

PREÁMBULO

El presente Acuerdo de Protección de Datos de Criteo (en adelante, el “**APD**”) complementa las Condiciones Generales de Servicio de Criteo (en adelante, las “**Condiciones**”) y las Condiciones Específicas de Servicio de Criteo (en adelante, las “**Condiciones Específicas**”) pertinentes o cualquier otro acuerdo aplicable con el Cliente (colectivamente, el “**Acuerdo**”), incorporándose al Acuerdo entre Criteo y el Cliente para la prestación de los correspondientes Servicios de Criteo.

Este APD describe las obligaciones de protección y seguridad de las Partes con respecto a cualquier tratamiento de datos personales realizado en relación con la prestación de los Servicios de Criteo pertinentes, incluido el tratamiento de Datos de servicio si, y únicamente en la medida en que, dichos datos contienen datos personales, de acuerdo con los requisitos de la Ley de protección de datos.

Este APD está organizado en torno a las siguientes secciones:

- **Sección I: Condiciones comunes**
 - La Sección I se aplica cuando el Cliente ha solicitado Servicios a Criteo, independientemente del tipo de Servicios solicitados.
- **Sección II: Condiciones de corresponsables del tratamiento**
 - La Sección II se aplica cuando el Cliente ha solicitado Servicios en los que Criteo y el Cliente actúan como Corresponsables del tratamiento según lo establecido en las Condiciones Específicas pertinente (los “**Servicios de Corresponsable del tratamiento**”).
- **Sección III: Condiciones de Responsable del tratamiento a Encargado del tratamiento (sólo aplicable al Servicio de Mabaya)**
 - La Sección III se aplica cuando el Cliente ha solicitado Servicios en los que el Cliente actúa como Responsable del tratamiento y Criteo actúa como Encargado del tratamiento, tratando Datos personales en nombre del Cliente según se establece en las Condiciones Específicas pertinente (los “**Servicios de Responsable del tratamiento a Encargado del tratamiento**”).

La Sección I de este APD siempre se aplica a las Partes. La aplicación de la Sección II y/o III dependerá del estado bajo el cual Criteo opere y que se especifique en las Condiciones Específicas o en cualquier otro acuerdo aplicable al Servicio solicitado por el Cliente.

Sección I: Condiciones comunes

Las disposiciones de esta Sección I “Condiciones comunes” son siempre de aplicación cuando el Cliente ha solicitado Servicios a Criteo, independientemente del tipo de Servicios solicitados.

1 Definiciones

A menos que se indique lo contrario en el presente documento, se aplican a este APD las definiciones establecidas en el Acuerdo. También se aplicarán a este APD las definiciones adicionales establecidas a continuación.

“Consentimiento” se refiere a cualquier indicación libremente dada, específica, informada e inequívoca de los deseos del Interesado mediante la cual, a través de una declaración o una acción afirmativa clara, denota que está de acuerdo con el Tratamiento de Datos personales relacionados con él o ella.

“Responsable del tratamiento” se refiere a la persona física o jurídica, autoridad pública, agencia u otro organismo que, sola o conjuntamente con otras, determina los fines y medios del Tratamiento de Datos personales. En virtud de la Sección II de este APD, Criteo S.A., como sociedad matriz del Grupo Criteo, y el Cliente actúan como Corresponsables del tratamiento y en virtud de la Sección III de este APD, el Cliente actúa como Responsable del tratamiento. El término “Responsable del tratamiento” se considera “Negocio” en virtud de la Ley de Derechos de Privacidad de California (California Privacy Rights Act, CPRA).

| | | |
|--|--------------|--|
| “Ley de protección de datos” | de de | Significa todas las leyes y reglamentos presentes y futuros relativos al Tratamiento de Datos Personales y privacidad, incluyendo sin limitación (a) el Reglamento General de Protección de Datos de la Unión Europea (“RGPD UE”), (b) la Ley de Protección de Datos del Reino Unido de 2018 y el RGPD (“RGPD del Reino Unido”), (c) la Ley de Privacidad del Consumidor de California (“CCPA”) y la Ley de Derechos de Privacidad de California (“CPRA”), (d) la Ley de Privacidad del Consumidor en Virginia (“VCDPA”), (e) la Ley de Privacidad de Colorado, (f) la Ley de Privacidad de Connecticut (“CTDPA”), (g) la Ley de Privacidad del Consumidor de Utah (“UCPA”), (h) la Ley de Privacidad del Consumidor de Oregón (“OCA”), la Ley de Privacidad y Seguridad de Datos de Texas (“TDPSA”), (j) la Ley de Privacidad del Consumidor de Montana (“MTCDPA”), (k) la Ley de Protección de la Información Personal de Corea del Sur (Ley nº 10465 de 29 de marzo de 2011), junto con cualquier normativa que las modifique o sustituya en cada momento. Para mayor claridad, Ley de Protección de Datos también incluye todos los requisitos legalmente vinculantes emitidos por las autoridades de protección de datos competentes i) que rigen el tratamiento y la seguridad de la información relacionada con las personas y proporcionan normas para la protección de los derechos y libertades de dichas personas con respecto al tratamiento de los datos relacionados con ellas, ii) que especifican las normas para la protección de la privacidad en relación con el tratamiento de datos y las comunicaciones electrónicas, o iii) que promulgan derechos para personas que sean exigibles para las organizaciones con respecto al tratamiento de sus datos personales, incluidos los derechos de acceso, rectificación y supresión. Cualquier Ley de Protección de Datos listada aquí aplica únicamente al Cliente en la medida que así se establezca según los criterios de cada regulación. |
| “Interesado(s)” | | se refiere a una persona física identificable que puede ser identificada, directa o indirectamente, en particular mediante referencia a un identificador (por ejemplo, un nombre, un número de identificación, datos de ubicación, un identificador en línea) o a uno o más factores específicos de esa persona física. A efectos de este APD, “Interesado” se refiere a las personas físicas cuyos Datos personales se tratan como parte de la prestación de los Servicios de Criteo pertinentes. |
| “Corresponsable del tratamiento” | | se refiere a un Responsable del tratamiento que actúa conjuntamente con otro u otros. En virtud de la Sección II de este APD, Criteo y el Cliente actúan como corresponsables del tratamiento. |
| “Datos personales” | | se refiere a cualquier información que identifique, se relacione, describa o pueda asociarse, o pueda vincularse razonablemente, con una persona física o un domicilio identificados o identificables tratados en relación con la prestación de los Servicios de Criteo pertinentes. |
| “Violación de la seguridad de los Datos personales” | | se refiere a una infracción de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilícito a Datos personales transmitidos, almacenados o tratados, en general. |
| “Encargado del tratamiento” | del | se refiere a una persona física o jurídica, autoridad pública, agencia u otro organismo que trata Datos personales en nombre del Responsable del tratamiento. En virtud de la Sección II de este APD, los encargados del tratamiento que pueden ser contratados por Criteo o el Cliente son Encargados del tratamiento y en virtud de la Sección III de este APD, Criteo actúa como Encargado del tratamiento. |
| “Tratamiento” | | se refiere a cualquier operación o conjunto de operaciones que se realice en Datos personales o en conjuntos de Datos personales, ya sea por medios automatizados o no, como la recogida, el registro, la organización, estructuración, conservación, adaptación o alteración, recuperación, consulta, el uso, la comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, el cotejo o la combinación, limitación, supresión o destrucción. |
| “Autoridad reguladora” | | se refiere al poder público u organismo gubernamental aplicable responsable de supervisar el cumplimiento de la Ley de protección de datos, incluyendo sin limitación: la Comisión Nacional de la Informática y las Libertades de Francia – CNIL – (la autoridad reguladora de Criteo); la Oficina del Comisionado de Información del Reino Unido; la Agencia de Protección de la Privacidad de California; o también los procuradores generales del estado de EE. UU. |

Los términos “Business”, “Fines comerciales”, “Venta”, “Proveedor de servicios” y “Compartir” tendrán el mismo significado que en la Ley de protección de datos aplicable, y sus términos reconocidos se interpretarán en consecuencia.

2 Cumplimiento de la legislación

- 2.1** Cada Parte cumplirá, y tendrá que ser capaz de demostrar el cumplimiento de, sus respectivas obligaciones en virtud de la Ley de protección de datos y de conformidad con este APD.
- 2.2** El Cliente reconoce y acepta específicamente que su uso de los Servicios de corresponsable del tratamiento y de responsable a encargado del tratamiento cumple con la Ley de protección de datos.

3 Autorizaciones

- 3.1** Una Parte no divulgará Datos personales a la otra Parte, excepto cuando la Parte divulgadora garantice a la otra Parte que esta divulgación cumple con la Ley de protección de datos y que ha cumplido con cualquier requisito aplicable de información, notificación o de autorización o consentimiento del poder público o los Interesados pertinentes, con respecto a cualesquiera Datos personales que proporcione la Parte divulgadora a la otra Parte. Cada Parte divulgadora debe conservar pruebas del cumplimiento de dichos requisitos durante la vigencia del Acuerdo y proporcionarlas inmediatamente a la otra Parte previa solicitud.

Nada de lo contenido en este APD prohibirá o limitará los derechos de Criteo a llevar a cabo la anonimización de los Datos personales tratados en relación con el Acuerdo, y en la medida en que lo exija la Ley de protección de datos, el Cliente autoriza por el presente a Criteo a ejecutar técnicas de anonimización en cumplimiento de la Ley de protección de datos. En aras de la claridad, los datos resultantes de la anonimización efectiva y conforme no están sujetos a este APD ni, de manera más general, a la Ley de protección de datos.

4 Cooperación

- 4.1** Las Partes cooperarán para cumplir con la Ley de protección de datos y con sus obligaciones conforme al presente APD.

Las Partes conservarán la documentación correspondiente sobre las actividades de Tratamiento llevadas a cabo por cada una de ellas y sobre su cumplimiento de la Ley de protección de datos y de este APD con respecto al Corresponsable del tratamiento y a los Servicios de Responsable del tratamiento a Encargado del tratamiento.

En caso de investigación, procedimiento, solicitud formal de información o documentación, o cualquier suceso similar en relación con una autoridad de protección de datos y en relación con el Corresponsable del tratamiento o los Servicios de responsable a encargado del tratamiento o con los Datos personales, las Partes tratarán de forma inmediata y adecuada las consultas de la otra Parte relacionadas con el Tratamiento de Datos personales en virtud del Acuerdo.

- 4.2** En caso de cualquier modificación a la Ley de protección de datos o la promulgación de una nueva, las Partes de mutuo acuerdo realizarán las modificaciones o revisiones necesarias a este APD.

5 Delegados de protección de datos

Criteo y el Cliente nombraron a un delegado de protección de datos. Puede ponerse en contacto con el delegado de protección de datos de Criteo en: dpo@criteo.com. Los datos de contacto del delegado de protección de datos del Cliente deben comunicarse a Criteo.

Sección II: Condiciones de los Corresponsables del tratamiento

6 Ámbito de esta Sección II

Esta Sección II se aplicará únicamente con respecto al Tratamiento de Datos personales llevado a cabo en el contexto de la prestación por parte de Criteo de los Servicios de Corresponsable del tratamiento solicitados por el Cliente.

De conformidad con el artículo 26 del RGPD, las Partes determinan sus respectivas responsabilidades para el cumplimiento de sus obligaciones en virtud del RGPD.

- 6.1** A efectos de la CPRA, el Cliente será un “Business” y Criteo será un “Tercero”.

7 Obligaciones de las Partes al actuar como Corresponsables del tratamiento

7.1 Al tratar Datos personales como Corresponsables del tratamiento en virtud de la Sección II de este APD, cada Parte acepta que:

Cumplirá con cualquier requisito que surja en virtud de la Ley de protección de datos y no ejecutará sus obligaciones en virtud de este APD ni pedirá al otro corresponsable del tratamiento que cumpla con sus obligaciones de tal manera que haga que el otro corresponsable del tratamiento incumpla alguna de sus obligaciones en virtud de la Ley de protección de datos.

Tendrá en cuenta todos los principios de protección de datos previstos en la Ley de protección de datos, incluidos, entre otros, los principios de limitación de la finalidad, minimización de datos, precisión, limitación de conservación, seguridad, integridad y confidencialidad, transparencia y protección de Datos personales por diseño y por defecto.

Mantendrá un registro del Tratamiento de los Datos personales bajo su responsabilidad.

Ejecutará medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad correspondiente a los riesgos que presenta el Tratamiento de los Datos personales que lleva a cabo (incluido, para el Cliente, en relación con las Propiedades digitales del Cliente), en particular para proteger los Datos personales contra la destrucción accidental o ilícita o la pérdida o alteración accidental, así como la divulgación o acceso no autorizados.

Tomará todas las medidas necesarias para abordar cualquier Violación de la seguridad de los Datos personales relacionada con los Datos personales que trata, mitigar sus efectos, prevenir posteriores infracciones de la seguridad de los datos personales y, cuando sea necesario, informará de ello a la(s) autoridad(es) de protección de datos competentes y a los Interesados.

Cooperará en la preparación de las evaluaciones de impacto relativas a la protección de datos que sean necesarias.

- (a) Llevará a cabo cualquier evaluación, consulta y/o notificación a las autoridades de protección de datos competentes o a los Interesados, en relación con el Tratamiento que lleve a cabo; y
- (b) Gestionará las solicitudes y/o quejas de los Interesados que reciba, en particular las solicitudes relacionadas con el ejercicio de sus derechos en virtud de la Ley de protección de datos, incluidos los derechos de acceso, rectificación, supresión y objeción y el derecho a retirar el Consentimiento. Cuando una Parte reciba una solicitud de derecho de un Interesado con respecto a Datos personales tratados por la otra Parte, dicha Parte receptora remitirá al Interesado a la política de privacidad de la otra Parte explicando cómo ejercer su solicitud de derecho con dicha otra Parte, a fin de permitir que dicha otra Parte responda directamente a la solicitud del Interesado.

Obligaciones de Criteo

Criteo será el único responsable, de acuerdo con y en la medida requerida por la Ley de protección de datos, de incluir un enlace a la página de Política de Privacidad de Criteo (www.criteo.com/privacy), que incluirá información para los Interesados sobre cómo desactivar el Servicio Criteo (e insertará un enlace de “exclusión voluntaria”) en todos los anuncios publicados en las Propiedades digitales del Cliente.

7.2 En la medida que Criteo es un Tercero de conformidad con la CPRA: (a) el uso de Datos Personales de Criteo se limitará a los propósitos específicos identificados en el Acuerdo y Criteo no excederá dichos propósitos específicos; (b) Criteo cumplirá con las obligaciones que le son aplicables y proveerá el mismo nivel de protección de privacidad respecto a Datos Personales que sea requerido a un Negocio de conformidad con la CPRA ; (c) Criteo concede al Cliente el derecho, con una notificación previa razonable, de tomar medidas razonables y apropiadas para asegurar que Criteo utiliza Datos Personales de conformidad con este Contrato y la Ley de protección de datos aplicable, incluyendo medidas razonables y apropiadas para detener y remediar el uso no autorizado de Datos Personales; y (d) Criteo notificará al Cliente si determina que ya no puede cumplir con sus obligaciones bajo la Ley de protección de datos aplicable.

8 Obligaciones del Cliente

8.1 El Cliente será el único responsable, de acuerdo con y en la medida requerida por la Ley de protección de datos, de:

- (a) proporcionar a los Interesados toda la información necesaria de conformidad con la Ley de protección de datos, incluido de conformidad con los Artículos 13 y 14 del RGPD, con respecto al Tratamiento de los Datos personales en relación con los Servicios de corresponsable del tratamiento;

proporcionar un aviso adecuado en las Propiedades digitales del Cliente para cualquier Tratamiento de Datos personales pertinente por parte de Criteo respecto de los Servicios de corresponsable del tratamiento, incluido un enlace a la política de privacidad de Criteo (www.criteo.com/privacy);

- (b) recoger y documentar el Consentimiento o los procedimientos de exclusión del Tratamiento, según corresponda, obtenidas de los Interesados;
- (c) implementar mecanismos de elección para solicitar un Consentimiento válido de los Interesados o procedimientos de exclusión voluntaria, según proceda de conformidad con la Ley de protección de datos y, cuando proceda, con los requisitos específicos de la Autoridad Reguladora local competente;
- (d) cuando sean aplicables provisiones de exclusión voluntaria, ofrecer a los Interesados el derecho de exclusión de la venta y compartir sus Datos personales o el uso de los Datos personales con fines de publicidad dirigida;
- (e) cumplir con los requisitos aplicables al periodo de validez del Consentimiento recogido y solicitar el Consentimiento una vez que este periodo de validez haya caducado; y
- (f) proporcionar inmediatamente a Criteo, previa solicitud y en cualquier momento, pruebas de que el Cliente ha obtenido el Consentimiento de un Interesado.

Sección III: Condiciones de Responsable del tratamiento a Encargado del tratamiento (sólo aplicable al Servicio de Mabaya)

9 Ámbito de esta Sección III

9.1 Esta Sección III se aplicará únicamente con respecto al Tratamiento de Datos personales llevado a cabo en el contexto de los Servicios de Responsable del tratamiento a Encargado del tratamiento que solicite el Cliente, actuando como Responsable del tratamiento o Business (según proceda), y en el que Criteo actúe como Encargado del tratamiento o Proveedor de Servicios (según proceda), y para el cual el objeto, la naturaleza y el fin, el tipo de Datos personales, las categorías de Interesados y la duración del Tratamiento se establecen en el Apéndice 1 “Servicios de Responsable del tratamiento a Encargado del tratamiento: Detalles del tratamiento de Datos personales”.

10 Obligaciones del Cliente

El Cliente no proporcionará Datos personales a Criteo excepto cuando sea necesario para la prestación de los Servicios de Criteo y a menos que el Cliente haya hecho las notificaciones correspondientes y haya obtenido el Consentimiento necesarios, en cada caso, de los Interesados cuyos Datos personales sean tratados por Criteo conforme al Acuerdo. El Cliente, en su uso de los Servicios de Criteo, tratará los Datos personales de acuerdo con los requisitos de la Ley de protección de datos y notificará inmediatamente a Criteo si el Cliente infringe cualquier Ley de protección de datos. Las instrucciones del Cliente para Criteo relacionadas con el Tratamiento de Datos personales cumplirán con la Ley de protección de datos. El Cliente será el único responsable de garantizar la exactitud, legalidad y calidad de los Datos personales y de garantizar que el Tratamiento confiado a Criteo tenga una base jurídica adecuada de conformidad con la Ley de protección de datos.

Obligaciones de Criteo

Instrucciones del Cliente. Criteo tratará los Datos personales para los Servicios de Responsable de tratamiento a Encargado del tratamiento pertinentes únicamente según las instrucciones documentadas del Cliente. El Cliente no podrá indicar a Criteo que trate Datos personales de una manera no compatible con el Acuerdo y, más concretamente, con este APD. Criteo informará inmediatamente al Cliente en caso de estimar, razonablemente, que no puede seguir sus instrucciones, o si dichas instrucciones no son compatibles con las Condiciones Específicas o, en general, con el Acuerdo.

Datos inexactos u obsoletos. Criteo informará al Cliente si tiene conocimiento de que los Datos personales son inexactos o han quedado obsoletos, y cooperará previa solicitud con el Cliente para suprimir o rectificar dichos datos.

Tratamiento de datos personales. En la medida en que lo exija la Ley de protección de datos aplicable, el Cliente solo indicará a Criteo que trate Datos personales para los Fines comerciales permitidos en virtud de la Ley de protección de datos aplicable y revelará Datos personales a Criteo solo para los fines limitados y especificados indicados en el Acuerdo. El Cliente se reserva el derecho, previo aviso razonable, de tomar las medidas apropiadas para ayudar a garantizar que Criteo utilice los Datos personales transferidos de forma coherente con las obligaciones del Cliente en virtud de la Ley de protección de datos aplicable, incluidas las medidas apropiadas para detener y remediar el uso no autorizado de los Datos personales.

Criteo no deberá: (a) Vender o compartir datos personales; (b) conservar, usar, o divulgar Datos personales para cualquier fin distinto de los Fines comerciales especificados en el Acuerdo; (c) conservar, usar, o divulgar Datos personales fuera de la relación comercial directa entre el Cliente y Criteo; o (d) combinar los Datos personales que reciba del Cliente con los Datos personales que reciba de, o en nombre de, otra persona o personas, o recopile de su propia interacción con los Interesados, siempre que Criteo pueda combinar Datos personales para llevar a cabo un Fin comercial (con la excepción de “servicios de publicidad y marketing”, según se define en la Ley de protección de datos aplicable). Criteo cumplirá con las obligaciones aplicables y proporcionará el mismo nivel de protección de la privacidad que exige la Ley de protección de datos aplicable, y ayudará al Cliente mediante las medidas técnicas y organizativas adecuadas para cumplir con los requisitos de la Ley de protección de datos, teniendo en cuenta la naturaleza del tratamiento. Criteo notificará al Cliente si determina que ya no puede cumplir sus obligaciones en virtud de la Ley de protección de datos aplicable.

10.1 Medidas técnicas y organizativas. Criteo implementará las medidas técnicas y organizativas adecuadas para garantizar la seguridad de los Datos personales, incluida la protección contra una Violación de la seguridad de los Datos personales. En el cumplimiento de sus obligaciones en virtud de este párrafo, Criteo ejecutará al menos las medidas técnicas y organizativas especificadas en el Apéndice 2 “Anexo de seguridad”. Por el presente, el Cliente confirma a Criteo que considera que las medidas técnicas y organizativas de Criteo especificadas en el Apéndice 2 “Anexo de seguridad” proporcionan un nivel adecuado de seguridad. Criteo también ayudará al Cliente a cumplir con sus obligaciones en relación con la seguridad del tratamiento de datos personales, incluyendo en virtud del artículo 32 del RGPD.

10.2 Violación de la seguridad de los Datos personales. En caso de Violación de la seguridad de los Datos personales relacionada con los Datos personales tratados por Criteo, Criteo tomará las medidas adecuadas para abordar la Violación, incluidas medidas para mitigar sus efectos adversos. Criteo también informará al Cliente sin demora indebida en cuanto haya tenido conocimiento del incumplimiento y tras disponer del plazo necesario para facilitar la información pertinente, incluida, por ejemplo, una descripción de la naturaleza del incumplimiento (incluidas, cuando sea posible, categorías y número aproximado de Interesados y registros de Datos personales afectados), sus posibles consecuencias y las medidas adoptadas o propuestas para abordar el incumplimiento, incluidas, cuando proceda, medidas para mitigar sus posibles efectos adversos. En caso de una Violación de la seguridad de los Datos personales relacionada con los Datos personales tratados por Criteo, el Cliente será el único responsable de notificar a los Interesados y/o a las Autoridades Reguladoras según lo requiera la Ley de protección de datos, y Criteo cooperará y ayudará al Cliente a permitir el cumplimiento de cualquier solicitud de una Autoridad Reguladora y/o Interesados afectados, teniendo en cuenta la naturaleza del Tratamiento y la información disponible para Criteo. Antes de que se realice dicha notificación, el Cliente consultará y dará a Criteo la oportunidad de comentar cualquier notificación realizada en relación con una Violación de la seguridad de los Datos personales. Nada de lo contenido en este APD se interpretará como una exigencia de que Criteo infrinja o demore el cumplimiento de cualquier obligación legal que pueda tener con respecto a una Violación de la seguridad de los Datos personales. Criteo no tendrá responsabilidad por las obligaciones de gestión y notificación de Violación de la seguridad de los Datos personales descritas en esta Sección, a menos que la Violación de la seguridad de los Datos personales sea causada por el incumplimiento por Criteo de las obligaciones de seguridad en virtud de la Sección 12.4 de este APD u otra infracción de la Ley de protección de datos por parte de Criteo.

10.3 Acceso a Datos personales. Criteo concederá acceso a los Datos personales a los miembros de su personal solo en la medida estrictamente necesaria para la ejecución, administración y supervisión del Acuerdo y de conformidad con este APD. Se asegurará de que las personas autorizadas para tratar los Datos personales se hayan comprometido a cumplir uno o varios acuerdos de confidencialidad o estén sujetas a una obligación legal de confidencialidad adecuada.

Derechos de los Interesados. En la medida en que lo permita la ley, Criteo notificará de inmediato al Cliente cualquier solicitud que haya recibido de un Interesado para ejercer los derechos del Interesado, incluidos los derechos a: conocimiento/acceso; corrección; eliminación; limitación; objeción; portabilidad de datos; excluirse del tratamiento y/o la venta o intercambio de datos personales; limitar el uso o la divulgación de Datos personales sensibles; o cualquier otra solicitud con respecto a los Datos personales del Interesado correspondiente, según lo establecido en la Ley de Protección de Datos aplicable. Criteo no responderá a la propia solicitud. Criteo ayudará razonablemente al Cliente implementando las medidas técnicas y organizativas adecuadas, en la medida de lo posible, para cumplir con sus obligaciones de responder a las solicitudes de los Interesados de ejercer sus derechos en virtud de la Ley de Protección de Datos, teniendo en cuenta la naturaleza del Tratamiento. En la medida en que lo permita la ley, el Cliente será responsable de cualquier coste derivado de la prestación de dicha asistencia por parte de Criteo. Nada de lo dispuesto en esta Sección 13 exigirá a que Criteo divulgue o revele ningún secreto comercial.

Evaluación de impacto relativa a la protección de datos. A solicitud del Cliente, a cargo del Cliente y en la medida requerida por la Ley de Protección de Datos, Criteo ayudará al Cliente a cumplir con cualquier evaluación de impacto relativa a la protección de datos requerida a solicitud del Cliente, teniendo en cuenta la información disponible para Criteo. En la medida en que lo exija el RGPD o el RGPD del Reino Unido, Criteo proporcionará asistencia razonable al Cliente en su cooperación o colaboración previa con una Autoridad Reguladora en la ejecución de sus tareas relacionadas con esta Sección 13.1.

Subencargados del tratamiento. Criteo podrá contratar a subencargados del tratamiento según se establece en el Apéndice 1 “Servicios de Responsable del tratamiento a Encargado del tratamiento: Detalles del tratamiento de datos personales”. El Cliente proporciona a Criteo la autorización general para contratar a otros subencargados para llevar a cabo el Tratamiento para los Servicios pertinentes de Responsable a Encargado. Previa solicitud por escrito del Cliente, Criteo informará al Cliente de cualquier cambio relativo a la adición o sustitución de subencargados del tratamiento. Si el Cliente se opone a dichos cambios por razones razonables [en relación con la protección de datos] en un plazo de treinta (30) días desde la notificación por parte de Criteo al Cliente, las Partes debatirán de buena fe con vistas a encontrar una solución mutuamente aceptable. Si las Partes no logran un acuerdo, Criteo podrá resolver el Acuerdo en su totalidad o en parte con respecto únicamente a los Servicios de Responsable a Encargado del tratamiento afectados. Cuando contrate a otro Encargado del tratamiento, Criteo celebrará un acuerdo vinculante para dicho Encargado del tratamiento y establecerá las mismas obligaciones de protección de datos, o más estrictas, que las establecidas en este APD, proporcionando en particular garantías suficientes para ejecutar medidas técnicas y organizativas similares.

10.4 Tratamiento de Datos personales al margen de las Instrucciones del Cliente. No obstante lo anterior, si la legislación aplicable o una decisión vinculante de una autoridad competente requiere que Criteo trate Datos personales al margen de las instrucciones del Cliente con el fin de prestar los Servicios de Responsable a Encargado del tratamiento, Criteo informará de ello al Cliente, a menos que lo prohíba la legislación aplicable.

10.5 Auditoría. El Cliente podrá solicitar por escrito, a intervalos razonables, que Criteo ponga a disposición del Cliente información relativa al cumplimiento de Criteo de sus obligaciones en virtud de la Sección III de este APD, en forma de copia de las fiscalizaciones o certificaciones de terceros más recientes de Criteo.

El Cliente puede solicitar una auditoría *in situ* de las actividades de Tratamiento de Criteo descritas en la Sección III de este APD mediante notificación razonable a Criteo. Dicha auditoría interna solo podrá realizarse cuando (i) la información puesta a disposición por Criteo según lo establecido anteriormente sea insuficiente, (ii) se haya producido una Violación de la seguridad de los Datos personales o (iii) dicha auditoría sea requerida por la Ley de protección de datos o una Autoridad Reguladora.

Las Partes acordarán el ámbito, el momento y la duración de la auditoría. La auditoría no puede interferir de forma injustificada con las actividades de Criteo.

El Cliente solo podrá nombrar a un auditor externo que no sea competidor de Criteo. Dicho auditor externo celebrará un acuerdo de confidencialidad con Criteo y el Cliente antes de llevar a cabo la fiscalización.

Después de la auditoría *in situ*, el Cliente compartirá inmediatamente con Criteo los resultados de esta.

Previa solicitud, las Partes pondrán a disposición de la Autoridad Reguladora la información mencionada en esta cláusula, incluidos los resultados de cualquier auditoría.

El Cliente asumirá todos los costes relacionados con las auditorías.

10.6 Cesión de Datos personales. Cualquier cesión de datos a un tercer país o a una organización internacional por parte de Criteo se realizará únicamente sobre la base de instrucciones documentadas del Cliente de conformidad con el Capítulo V del RGPD. El Cliente acepta que cuando Criteo contrate a un subencargado del tratamiento de conformidad con la Cláusula 0 para llevar a cabo actividades de Tratamiento específicas (en nombre del Cliente) y dichas actividades de Tratamiento impliquen una cesión de Datos personales en el sentido del Capítulo V del RGPD, Criteo y el Subencargado del tratamiento pueden garantizar el cumplimiento del Capítulo V del RGPD mediante el uso de cláusulas contractuales tipo adoptadas por la Comisión Europea de conformidad con el Artículo 46(2) del RGPD, siempre que se cumplan las condiciones de uso de dichas cláusulas contractuales tipo.

Consecuencias de la resolución. Si el Cliente resuelve un Servicio de Responsable del tratamiento a Encargado del tratamiento, o si el Acuerdo vence o se resuelve por cualquier motivo, Criteo, a elección del Cliente, eliminará todos los Datos personales tratados solo para ese Servicio de Responsable a Encargado del tratamiento, o devolverá al Cliente todos esos Datos personales.



Criteo proporcionará la certificación, según corresponda, de que se han eliminado las copias de dichos Datos personales, previa solicitud por escrito del Cliente, sin perjuicio de cualquier copia de seguridad operativa que conserve Criteo durante un periodo razonable de acuerdo con las normas del sector. Si la legislación aplicable prohíbe a Criteo eliminar los Datos personales, Criteo garantiza que continuará asegurándose del cumplimiento de este APD y solo tratará dichos Datos personales en la medida y durante el tiempo que exija la legislación aplicable.

Los firmantes autorizados de las Partes han formalizado debidamente este APD:

CLIENTE

Firma: _____

Nombre: _____

Cargo: _____

Fecha: _____

CRITEO

Firma: _____

Nombre: _____

Cargo: _____

Fecha: _____

APÉNDICE 1: Servicios de Responsable del tratamiento a Encargado del tratamiento: Detalles del tratamiento de datos personales

(sólo aplicable al Servicio de Mabaya)

| Categoría de Interesados | | | |
|--|--|--|--|
| Categorías de Interesados cuyos datos personales se tratan | Usuarios de Propiedades digitales del Cliente (compradores) | Empleados del Responsable del tratamiento | Vendedores (empleados/representantes) |
| Categorías de datos personales tratados | Identificadores que consisten en una serie de caracteres (identificador contenido en una cookie u otro) proporcionados por el Responsable del tratamiento de datos (cuando estos datos resulten ser Datos personales en virtud de la Ley de protección de datos) | Nombre y direcciones de correo electrónico de los empleados/representantes autorizados del Responsable del tratamiento | Direcciones de correo electrónico de los vendedores (para enviarles comunicaciones y notificaciones) |
| Datos sensibles | N/A | | |
| Naturaleza del tratamiento | Recogida, alojamiento, tratamiento para proporcionar el Servicio, supresión | | |
| Finalidad(es) para la(s) que se tratan los datos personales en nombre del responsable del tratamiento | Correlación de conversiones con clics (en el contexto de los Anuncios) | Comprobaciones de identidad (página de inicio de sesión) | |
| | | Administración de cuentas | |
| | | Enviar notificación por correo electrónico a los vendedores | |
| Duración del tratamiento | Vigencia del Acuerdo | | |

El Cliente reconoce y autoriza el uso por parte de Criteo de las siguientes entidades como subencargados del tratamiento, según corresponda, con respecto a los Servicios de Responsable a Encargado del tratamiento pertinentes:

| Subcarga del tratamiento | Contenido del tratamiento | Naturaleza del tratamiento | Categorías de Interesados | Categorías de datos personales tratados | Duración del tratamiento |
|---------------------------------|--|-----------------------------------|----------------------------------|--|---------------------------------|
| Amazon Web Services (AWS) | Alojamiento (centro de datos en Irlanda) | Alojamiento | Ver arriba | Ver arriba | Vigencia del Acuerdo |



| | | | | | |
|----------|--|---|-----------------------|-----------------------------------|----------------------|
| Sendgrid | Envío de correos electrónicos a clientes (EE. UU.) | Usar datos de contacto para enviar correos electrónicos | Empleados del cliente | Direcciones de correo electrónico | Vigencia del Acuerdo |
|----------|--|---|-----------------------|-----------------------------------|----------------------|

Apéndice 2 - Anexo de seguridad de Criteo

Este anexo de seguridad (el “Anexo”) representa controles de seguridad relativos a los Servicio de Criteo y a la gobernanza de seguridad general.

Este Anexo es complementario a los términos entre Criteo y el Cliente y forma parte del Acuerdo. En caso de contradicción entre el Acuerdo y este Anexo, este Anexo prevalecerá.

1. Definiciones

Las siguientes definiciones son aplicables al presente Anexo:

Información confidencial: se refiere, específicamente en el contexto de este Anexo, al proceso de información del Cliente y Criteo, almacenada y transmitida por las plataformas de servicio de Criteo y los activos de datos relacionados y los controles de seguridad de apoyo aplicados para proteger la seguridad de los datos.

Activos de datos: se refiere a cualquier plataforma tecnológica, componente, dato o información procesada a través de plataformas de productos de servicio de Criteo que traten, transmitan o almacenen Información confidencial.

Violación de la seguridad de los Datos personales: se refiere a una infracción de la seguridad que conduce a la destrucción, pérdida, alteración, divulgación no autorizada o acceso accidental o ilícito a Datos personales transmitidos, almacenados o tratados, en general.

Incumplimiento de la seguridad: se refiere a cualquier acceso o uso, divulgación, alteración o destrucción no autorizados, reales o potenciales, de la Información confidencial, o cualquier acto u omisión que comprometa los datos relevantes para los servicios contractuales relacionados con la protección de la seguridad, confidencialidad o integridad de la Información confidencial.

2. Controles de seguridad

Criteo mantiene y tiene sistemas compatibles con los siguientes controles de seguridad y privacidad relacionados con los servicios de Criteo:

Gestión y gobernanza de la seguridad: Criteo mantendrá un Sistema de gestión de la seguridad similar a la ISO 27002, que incluirá otras prácticas recomendadas de privacidad y seguridad conocidas en el sector y respaldará los controles de seguridad. Eso incluirá la documentación adecuada (políticas de seguridad, procesos, directrices, estándares, estándares de configuración y controles de seguridad asociados) para garantizar una protección adecuada de los activos de datos de Criteo y del Cliente durante todo el ciclo de vida del Servicio de Criteo.

Evaluaciones de seguridad: No más de una vez por año natural y solo tras la recepción de una solicitud por escrito con un aviso no inferior a treinta (45) días hábiles de antelación, se permitirá al Cliente realizar evaluaciones de seguridad en el Sistema de gestión de seguridad de Criteo y controles de seguridad asociados directamente a los servicios prestados como Encargado del tratamiento. Las Evaluaciones de seguridad se limitarán a cuestionarios de seguridad detallados generales, consultas o preguntas específicas relacionadas con los servicios contratados y excluir auditorías físicas, pruebas de penetración, exploraciones u otras



actividades intrusivas. Las Evaluaciones de seguridad deben ser realizadas preferentemente por un auditor externo, que estará sujeto a confidencialidad y someterá su informe para su validación a Criteo antes de que se proporcionen los resultados finales al Cliente. Dichas solicitudes se respaldarán de inmediato proporcionando acceso a los controles de seguridad de Criteo aplicados para proteger los activos de datos de Criteo y del Cliente contra amenazas, riesgos y vulnerabilidades de seguridad, con respuestas proporcionadas dentro de plazos razonables y representadas con precisión.

Garantía de seguridad de terceros: Criteo mantendrá controles de garantía de seguridad adecuados para gestionar los riesgos de seguridad de los datos para servicios de terceros con el fin de garantizar la protección de los activos de datos de Criteo y del Cliente.

Formación en seguridad: Criteo mantendrá programas adecuados de concienciación sobre seguridad y privacidad para proteger proactivamente los activos de datos de Criteo y del Cliente con contenido alineado con las mejores prácticas del sector para mitigar los riesgos para la seguridad de los datos.

Controles de seguridad física y medioambiental: Criteo mantendrá controles de seguridad físicos y medioambientales adecuados para proteger contra los riesgos de seguridad de los datos, y proteger contra los riesgos de confidencialidad, integridad y disponibilidad. Todos estos controles estarán alineados con las mejores prácticas aplicables del sector, operativas y de seguridad para proteger contra el riesgo de seguridad física y ambiental, incluidos los controles de acceso físico, la supervisión de seguridad física y las protecciones ambientales contra interrupciones de energía, riesgos de incendio y riesgos operativos relacionados.

Control de acceso: Criteo mantendrá un sistema integral de gestión de control de acceso alineado con las mejores prácticas del sector para proteger los activos de datos de Criteo y de clientes con la gobernanza adecuada para el acceso, garantizando controles adecuados para la autorización y autenticación, basados en el principio del menos privilegiado. Estos controles incluirán la identificación de cuentas de privilegios con autenticación multifactor (multifactor authentication, MFA) adecuada aplicada a los permisos con acceso a la Información confidencial de seguridad. Todas las cuentas autorizadas, generales o administrativas, tendrán registros de acceso recopilados, supervisados, con permisos revisados periódicamente.

Sistema de gestión de continuidad del negocio (Business Continuity Management, BCM): Criteo mantendrá un Sistema de gestión de continuidad del negocio (Business Continuity Management, "BCM") que detallará los controles de continuidad, funciones, responsabilidades y medidas de recuperación para mantener los requisitos de disponibilidad del Servicio contratado en respuesta a un amplio espectro de posibles desastres y riesgos operativos que podrían interrumpir las operaciones y la entrega oportuna de materiales y servicios. Criteo mantendrá un Sistema BCM que incluya intervalos de prueba periódicos para garantizar la eficacia de los controles. Previa solicitud específica por escrito del Cliente, Criteo respaldará las evaluaciones y preguntas razonables relacionadas con la eficacia de los controles de su Sistema BCM.

Seguridad de aplicaciones y software: Criteo mantendrá los procesos adecuados de Desarrollo de Software Seguro (Secure Software Development, "SDL") que garanticen la ejecución efectiva de los controles de lanzamiento, cambio y configuración y que se mantengan los controles de seguridad de las aplicaciones adecuados para proteger los activos de datos de la empresa y del cliente. Eso incluirá el mantenimiento de versiones y componentes de software en los niveles adecuados para garantizar una protección adecuada.

Seguridad del dispositivo: Criteo mantendrá la seguridad adecuada del dispositivo para sus empleados, que incluye supervisión, detección y respuesta de seguridad las 24 horas todos los días del año a través de la protección de terminales EDR y las líneas base de configuración aplicadas.

Seguridad de la red: Criteo mantendrá controles de seguridad de red adecuados para proteger contra la interrupción de la disponibilidad del Servicio o un incumplimiento de la seguridad. Esto incluirá la supervisión de incidentes de seguridad y la respuesta de detección las 24 horas todos los días del año, y la aplicación de las mejores prácticas de seguridad, incluida la segmentación y el análisis de vulnerabilidades.

Cifrado: Criteo mantendrá cifrados y protocolos adecuados para proteger los datos en tránsito, con el cifrado adecuado o controles equivalentes aplicados si se necesita que los activos de datos se transfieran a través de medios externos si se solicita.



Informe de incumplimientos de seguridad: Criteo notificará al Cliente cualquier Incumplimiento de la seguridad de la Información confidencial de seguridad (incluidos Datos personales), en un plazo de 72 horas. Criteo, a su cargo, mitigará, investigará y proporcionará datos e información relevantes adecuados en un informe de incidentes de seguridad, detallando los datos afectados y la información relacionada necesaria si se detecta un incumplimiento de la seguridad afecta a la Información confidencial.

Gestión de incidentes de seguridad: Criteo mantendrá capacidades de detección y respuesta de seguridad las 24 horas todos los días del año para garantizar una detección y respuesta adecuadas a los riesgos de seguridad de datos reales y potenciales para los activos de datos de Criteo. Estos controles de gestión de incidentes de seguridad serán operados y mantenidos por un equipo de seguridad específico.

Gestión de vulnerabilidades: Criteo mantendrá y operará un sistema integral de gestión de vulnerabilidades con controles adecuados alineados con las mejores prácticas y estándares del sector. Estos controles incluyen análisis de vulnerabilidades en plataformas de entornos de producción, con informes, consideraciones y mitigación de vulnerabilidades detectadas adecuadamente gestionadas. Tales análisis se aplicarán interna y externamente.