RGPD: Reglamento General de Protección de Datos Una evolución, no una revolución

Renuncia de responsabilidades
Este artículo no constituye ningún tipo de asesoramiento jurídico, ni la información en él contenida está pensada para reproducir la relación de un abogado-cliente. Solicita asesoramiento legal profesional si fuera necesario.

Introducción

El RGPD (Reglamento General de Protección de Datos) europeo sustituye a la Directiva de protección de datos de 1995 y unifica las diversas leyes de privacidad de datos vigentes en los 28 estados miembros.

Desde la fundación de la empresa en Europa en 2005, Criteo tiene un sólido historial a la hora de garantizar que nuestra tecnología tiene altos niveles de privacidad y seguridad de datos a la vez que ayudan a nuestros clientes a cumplir con las expectativas de los consumidores sobre anuncios personalizados y relevantes. Como empresa global con oficinas principales en múltiples países de la Unión Europea y que colabora con miles de anunciantes y publishers cuyos clientes y usuarios están basados en la Unión Europea, estamos acostumbrados a tratar con los requisitos nacionales en todo el mundo.

Nuestra visión en Criteo es que la consistencia y la certeza en relación a la privacidad y la protección de datos es una situación en la que todos salen ganando, tanto las empresas como los consumidores de éstas. Por este motivo, Criteo se compromete con el cumplimiento del RGPD y puesto que estamos trabajando con clientes y partners sujetos a las nuevas normativas, también con ofrecerles el apoyo que necesitan y compartir pautas adecuadas para que gestionen la transición de la mejor manera posible. Criteo está lista para afrontar el reto del RGPD y prevé un impacto limitado del nuevo reglamento en la capacidad de nuestros clientes y partners de trabajar con Criteo.

En general, esta actualización del reglamento es una evolución en línea con las políticas de protección de datos en todos los estados miembros de la Unión Europea, además de ofrecer una aplicación consistente por parte de las Autoridades de

protección de datos locales (DPA) en cada uno de los estados miembros europeos. Los objetivos del RGPD son claros:

- Modernizar el sistema legal para proteger los datos personales en una era de globalización e innovación tecnológica.
- Reforzar los derechos de las personas y a la vez reducir las cargas administrativas para garantizar un flujo libre de datos personales en la UE.
- Aportar claridad y coherencia a las normativas de protección de datos personales y garantizar la aplicación consistente y la implementación efectiva en toda la UE.

¿Qué son los datos personales según los define el RGPD?

El RGPD protege la privacidad de los ciudadanos de la UE y atañe a todas las empresas que recopilan o procesan datos personales sobre individuos en la Unión Europea, aún cuando la empresa no esté establecida en la Unión Europea. Una confirmación significativa para el sector del marketing digital es que el RGPD se aplica a cualquier tipo de información relacionada con una persona natural identificada o identificable e incluye identificadores online como ID de cookies e ID de publicidad móvil. Estos identificadores online se mencionan explícitamente en la definición de datos personales, lo que confirma la amplia interpretación de datos personales ya aplicados en las leyes de la UE.

Es importante señalar que estos identificadores online ya eran considerados datos personales por muchos DPA europeos. No se trata pues de un requisito nuevo para Criteo ya que solo recopilamos datos personales no sensibles en forma de cookies. Por lo tanto, estamos muy familiarizados con dichas distinciones y tenemos métodos de cumplimiento bien establecidos a la vez que garantizamos resultados a nuestros clientes.

Hay una serie de preguntas habituales que las empresas se plantean en lo relativo a la gestión de datos. En primer lugar, ¿qué son los «datos personales» según los define el RGPD? Los datos personales son cualquier dato que incluya:

- *Información de identificación directa* como el nombre de la persona, su número de teléfono, etc.
- *Datos seudonimizados o información de identificación no directa*, que no permita la identificación directa de los usuarios pero sí la individualización de comportamientos individuales (por ejemplo para ofrecer el anuncio adecuado al usuario adecuado en el momento adecuado).

El RGPD establece una distinción clara entre información personal de identificación directa y datos seudonimizados. Fomenta el uso de información seudonimizada e indica expresamente que la aplicación de la seudonimización a datos personales puede reducir los riesgos para las personas a las que se refieren y ayudar a los controladores y procesadores a cumplir con sus obligaciones de protección de datos"[1].

[1] *Reglamento General de Protección de Datos – Considerando que (28)*

Los datos que recopila y procesa Criteo para sus clientes y partners no se tratan de datos sensibles tal como se definen en el RGPD. ¿Cómo se definen los «datos sensibles»? Se trata de cualquier dato que revele:

- Origen racial o étnico
- Opiniones políticas
- Creencias religiosas o filosóficas
- Afiliación a sindicatos
- Datos genéticos
- Datos biométricos con el fin de identificar a la persona de manera única
- Datos relativos a la salud o la vida sexual de la persona y/u orientación sexual

Criteo recopila y procesa para sus clientes y partners identificadores online seudonimizados vinculados con eventos de navegación. En su colaboración con Criteo, nuestros clientes y partners solo necesitan acceder a datos seudonimizados que no permiten la identificación directa de los usuarios. Estos datos seudonimizados incluyen:

- ID de cookies
- Direcciones de email encriptadas
- Móvil ID
- Cualquier otro identificador técnico que permita a Criteo señalar un comportamiento individual sin identificar directamente a las personas

¿Cuál es la diferencia entre consentimiento inequívoco y explícito?

El RGPD también establece una clara distinción entre consentimiento inequívoco y explícito de la persona. Aunque ambas formas de consentimiento requieren una acción positiva por parte del individuo, el consentimiento explícito implica una interpretación estricta de lo que constituye esta acción positiva por parte del usuario (p.ej. seleccionar una casilla, hacer clic en un botón «Acepto»). Esto se aplica únicamente a los datos personales sensibles tales como raza, religión, orientación sexual, afiliación política y estado de salud. Y lo que es más importante, los identificadores online únicamente (p.ej. cookies) se categorizan como datos personales no sensibles, por lo tanto, no se requiere un consentimiento de opt-in explícito.

¿Qué significa esto y cómo se aplica a nuestro negocio? El RGPD ofrece seis bases legales para la recopilación de datos y el procesamiento de datos en Europa. Así que si alguien está recopilando datos personales de cualquier tipo, deberá haber una base legal para ello. Las seis bases legales son:

- El interés vital de la persona
- El interés público
- Necesidad contractual
- Cumplimiento con obligaciones legales
- Consentimiento inequívoco válido de la persona
- Interés legítimo del controlador de datos

Es importante tener presente que todas estas seis bases legales *tienen el mismo valor legal, lo que significa que *son independientes y *exclusivas entre sí. Para empresas en la industria del marketing o marketing digital o que recopilan datos con fines de marketing, las dos bases legales que podrían aplicarse son: 1) consentimiento inequívoco de la persona y 2) interés legítimo del controlador de datos.

En Criteo consideramos el consentimiento inequívoco válido como la base más aplicable para nuestros clientes y socios que recopilan datos personales, incluidos identificadores online.

Desde 2009 y con la adopción de la Directiva ePrivacy (más conocida como la directiva de las cookies) se ha exigido el consentimiento para la recopilación de datos para el retargeting mediante cookies. Los clientes y partners publishers de Criteo que no procesan datos sensibles, sino que trabajan con datos relacionados con la navegación web, intención de compra e historial de compra vinculados con los identificadores técnicos seudonimizados ya están acostumbrados a cumplir con dichos requisitos.

Prevemos que las normas sobre el consentimiento inequívoco válido serán una evolución de las leyes ya muy protectoras que existen en Europa. La CNIL (Autoridad francesa de protección de datos y autoridad supervisora de Criteo) ofrece las mismas recomendaciones sobre el consentimiento para recopilar datos por parte de los usuarios[2] y recomienda varias soluciones técnicas fáciles de usar para los administradores de sitios web para garantizar el cumplimiento.

Las condiciones requeridas por el RGPD para el consentimiento inequívoco válido son muy similares si no idénticas a las condiciones ya detalladas por el Grupo de trabajo del Artículo 29 en una opinión pasada[3]:

> ***Información específica:*** *"Para ser válido, el consentimiento debe ser específico y debe estar basado en la información apropiada proporcionada a la persona. En otras palabras, no es válido el consentimiento global sin especificar el propósito exacto del procesamiento de datos.»*

---

[2] *CNIL: "Cookies, cómo garantizar que mi sitio web cumple con la normativa" https://www.cnil.fr/fr/cookies-comment-mettre-mon-site-web-en-conformite*

[3] *Grupo de trabajo del Artículo 29 – 2013 Guía sobre obtener consentimiento para cookies: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp208_en.pdf*

Tiempo: *«Como regla general, el consentimiento debe darse antes de que comience el procesamiento de datos».*

Elección activa*: "El consentimiento debe ser inequívoco. Por lo tanto, el procedimiento de solicitud y aceptación del consentimiento no debe dejar lugar a dudas en cuanto a la intención de la persona interesada. En principio no hay límites con relación a la forma que puede tomar el consentimiento. No obstante, para que el consentimiento sea válido, debe ser una indicación activa de los deseos del usuario. La mínima expresión de una indicación podría ser cualquier tipo de señal, lo suficientemente clara como para poder indicar los deseos de la persona interesada y para ser entendible por el controlador de datos».*

Libremente expresado*: "El consentimiento solo puede ser válido si la persona interesada es capaz de ejercer una elección real y no hay riesgo de engaño, coacción o consecuencias negativas significativas si no da su consentimiento."*

¿Cómo se aplica el «interés legítimo del controlador de datos»?

Para que el interés sea legítimo, la finalidad del procesamiento de datos debe ser la que cabe esperar. El procesamiento de datos personales con fines de marketing directo puede considerarse como realizado en interés legítimo. No obstante, este interés legítimo no puede saltarse los derechos de privacidad fundamentales de los usuarios y se deberán implementar las medidas de seguridad apropiadas para mitigar los riesgos potenciales para la privacidad del usuario.

Los estándares básicos que deben cumplirse antes de tratar de reclamar un interés legítimo son:

- Una explicación de qué datos se están recopilando, la finalidad específica para la que se recopilan dichos datos, así como, cómo afecta a la experiencia online del usuario. Por ejemplo:

  "Nuestro [sitio web/app] utiliza cookies/ ID de publicidad para fines publicitarios. Esto nos permite mostrar nuestros anuncios a los visitantes que están interesados en nuestros productos en los sitios web y apps de nuestros partners. Las tecnologías de retargeting utilizan tus cookies o ID móvil y muestran publicidad en función de tu comportamiento de navegación. Para leer más y/o rechazar sus servicios, consulta sus políticas de privacidad publicadas a continuación». [Añade el enlace a la política de privacidad de tu partner, p.ej. la política de privacidad está en: http://www.criteo.com/es/privacy/]

- Una manera en la que los usuarios puedan controlar su experiencia, incluida una opción de cancelación de recopilación de datos de fácil uso y acceso, con indicaciones claras sobre cómo aquello afectará a la experiencia de navegación.
- Fácil acceso a una política de privacidad, así como información sobre los estándares de privacidad del sector o compromisos que ha adoptado tu empresa. Por ejemplo: Criteo es miembro de la Network Advertising Initiative.

Hay una serie de cuestiones que toda empresa debería poder contestar para poder establecer si hay un interés legítimo:

- ¿Cuál es el propósito de la operación?
- ¿Es necesario cumplir uno o más objetivos concretos de la organización?
- ¿El RGPD u otra legislación identifica específicamente la actividad de procesamiento como una actividad legítima, sujeta a la imparcialidad y resultados positivos?
- ¿Hay alguna otra manera de lograr el objetivo?
- ¿La persona espera que tenga lugar la actividad de procesamiento?
- ¿Cuál es la naturaleza de los datos que se van a procesar? ¿Los datos de esta naturaleza tienen alguna protección especial en el marco del RGPD?
- ¿El procesamiento limitaría o minaría los derechos de las personas?
- ¿Se da un aviso de procesamiento justo a la persona? Si es así, ¿cómo? ¿Son lo suficientemente claros y directos en relación al objetivo de proceso?

¿Cuál es el enfoque de Criteo con relación a la privacidad de datos?

En Criteo la privacidad es nuestro eje principal. Adoptamos importantes medidas para proteger y procesar los datos en cumplimiento con las Leyes de protección de datos y privacidad. Esto incluye el RGPD.

Nuestros equipos de producto desarrollan cada funcionalidad con la privacidad en mente; es el pilar del Privacy by Design, un enfoque sofisticado que garantiza un nivel de seguridad líder en el sector para marketers y consumidores por igual.

Privacy by Design es una práctica instaurada en Criteo y un compromiso para garantizar la privacidad, seguridad y protección en el sector para los consumidores y marketers. Los principales elementos son:

- Tal como requiere el RGPD, en 2013 designamos un Delegado de privacidad de datos, junto con un equipo de expertos en privacidad.
- Estos expertos son parte de la organización de Producto e I+D. Realizan evaluaciones continuas sobre el impacto en la privacidad para supervisar posibles riesgos durante el ciclo de vida de los productos y mitigarlos de manera proactiva.
- El equipo de Privacidad de datos ofrece formación sobre privacidad en toda la compañía, vela por el cumplimiento de los códigos de conducta y es íntegro para garantizar que creamos los mejores productos y servicios.
- Habitualmente revisamos y documentamos nuestras políticas internas, modificamos políticas de privacidad ya existentes si fuera necesario y velamos por el cumplimiento de estas políticas entre nuestros partners y proveedores.

Estrictas medidas para la seguridad de los datos

Tal como requiere el RGPD, Criteo ya mantiene en vigor estrictas medidas de seguridad cuando recopila datos sobre consumidores de nuestros clientes. Utilizamos modernos métodos seudonimizados, incluidos procesos de doble encriptación MD5 y SHA-256, que pueden considerarse pautas a seguir en el marco del RGPD, y nunca almacenamos voluntariamente ninguna información personal de identificación directa sobre consumidores individuales. Para garantizar el cumplimiento y un rendimiento óptimo, almacenamos datos sobre consumidores europeos en el centro de datos europeo más próximo a ellos.

Ad Choices: Centrados en el control y los derechos de los consumidores

Criteo es consciente desde hace tiempo de la necesidad de equilibrar las experiencias de publicidad relevantes con las expectativas de privacidad, además de permitir a los consumidores controlar su experiencia. Los consumidores entienden que se trata de un intercambio. Por este motivo Criteo se comprometió con el programa Ad Choices ya en 2008 para permitir a los consumidores, con un solo clic, ver exactamente dónde está Criteo utilizando los datos y cómo proteger su privacidad. Cuando un consumidor decide desactivar la publicidad (opt-out), detenemos inmediatamente el seguimiento y el retargeting. Eliminamos todos los identificadores de sus navegadores, lo que nos impide dirigirnos a ellos en el futuro. Según las normativas de protección de datos europeas, los datos recopilados sobre los consumidores solo pueden conservarse durante 13 meses.

Líderes en el sector: Inversión en normativas y certificaciones

Criteo tiene un amplio número de certificaciones en vigor que son revisadas anualmente por organismos estándar y gubernamentales, entre ellas:

- Estándares de la «Network Advertising Initiative»
- IAB Europe
- Principios autorreguladores de la Alianza europea para la ética en la publicidad para la publicidad online basada en comportamiento
- Principios autorreguladores de la Alianza europea para la ética en la publicidad digital
- Principios autorreguladores de la Alianza canadiense para la ética en la publicidad digital
- Certificación para recopilación de datos de confianza de TrustArc

¿Cuáles son tus responsabilidades?

El RGPD exige que las compañías de la Unión Europea que recopilan datos, que cumplan con las nuevas normativas sobre protección y seguridad de datos. Esto también afecta a empresas mundiales con sede fuera de la UE si se dirigen a una

audiencia europea. El RGPD es beneficioso para tu negocio ya que aglutina las diversas leyes de privacidad de datos vigentes en los 28 estados miembros europeos. En este sentido, Criteo está ayudando a nuestros clientes y partners a asegurarse de que saben los pasos que deben dar para garantizar el cumplimiento con el RGPD. A continuación, compartimos contigo una serie de pautas que debes tener en cuenta en el proceso de cumplimiento:

Designa un Delegado de Protección de Datos (DPD)

El RGPD requiere la designación de un Delegado de Protección de Datos (DPD) en el caso de que:

- el procesamiento sea realizado por una autoridad u organismo público, a excepción de los juzgados que actúen en calidad de órgano jurisdiccional;
- las principales actividades del responsable del tratamiento consisten en operaciones de procesamiento que, debido a su naturaleza, su alcance y/o su finalidad, requieran una supervisión de datos periódica y sistemática de los temas relativos a datos a gran escala; o
- las actividades clave del responsable consisten en el procesamiento a gran escala de datos sensibles (datos que revelan el origen racial o étnico, opiniones políticas, creencias religiosas o filosóficas, condiciones de salud u orientación sexual, etc.) o datos personales relacionadas con infracciones y condenas penales.

Este delegado supervisará y gestionará los datos y las operaciones exigidas por las normativas. Además, el DPD debe probar que no existen conflictos de interés en términos de protección de datos para tu organización.

Asegúrate de que tu DPD está dispuesto a colaborar

Tus empleados son tu mejor apuesta para ayudarte a entender qué puede estar faltándole a las políticas de protección de datos actuales de tu compañía. Asegúrate de que el DPD y los equipos de IT, Legal y de Compliance conocen a la perfección las prácticas de datos de la compañía. Deberán trabajar juntos para crear un proceso que cumpla con los requisitos exigidos con relación a la recopilación de datos en tu organización.

Ofrece transparencia y control

La información y el lenguaje utilizado en los consentimientos que ofrezcas a los clientes deben ser lo más claros y transparentes posible. Tu sitio web debe dejar de manera explícita, clara y exacta lo que los clientes están aceptando o no, y, en concreto, qué tipos de datos te están proporcionando. Este es un punto clave para el cumplimiento del RGPD.

Prioriza el control de los datos

Debes implementar un proceso de Evaluación del Impacto sobre la Privacidad para todo el procesamiento que pueda poner en riesgo los derechos de las personas. Además, tu empresa debe poder explicar cómo se están recopilando, usando o

incluso editando los datos personales que recopila y debe tener procesos implantados que permitan a los ciudadanos de la UE suministrar, revisar y/o rechazar fácilmente dichos datos. El RGPD indica que es obligatorio garantizar que la infraestructura de datos de tu compañía mantenga registro de actividades de procesamiento y ofrezca visibilidad en el cumplimiento de tus prácticas.

Supervisa el acceso de los empleados y personal externo a los datos

Debes establecer políticas de autorización de empleados estrictas que limiten el acceso a los datos y garanticen la privacidad. Estas políticas deberán actualizarse continuamente para reflejar las necesidades de tu compañía y supervisarse para evitar infracciones, especialmente las relacionadas con las transferencias de datos. Según el Capítulo V del RGPD, las transferencias con destino fuera de la UE deberán cumplir las mismas condiciones de protección y regulación que las organizaciones de la UE.

Los requisitos del RGPD son estrictos y estar completamente preparado para ello exigirá mucho más que marcar casillas en una checklist con los proveedores con los que trabajas. A pesar de todo lo que implica, el RGPD, tal y como nosotros lo vemos, solo puede ser algo bueno tanto para las empresas como para los consumidores, ya que ofrece consistencia y certeza en la privacidad y protección de datos.

¿Cómo afecta el RGPD a las soluciones de Criteo?

En la base de nuestra tecnología está el Criteo Shopper Graph, que recopila los datos de comportamiento de compra recopilados del Criteo Commerce Marketing Ecosystem y suministra información a todas nuestras soluciones de Commerce Marketing.

Criteo Shopper Graph se desglosa en tres conjuntos de datos de confianza, que combinan tres tipos de datos clave sobre los consumidores:

- Identificadores técnicos seudonimizados
- Intereses según el producto y servicios de nuestros clientes
- Estadísticas de medición sobre la performance de nuestros servicios

Garantizamos que la recopilación de estos datos se limita a lo que es estrictamente necesario para nuestros servicios con el fin de ofrecer la información relevante a los compradores sobre los productos que desean en el lugar adecuado, en el momento adecuado y con los mensajes adecuados. Por ejemplo:

- Criteo utiliza sólidos algoritmos de encriptación de datos para garantizar que en nuestros sistemas no se guarda información de identificación directa.
- Nunca almacenamos ningún dato durante más tiempo del estrictamente necesario y respetamos las recomendaciones de las Autoridades de protección de datos de la UE sobre cookies y publicidad digital.

- Ofrecemos mecanismos de elección fáciles de usar: todos los productos de Criteo tienen el mismo sencillo proceso de opt-out accesible en todos nuestros anuncios y políticas de privacidad. También somos miembro registrado en las plataformas de opt-out NAI, DAA e IAB Europe que permiten al consumidor cancelar la publicidad personalizada.
- Los consumidores pueden fácilmente cancelar el servicio de Criteo haciendo clic en el link de Ad Choices del anuncio e informarse sobre por qué están viendo el anuncio. Una vez que un usuario decide cancelar los servicios de Criteo, toda la información recopilada se borrará o no se podrá recuperar, incluidos los datos del usuario que has conseguido como parte de una campaña de Criteo.

Conclusión

En un momento en el que las empresas del sector del marketing digital están actualizando sus prácticas para garantizar el cumplimiento del RGPD, es importante recordar que los ciudadanos europeos conocen bien la publicidad dirigida, conocen los identificadores que permiten realizarla y esperan ver anuncios relevantes. Criteo se asoció con IPSOS[4] para llevar a cabo una encuesta con el fin de saber cuáles son las expectativas de los usuarios europeos y cuál es su relación con la publicidad online personalizada. En la encuesta participaron 3.000 usuarios de Internet, con edades comprendidas entre los 16 y 65 años en Francia, Reino Unido y España, con el fin de establecer una muestra demográfica representativa de diferentes sexos, edades, regiones y niveles de ingresos.

Los arrojados por la encuesta son:

- 90% de los usuarios de Internet conocen lo que es el retargeting
- 68% saben que las cookies permiten realizar la publicidad personalizada
- 75% espera que se le muestren anuncios acorde a sus intereses
- 73% prefiere ver anuncios relevantes en lugar de pagar por una cuota adicional para evitar ver los anuncios

Criteo considera que proteger la privacidad de los consumidores y ser claro y transparente sobre las prácticas empresariales es de vital importancia para todos. Cuando los consumidores entienden exactamente cómo se está utilizando su información y tienen control sobre sus datos de navegación personales, esto fortalece su confianza y lealtad a una compañía.

Somos conscientes y estamos preparados para las implicaciones del RGPD y deseamos ayudar a nuestros clientes y partners a conocer mejor cómo funcionan nuestros productos y servicios. Si trabajamos juntos en comprender y prepararnos para las normativas, podremos seguir disfrutando, como hasta ahora, de nuestra relación de negocio.

---

[4] *Estudio Criteo-IPSOS, 2017*