para garantizar el cumplimiento de las Medidas de seguridad por parte de sus empleados, contratistas y Subencargados del tratamiento de datos en la medida en que sea aplicable a su ámbito de actuación, lo que incluye garantizar que todas las personas autorizadas para tratar los Datos personales del cliente se hayan comprometido a su confidencialidad o se encuentren bajo una obligación legal de confidencialidad.
- 7.1.3 **Asistencia de seguridad de Google.** El Cliente acepta que Google (teniendo en cuenta la naturaleza del tratamiento de los Datos personales del cliente y la información que Google tenga disponible) ayudará al Cliente a cumplir las obligaciones del Cliente con respecto a la seguridad de datos personales y violaciones de datos personales, incluyendo (si procede) las obligaciones del Cliente en virtud de los artículos 32 a 34 (inclusive) del RGPD:

- (a) implementar y mantener las Medidas de seguridad de acuerdo con la Sección 7.1.1 (Medidas de seguridad de Google);
- (b) cumplir las condiciones de la Sección 7.2 (Incidentes de datos);
y
- (c) proporcionar al Cliente la Documentación de seguridad de acuerdo con la Sección 7.5.1 (Revisiones de la documentación de seguridad) y la información contenida en las presentes Condiciones 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 rápidamente medidas razonables para minimizar el daño y proteger los Datos personales del cliente.
- 7.2.2 **Detalles del incidente de datos.** Las notificaciones realizadas en virtud de la Sección 7.2.1 (Notificación de incidentes) describirán, en la medida de lo posible, los detalles del Incidente de datos, incluidas las medidas adoptadas para mitigar los riesgos potenciales y los pasos que Google recomienda al Cliente para abordar el Incidente de datos.
- 7.2.3 **Entrega de notificaciones.** Google enviará su notificación de cualquier Incidente de datos a la Dirección de correo electrónico de notificación o, a discreción de Google (incluso si el Cliente no ha proporcionado una Dirección de correo electrónico de notificación), mediante otra comunicación directa (por ejemplo, llamando por teléfono o manteniendo un encuentro en persona). El Cliente es el único responsable de proporcionar la Dirección de correo electrónico de notificación y de garantizar que la Dirección de correo electrónico de notificación esté al día 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 cumplir las obligaciones de notificación de terceros relacionadas con cualquier Incidente de datos.
- 7.2.5 **Ausencia de reconocimiento de culpa por parte de Google.** La notificación o respuesta de Google a un Incidente de datos en virtud de la presente Sección 7.2 (Incidentes de datos) no se interpretará como un reconocimiento por parte de Google de ninguna culpa o 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 de su uso de los Servicios del encargado del tratamiento, incluyendo:
 - (i) hacer un uso apropiado de los Servicios del encargado del tratamiento para garantizar un nivel de seguridad apropiado al riesgo con respecto a los Datos personales del cliente; y
 - (ii) proteger las credenciales, sistemas y dispositivos de autenticación de cuenta que utilice el Cliente para acceder a los Servicios del encargado del tratamiento; y
- (b) Google no tiene la obligación de proteger los Datos personales del cliente que el Cliente elija almacenar o transferir fuera de los sistemas de Google y sus Subencargados del tratamiento de datos.

7.3.2 **Evaluación de seguridad del Cliente.** El Cliente reconoce y acepta (teniendo en cuenta las posibilidades técnicas más reciente de la tecnología, los costes de implementación y la naturaleza, alcance, contexto y propósitos del tratamiento de los Datos personales del cliente, así como los riesgos para los individuos) las Medidas de seguridad implementadas y mantenidas por Google, tal y como se establece en la Sección 7.1.1 (Medidas de seguridad de Google), proporciona un nivel de seguridad adecuado al riesgo con respecto a los Datos personales del cliente.

7.4 **Certificación de seguridad.** Para evaluar y ayudar a garantizar la efectividad continua de las Medidas de seguridad, Google mantendrá la Certificación ISO 27001.

7.5 **Revisiones y auditorías de cumplimiento normativo.**

7.5.1 **Revisiones de la documentación de seguridad.** Para demostrar el cumplimiento por parte de Google de sus obligaciones en virtud de las presentes Condiciones del tratamiento de datos, Google proporcionará la Documentación de seguridad para su revisión por parte del Cliente.

7.5.2 **Derechos de auditoría del Cliente.**

- (a) Google permitirá que el Cliente o un auditor externo designado por el Cliente realice auditorías (incluidas inspecciones) para verificar que Google cumpla las obligaciones contraídas en virtud de las presentes Condiciones del tratamiento de datos de acuerdo con la Sección 7.5.3 (Condiciones comerciales adicionales para auditorías). Google contribuirá a tales auditorías tal y como se describe en la Sección 7.4 (Certificación de seguridad) y en la presente Sección 7.5 (Revisiones y auditorías de cumplimiento normativo).
- (b) Si las Cláusulas Contractuales Tipo se aplican en virtud de la Sección 10.2 (Transferencias de datos), Google permitirá al

Cliente o a un auditor externo designado por el Cliente realizar auditorías como se describe en las Cláusulas Contractuales Tipo de acuerdo con la Sección 7.5.3 (Condiciones comerciales adicionales para las auditorías).

- (c) El Cliente también puede realizar una auditoría para verificar el cumplimiento de Google de las obligaciones contraídas en virtud de las presentes Condiciones 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 **Condiciones comerciales adicionales para auditorías.**

- (a) El Cliente enviará a Google cualquier solicitud de auditoría conforme a la Sección 7.5.2 (a) o 7.5.2 (b) tal y como se describe en la Sección 12.1 (Ponerse en contacto con Google).
- (b) Tras la recepción por parte de Google de una solicitud conforme a la Sección 7.5.3(a), Google y el Cliente discutirán y acordarán por adelantado la fecha razonable de inicio, alcance y duración de cualquier auditoría conforme a la Sección 7.5.2(a) o 7.5.2(b), y los controles de seguridad y confidencialidad aplicables a la misma.
- (c) Google puede cobrar un importe (basado 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 detalles de cualquier importe aplicable y la base de su cálculo, antes de cualquier auditoría. El Cliente será responsable de los honorarios cobrados por cualquier auditor tercero designado por el Cliente para ejecutar dicha auditoría.
- (d) Google puede oponerse a cualquier auditor tercero designado por el Cliente para realizar cualquier auditoría conforme a la Sección 7.5.2(a) o 7.5.2(b) si el auditor, según la opinión razonable de Google, no está debidamente cualificado o no es independiente, es un competidor de Google o es manifiestamente poco idóneo. Cualquier objeción de este tipo por parte de Google requerirá que el Cliente designe a otro auditor o realice la auditoría él mismo.
- (e) Nada de lo previsto en las presentes Condiciones del tratamiento de datos requerirá que Google divulgue al Cliente o a su auditor externo, o que permita al Cliente o su auditor externo acceder a:
 - (i) cualquier dato de cualquier otro Cliente de una Entidad de Google;
 - (ii) cualquier información contable o financiera interna de una Entidad de Google;

- (iii) cualquier secreto comercial de una entidad de Google;
- (iv) cualquier información que, en la opinión razonable de Google, podría: (A) comprometer la seguridad de los sistemas o locales de cualquier Entidad de Google; o (B) hacer que cualquier Entidad de Google incumpliese sus obligaciones conforme a la Legislación europea de protección de datos o sus obligaciones de seguridad y/o privacidad con el Cliente o cualquier tercero; o
- (v) cualquier información a la que el Cliente o su auditor externo intente acceder por cualquier razón que no sea el cumplimiento de buena fe de las obligaciones del Cliente conforme a la Legislación europea de protección de datos.

7.5.4 No modificación de las Cláusulas Contractuales Tipo. Si las Cláusulas Contractuales Tipo se aplican en virtud de la Sección 10.2 (Transferencias de datos), nada en esta Sección 7.5 (Revisiones y auditorías de cumplimiento) varía o modifica ningún derecho u obligación del Cliente o de Google LLC en virtud de las Cláusulas Contractuales Tipo.

8. Evaluaciones de impacto y consultas

El Cliente acepta que Google (teniendo en cuenta la naturaleza del tratamiento y la información que Google tenga disponible) ayudará al Cliente a cumplir las obligaciones del Cliente con respecto a las evaluaciones de impacto y consultas previas, incluyendo (si procede) las obligaciones del Cliente de conformidad con los artículos 35 a 36 (inclusive) del RGPD:

- (a) proporcionando la Documentación de seguridad de acuerdo con la Sección 7.5.1 (Revisiones de la documentación de seguridad);
- (b) proporcionando la información contenida en las presentes Condiciones del tratamiento de datos; y
- (c) proporcionando o poniendo a su 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, Google:

- (a) si la solicitud se realiza a través de una Herramienta del interesado, responderá directamente a la solicitud del interesado de acuerdo con la funcionalidad estándar de esa Herramienta del interesado; o

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

9.2 **Asistencia de Google con la solicitud del interesado.** El Cliente acepta que Google (teniendo en cuenta la naturaleza del tratamiento de los Datos personales del cliente y, si procede, el artículo 11 del RGPD) ayudará al Cliente a cumplir cualquier obligación del Cliente de responder a las solicitudes de los interesados, incluyendo (si procede) la obligación del Cliente de responder a las solicitudes de ejercicio de los derechos del interesado establecidas en el Capítulo III del RGPD:

- (a) proporcionando la funcionalidad de los Servicios del encargado del tratamiento;
- (b) cumpliendo con los compromisos establecidos en la Sección 9.1 (Respuestas a las solicitudes de los interesados); y
- (c) si procede en lo que respecta a los Servicios del encargado del tratamiento, poniendo a disposición Herramientas del interesado.

10. Transferencias de datos

10.1 **Almacenamiento de datos e instalaciones de tratamiento.** El Cliente acepta que Google, sin perjuicio de la Sección 10.2 (Transferencias de Datos), almacene y efectúe el tratamiento de Datos personales del cliente en cualquier país en el que Google o cualquiera de sus Subencargados del tratamiento de datos mantenga instalaciones.

10.2 **Transferencias de Datos.** Si el almacenamiento y/o tratamiento de los Datos personales del cliente implica transferencias de Datos Personales del Cliente desde el EEE, Suiza o el Reino Unido a cualquier país tercero que no esté sujeto a una decisión de adecuación bajo la Legislación europea de protección de datos:

- (a) Se considerará que el cliente (como exportador de datos) ha suscrito las Cláusulas Contractuales Tipo con Google LLC (como importador de datos);
- (b) las transferencias estarán sujetas a las Cláusulas Contractuales Tipo; y
- (c) Google se asegurará de que Google LLC cumpla con sus obligaciones en virtud de dichas Cláusulas Contractuales Tipo con respecto a dichas transferencias.

10.3 **Información del centro de datos.** La información sobre las ubicaciones de los centros de datos de Google se encuentra disponible en www.google.com/about/datacenters/inside/locations/index.html.

11. Subencargados del tratamiento de datos.

11.1 **Consentimiento para la contratación del Subencargado del tratamiento de datos.** El Cliente autoriza específicamente la contratación de las filiales de Google como Subencargados del tratamiento de datos ("**Subencargados del tratamiento de**

datos de filiales de Google”). Además, el Cliente generalmente autoriza la contratación de otros terceros como Subencargados del tratamiento de datos (**“Subencargados del tratamiento de datos terceros”**). Si se aplican las Cláusulas Contractuales Tipo en virtud de la Sección 10.2 (Transferencias de datos), las autorizaciones anteriores constituyen el consentimiento previo por escrito del Cliente para la subcontratación por parte de Google LLC del tratamiento de los Datos personales del Cliente.

- 11.2 **Información sobre los Subencargados del tratamiento de datos.** La información sobre los Subencargados del tratamiento de datos se encuentra disponible en privacy.google.com/businesses/subprocessors.
- 11.3 **Requisitos de contratación del Subencargado del tratamiento de datos.** Al contratar a cualquier Subencargado del tratamiento de datos, Google:
- (a) garantizará por medio de un contrato por escrito que:
 - (i) el Subencargado del tratamiento de datos solo acceda a los Datos personales del cliente y utiliza los mismos en la medida que sea preciso para cumplir las obligaciones que le subcontraten, y lo hace de conformidad con el Contrato (incluidos las presentes Condiciones del tratamiento de datos) y si es aplicable en virtud de la Sección 10.2 (Transferencias de datos), las Cláusulas Contractuales Tipo; y
 - (ii) si el RGPD es aplicable al tratamiento de Datos personales del cliente, las obligaciones de protección de datos establecidas en el artículo 28, apartado 3, del RGPD se imponen al Subencargado del tratamiento de datos; y
 - (b) seguirá siendo totalmente responsable de todas las obligaciones subcontratadas, y todos los actos y omisiones del Subencargado del tratamiento de datos.
- 11.4 **Oportunidad de oponerse a los cambios del Subencargado del tratamiento de datos.**
- (a) Cuando se contrate a un nuevo Subencargado del tratamiento de datos terceros durante la Vigencia, Google informará al Cliente de la contratación (incluido el nombre y la ubicación del subencargado del tratamiento de datos correspondiente y las actividades que realizará), al menos 30 días antes de que el nuevo Subencargado del tratamiento de datos terceros trate cualquier Dato personal del cliente, enviando un correo electrónico a la Dirección de correo electrónico de notificación.
 - (b) El Cliente puede oponerse a cualquier nuevo Subencargado del tratamiento de datos tercero rescindiendo el Contrato inmediatamente después de notificarlo por escrito a Google, con la condición de que el Cliente proporcione dicha notificación en el plazo de los 90 días posteriores a ser informado de la contratación del nuevo Subencargado del tratamiento de datos tercero tal y como se describe en la Sección 11.4(a). Este derecho de rescisión es el único y exclusivo recurso del

Cliente si el Cliente se opone a cualquier nuevo Subencargado del tratamiento de datos tercero.

12. Ponerse en contacto con Google; registros del tratamiento

- 12.1 **Ponerse en contacto con Google.** El Cliente puede ponerse en contacto con Google en relación con el ejercicio de sus derechos en virtud de las presentes Condiciones del tratamiento de datos a través de los métodos descritos en privacy.google.com/businesses/processorsupport o por otros medios que pueda proporcionar Google periódicamente.
- 12.2 **Registros del tratamiento de Google.** El Cliente reconoce que Google tiene la obligación en virtud del RGPD de: (a) recopilar y mantener registros de cierta información, incluidos el nombre y los datos de contacto de cada encargado del tratamiento y/o responsable del tratamiento en nombre de los cuales Google está actuando y (si procede) del representante local y el responsable de la protección de datos de dicho encargado del tratamiento o responsable del tratamiento; y (b) poner dicha información a disposición de cualquier Autoridad de Control. En consecuencia, el Cliente, cuando así lo solicite y sea aplicable al Cliente, proporcionará dicha información a Google a través de la interfaz de usuario de los Servicios del encargado del tratamiento o por otros medios que pueda proporcionar Google, y utilizará dicha interfaz de usuario u otros medios para garantizar que toda la información proporcionada se mantiene precisa y actualizada.

13. Responsabilidad

- 13.1 Límite de responsabilidad. Si el Contrato se rige por las leyes de:
- (a) un estado de los Estados Unidos de América, entonces, no obstante cualquier disposición contraria en el Contrato, la responsabilidad total de cualquiera de las partes hacia la otra parte en virtud de o en relación con las presentes Condiciones del tratamiento de datos se limitará al máximo importe monetario o importe en función de los pagos establecido como tope de la responsabilidad de esa parte en virtud del Contrato (para mayor claridad, cualquier exclusión de demandas de indemnización de la limitación de responsabilidad del Contrato no será aplicable a demandas de indemnización en virtud del Contrato relacionado con la Legislación europea de protección de datos o con la Legislación no europea de protección de datos); o
 - (b) una jurisdicción que no sea un estado de los Estados Unidos de América, entonces la responsabilidad de las partes en virtud de o en relación con las presentes Condiciones del tratamiento de datos estará sujeta a las exclusiones y limitaciones de responsabilidad en el Contrato.
- 13.2 Responsabilidad en caso de que apliquen las Cláusulas Contractuales Tipo. Si se aplican las Cláusulas Contractuales Tipo en virtud de la Sección 10.2 (Transferencias de datos), la responsabilidad total combinada de:

- (a) Google LLC y Google hacia el Cliente; y
- (b) El cliente hacia Google LLC y Google,

en virtud o en relación con el Contrato y las Cláusulas Contractuales Tipo combinados estarán sujetos a la Sección 13.1 (Límite de responsabilidad).

14. Tercera Parte Beneficiaria

En caso de que Google LLC no sea parte del Contrato y se apliquen las Cláusulas Contractuales Tipo en virtud de la Sección 10.2 (Transferencias de datos), Google LLC será una tercera parte beneficiaria de las Secciones 6.2 (Eliminación al vencimiento del plazo), 7.5 (Revisiones y auditorías de cumplimiento), 9.1 (Respuestas a las solicitudes de los interesados), 10.2 (Transferencias de datos), 11.1 (Consentimiento para la contratación de sub encargados del tratamiento) y 13.2 (Responsabilidad en caso de que apliquen las Cláusulas Contractuales Tipo). En la medida en que esta Sección 14 (Tercera Parte Beneficiaria) esté en conflicto o sea inconsistente con cualquier otra cláusula del Contrato, se aplicará esta Sección 14 (Tercera Parte Beneficiaria).

15. Efecto de las presentes Condiciones de tratamiento de datos

Si hubiese algún conflicto o contradicción entre las Cláusulas Contractuales Tipo, los Términos adicionales para Legislación no europea de protección de datos, y el resto de las presentes Condiciones del tratamiento de datos y/o el resto del Contrato, estas serán de aplicación según el siguiente orden de preferencia: (a) las Cláusulas Contractuales Tipo; (b) los Términos adicionales para Legislación no europea de protección de datos; (c) el resto de las presentes Condiciones del tratamiento de datos; and (d) el resto del Contrato. Con sujeción a lo dispuesto en las enmiendas en las presentes Condiciones del tratamiento de datos, el Contrato continuará siendo plenamente válido y efectivo.

16. Cambios a las presentes Condiciones del tratamiento de datos:

16.1 **Cambios a las URL.** Periódicamente, Google puede cambiar cualquier URL a la que se haga referencia en las presentes Condiciones del tratamiento de datos y el contenido en cualquiera de dichas URL, excepto que:

- (a) Google sólo podrá modificar las Cláusulas Contractuales Tipo de acuerdo con las Secciones 16.2(b) - 16.2(d) (Cambios a las Condiciones de Tratamiento de Datos) o incorporar cualquier nueva versión de las Cláusulas Contractuales Tipo que pueda adoptarse en virtud de la Legislación europea de protección de datos, en cada caso de manera que no afecte la validez de las Cláusulas Contractuales Tipo en virtud de la Legislación europea de protección de datos; y
- (b) Google sólo puede cambiar la lista de posibles Servicios del encargado del tratamiento de datos en privacy.google.com/businesses/adsservices:

- (i) para reflejar un cambio en el nombre de un servicio;
- (ii) para añadir un nuevo servicio; o
- (iii) para eliminar un servicio cuando o bien: (x) todos los contratos para la prestación de ese servicio se encuentren rescindidos; o (y) Google tenga el consentimiento del Cliente.

16.2 **Cambios a las Condiciones del tratamiento de datos.** Google puede cambiar las presentes Condiciones del tratamiento de datos si el cambio:

- (a) está expresamente permitido por las presentes Condiciones del tratamiento de datos, incluidos los descritos en la Sección 16.1 (Cambios a las URL);
- (b) refleja un cambio en el nombre o la forma de una entidad legal;
- (c) es necesario para cumplir la legislación y la normativas aplicables, una orden judicial o una directriz publicada por un ente regulador o agencia gubernamentales;
- (d) no: (i) da lugar a una degradación de la seguridad general de los Servicios del encargado del tratamiento; (ii) amplía el alcance ni elimina ninguna restricción de tratamiento de (x) en el caso de los Términos adicionales para Legislación no europea de protección de datos, los derechos de Google para usar o de cualquier modo tratar los datos que sean objeto de los mismos, o (y) en el caso del resto de las presentes Condiciones del tratamiento de datos, los Datos personales del cliente por parte de Google, tal y como se describe en la Cláusula 5.3 (Cumplimiento de las instrucciones por parte de Google); y (iii) tiene un impacto adverso significativo de cualquier otro modo sobre los derechos del Cliente en virtud de las presentes Condiciones del tratamiento de datos, según determine Google.

16.3 **Notificación de cambios.** Si Google tiene la intención de cambiar las presentes Condiciones del tratamiento de datos con arreglo a la Sección 16.2(c) o (d), Google informará al Cliente al menos 30 días (o el período más corto que se requiera para cumplir la legislación aplicable, la regulación aplicable, una orden judicial u orientación emitida por un regulador o agencia gubernamental) antes de que el cambio entre en vigor, (a) enviando un correo electrónico a la Dirección de correo electrónico de notificación; o (b) alertando al Cliente por medio de la interfaz de usuario para los Servicios del encargado del tratamiento. Si el Cliente se opone a tal cambio, el Cliente puede rescindir el Contrato mediante la notificación por escrito a Google en un plazo de 90 días a partir de la fecha en la que Google le haya informado del cambio.

Apéndice 1: Objeto y detalles del tratamiento de datos

Objeto

La prestación de Google de los Servicios del encargado del tratamiento y cualquier soporte técnico relacionado al Cliente.

Duración del tratamiento

La Vigencia más el período desde el vencimiento de la Vigencia hasta la eliminación de todos los Datos personales del cliente por parte de Google de acuerdo con las presentes Condiciones del tratamiento de datos.

Naturaleza y propósito del tratamiento

Google tratará (incluso, según corresponda a los Servicios del encargado del tratamiento y las instrucciones descritas en la Sección 5.2 (Instrucciones del Cliente), recopilando, registrando, organizando, estructurando, almacenando, alterando, recuperando, utilizando, divulgando, combinando, borrando y destruyendo) los Datos personales del cliente con el propósito de proporcionar los Servicios del encargado del tratamiento y cualquier soporte técnico relacionado al Cliente de acuerdo con las presentes Condiciones del tratamiento de datos.

Tipos de datos personales

Los Datos personales del cliente pueden incluir los tipos de datos personales descritos en privacy.google.com/businesses/adsservices.

Categorías de interesados

Los Datos personales del cliente afectan a las siguientes categorías de interesados:

- interesados sobre los cuales Google recopila datos personales en la provisión de los Servicios del encargado del tratamiento; y/o
- los interesados de los cuales se transfieren a Google datos personales en relación con los Servicios del encargado del tratamiento por parte del cliente, bajo las indicaciones del mismo, o en su nombre.

Dependiendo de la naturaleza de los Servicios del encargado del tratamiento, estos interesados pueden incluir individuos: (a) a quien haya ido o vaya dirigida en un futuro la publicidad en línea; (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 las condiciones, Google implementará y mantendrá las Medidas de seguridad establecidas en el presente Apéndice 2. Google puede actualizar o modificar las medidas de seguridad periódicamente siempre que dichas actualizaciones y modificaciones no den lugar a una degradación sustancial de la seguridad 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 los centros de datos físicamente seguros.

Redundancia. Los sistemas de infraestructura han sido diseñados para eliminar los puntos únicos de fallo y minimizar el impacto de los riesgos ambientales previstos. Circuitos duales, conmutadores, redes u otras instalaciones necesarias 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 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 constantemente una garantía fiable de suministro eléctrico 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 diésel tome el relevo. Los generadores diésel 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 un período de 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 accidental o pérdida. Google ha diseñado y

regularmente programa y pone a prueba sus programas de continuidad de la actividad/recuperación de desastres.

(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. Lo anterior está 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 sobre las actividades de ataque en curso y proporcionar información adecuada para responder a los incidentes. La detección de intrusiones de Google implica:

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; y
3. El empleo de tecnologías que remedian de forma automática ciertas situaciones peligrosas.

Respuesta a incidentes. Google hace un seguimiento de una variedad de canales de comunicación para detectar incidentes de seguridad y 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 (PFS, perfect forward secrecy) ayudan a proteger el tráfico y minimizan el impacto de una clave puesta en peligro o una penetración criptográfica.

2. Acceso y controles in situ

(a) **Controles in situ.**

Operativo de seguridad in situ del centro de datos. Los centros de datos de Google mantienen un operativo de seguridad in situ 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 in situ controla las cámaras de Circuito cerrado de televisión (“CCTV”) y todos los sistemas de alarma. El personal

del operativo de seguridad in situ 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 in situ. Todas las personas que accedan al centro de datos deben identificarse, así como mostrar un documento acreditativo al operativo de seguridad in situ. 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 específico y áreas internas que deseen visitar; (ii) firmar a requerimiento del operativo de seguridad in situ; 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 in situ 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 cuando acceden a las puertas del perímetro, 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 centros de datos se restringe por zonas y en función de las responsabilidades laborales del individuo. Las puertas contra incendios en 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 in situ se encarga del seguimiento, registro y 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 in situ 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 acceso.**

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, 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 procesar 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 pueden ser leídos, copiados, modificados o retirados sin autorización durante su tratamiento, uso y 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, registros, datos e información de configuración. Google requiere el uso de identificaciones 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 laborales del personal autorizado; los requisitos de las funciones laborales necesarios para realizar las tareas autorizadas; en función de las necesidades concretas de información. La concesión o modificación de derechos de acceso debe estar en conformidad con las políticas y 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 para 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 de la industria. 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 multiempresa 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 del 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 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 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 vigilar el cumplimiento de las Directrices de destrucción de discos.

4. Seguridad del personal

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

Se exige del personal que otorgue un acuerdo de confidencialidad y deben acusar recibo de las políticas de confidencialidad y privacidad de Google, así como cumplir con ellas. Se proporciona formación en seguridad al personal. Se exige del 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 de datos

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

Apéndice 3: Términos adicionales para Legislación no europea de protección de datos

Los siguientes Términos adicionales para Legislación no europea de protección de datos son complementarios a estas Condiciones del tratamiento de datos:

- "CCPA Service Provider Addendum" que puede encontrarse en privacy.google.com/businesses/processorterms/ccpa (con fecha de 1 de enero de 2020)

Condiciones del tratamiento de datos de Google Ads, Versión 2.0

12 de agosto del 2020

Versiones anteriores

- 1 de enero de 2020
- 31 de octubre de 2019
- 12 de octubre de 2017