DMP´s y la privacidad de datos

qualifio

Contenido

Introducción

¿Qué es una **Plataforma de gestión de datos (DMP)**? ¿Por qué las empresas recurren a ellas? ¿Son compatibles con el **Reglamento General de Protección de Datos (RGPD)** y la propuesta para un **Reglamento de Privacidad Electrónica**? Estas son grandes cuestiones que ocupan buena parte del tiempo y la energía de marcas, agencias y editoriales...

Plataformas de gestión de datos

Las Plataformas de gestión de datos (DMP) son plataformas que permiten a las empresas recoger, centralizar y organizar grandes cantidades de datos sobre clientes y clientes potenciales.

El objetivo principal de un DMP es **segmentar el público** objetivo (por ejemplo, hombres deportistas de entre 25 y 40 años que residan en la zona de Logroño) a través de la clasificación de los datos recabados de distintas fuentes. Estas pueden ser el historial de navegación de un usuario, las compras que realiza o su participación en un concurso o una encuesta.

Estas distintas fuentes de datos y su clasificación posibilitan enriquecer los datos que ya posee la empresa para facilitar las campañas de marketing diferenciadas. Además, los DMP´s tienen otros usos, como sustentar las decisiones sobre productos o la creación de contenidos personalizados o alimentar las herramientas de inteligencia de negocio.

FIRST PARTY DATA

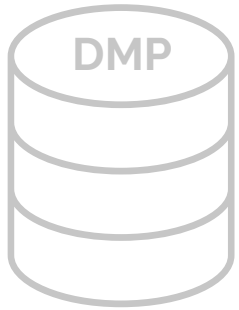
que pertenecen a la empresa. Estos datos han sido recabados por la propia empresa (a través de su CRM, sistema de incorporación de datos al CRM o *cookies*).

SECOND PARTY DATA

facilitados por los socios de la empresa.

THIRD PARTY DATA

recabados a través de terceros (empresas que han obtenido datos sobre todo a través de *cookies* o tecnologías de rastreo que afinan la segmentación existente).



DMP y datos personales

En general, los DMP´s clásicos no procesan datos personales a no ser que éstos se hayan enmascarado o pasado por un algoritmo *hash* antes de convertirse en un punto de datos en la plataforma. Es decir, antes del proceso de incorporación (*onboarding*) los datos personales pasan por un proceso previo de anonimización o pseudo anonimización.

A continuación, a los datos «enmascarados» **se les asigna una «ID»** que se sincroniza con otras fuentes de datos para formar un identificador único que amalgama las distintas fuentes de datos de la plataforma.

Las unidades típicas de estas ID y de su capacidad de sincronizarse entre sí son las *cookies* y los píxeles de seguimiento.

Entre las DMP más conocidas del mercado

salesforce DMP

ORACLE bluekai

CXENSE

Adobe Audience Manager

PERMUTIVE

LOTAME™

mediarithmics

weborama

Los DMP´s a la luz del RGPD y los reglamentos de privacidad electrónica [1]

Entonces, ¿el RGPD es de aplicación a los DMP?

No es una cuestión baladí, ya que afecta a la capacidad de identificar a una persona física y esto implica tener que entender cómo se enmascaran los datos personales a través de las cookies y si existe la posibilidad de que se puedan «desenmascarar» en algún momento.

La única referencia a las cookies en el RGPD se encuentra en el considerando 30. El considerando 30 reza *'Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de Internet, identificadores de sesión en forma de «cookies» u otros identificadores, como etiquetas de identificación por radiofrecuencia.'*

> **"Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas."**

Es decir, por desgracia, no es fácil llegar a una conclusión.

En la práctica, dependerá de las medidas para proteger la privacidad de los datos, las medidas de seguridad puestas en marcha y, en último término, las posibles conexiones que se pueden hacer entre los datos y las personas físicas.

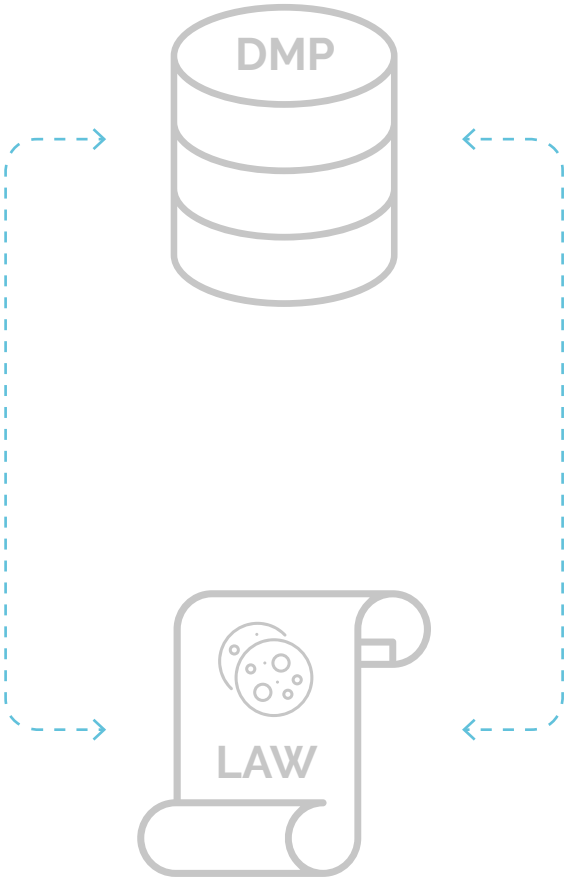
Si, por ejemplo, es posible realizar una conexión a través de una combinación e información (recordando que las direcciones de IP se consideran datos personales[2]) e identificar a una persona física en base a la información incluida en el DMP, la respuesta a esta cuestión debería ser que por supuesto el RGPD es de aplicación.

¿Y el Reglamento de Privacidad Electrónica?

En la medida que los DMPs se alimentan de información obtenida de *cookies* y otras tecnologías de rastreo, todo de terceros, la ley del 13 de junio de 2005 sobre comunicaciones electrónicas deberá ser de aplicación. Esta ley transpone la Directiva de Privacidad Electrónica, que está próxima a revisarse mediante la adopción de un reglamento.

Desde que se ha establecido que el RGPD y la Directiva de Privacidad Electrónica son de aplicación a estas herramientas (al menos para algunos DMP), es necesario considerar la cuestión de qué fundamentación legal existe para el tratamiento de dichos datos personales.

De conformidad con el RGPD, para que el tratamiento de datos sea legal, debe ajustarse al artículo 6.



Base para un tratamiento de datos ajustado a la ley

Dado que cada tipo de datos incluidos en una DMP proviene de una fuente distinta, es necesario establecer la base legal, que, en nuestra opinión, podría permitir el tratamiento de estos datos personales.

En relación a los first party data

Los first party data son cualesquiera datos recogidos mediante instrumentos (en línea o no) que son propiedad y están operados por una marca o editorial.

Por lo tanto, de cara al RGPD, una empresa puede basar su tratamiento de datos personales en uno de los tres fundamentos legales para dicho procesamiento[3]: el consentimiento del titular de los datos, la necesidad a la vista de un interés legítimo de la empresa o necesidad para actuar de conformidad a un contrato. Una de estas tres bases legales podría constituir la base del tratamiento de datos personales con vista a la función de un DMP.

Respecto al borrador actual del Reglamento de Privacidad Electrónica, podrían aducirse dos fundamentos para justificar que la sociedad realice el tratamiento de los datos recabados. En particular, a través de las cookies propias, el consentimiento del usuario final o en base al Artículo 8 de la propuesta de reglamento, que establece que si *«cuando sean necesarios para la prestación de un servicio (...) solicitado por el usuario final»*.

La justificación para la fundamentación legal para tratar estos *first party data* se refiere en último término al responsable del tratamiento en virtud del RGPD. El responsable del tratamiento deberá ser capaz de demostrar que existe bien consentimiento, bien necesidad en relación al cumplimiento de un contrato o la prestación de un servicio, o, finalmente, bien proporcionalidad entre sus intereses legítimos y el respeto a la privacidad de las personas afectadas.

PROCESO DE INCORPORACIÓN (ONBOARDING) DE DATOS CRM EN UN DMP

El proceso de incorporación (*onboarding*) de datos CRM en un DMP consiste en crear un enlace entre la información que tiene una sociedad en su plataforma CRM y la información incluida en un DMP. Este enlace es posible mediante la asociación de información incluida en el CRM con un identificador a través de una cookie. Esta *cookie* se utiliza para asociar la información que contiene el CRM y también para trocear (*«hash»*) o enmascarar datos personales del CRM antes de introducirlos en el DMP.

En relación a los second party data

Second party data se reciben a través de partners de negocio y se integran en el DMP. En este proceso, cada uno de los protagonistas debe verificar que cumple con sus obligaciones. Solo entonces, el procesamiento final (es decir la integración de los datos en el DMP) será válido y legal.

DATOS RECOGIDOS DE INDIVIDUOS

Los socios comerciales recogen datos y los envían a otra empresa

La empresa recibe los second party data

ESTOS SE INTEGRAN EN EL DMP

FUNDAMENTO LEGAL PARA QUE UNA EMPRESA RECOJA LOS DATOS

En relación al objeto de una transferencia a una empresa externa, la única posibilidad será, en nuestra opinión, basar la transferencia en el fundamento del consentimiento o la realización de un contrato (que en este caso sería, el contrato de compraventa de datos).

De hecho, como sabemos, el RGPD obliga a facilitar al titular de los datos información exhaustiva, clara, transparente y fácilmente accesible sobre los datos recabados y el objeto para el cual se procesarán.

Con la excepción del contrato de compraventa de datos (a través del cual se informará al titular de datos de la transferencia) creemos que, a este respecto, la base legal para asegurar el mayor nivel posible de transparencia y adherencia a los requisitos del RGPD, así como a la propuesta de Reglamento de Privacidad Electrónica, es el fundamento legal del consentimiento.

Merece la pena recordar que las «condiciones del consentimiento» que la propuesta de Reglamento de Privacidad Electrónica establece para este contexto serán idénticas a las establecidas en el RGPD[4].

INFORMACIÓN SOBRE LAS OPERACIONES DE TRATAMIENTO EN EL DMP EN VIRTUD DEL RGPD

La empresa que recibe los datos personales no los ha recabado *de facto* ella misma. Por lo tanto, en virtud del Artículo 14 del RGPD, los titulares de los datos deberán ser informados de dicho tratamiento.

Esta información deberá estar disponible en un documento específico[5] que aborde la protección de la privacidad: una política de privacidad.

Por lo tanto, se deberá informar a la persona afectada de que la sociedad recibe y procesa datos de socios externos de conformidad con los requisitos del artículo 14.

Además, en relación al deber de información y transparencia durante el tratamiento, el Grupo 29[6] establece que :

> **“la obligación de facilitar información debe garantizar que el titular de los datos puede esperar razonablemente que sus datos, en el momento y el contexto en el que se recabaron, se sometieron a un proceso de tratamiento concreto. En otras palabras, el objeto del tratamiento de los datos no debería ser una sorpresa para el titular de este.”**[7]

La empresa, en tanto que responsable del tratamiento, también será responsable de asegurarse de la validez del fundamento legal esgrimido por el socio que recaba y transfiere datos personales en su nombre y representación.

Integración de second party data en el DMP

La integración de tecnologías de terceros en un DMP implica una subcontratación o una responsabilidad mancomunada sobre el tratamiento de datos[8]; en ese caso, las operaciones de tratamiento deberían regirse por «*un contrato u otro acto jurídico regido por la ley de la Unión o de un Estado miembro*».[9]

En la práctica, estos contratos o actos legales adoptan la forma de Acuerdos de Tratamiento de Datos (*Data Processing Agreement* o DPA) o Acuerdos de Responsabilidad Conjunta (*Joint Controllers Agreement* o JCA) firmado por las distintas entidades implicadas[1].

En relación a los third party data

Los *third party data* son cualesquiera datos adquirido a través de plataformas de terceros o fuera de los instrumentos (en línea o no) que son propiedad y están operados por una marca o editorial.

Hay que recordar que, para este tipo de datos, solo los datos que identifican o hacen identificable a una persona física son objeto del ámbito de aplicación del RGPD.

Además, dado que la mayor parte de estos datos se adquieren a través de *cookies*, será necesario comprobar que se han obtenido legalmente de conformidad con el actual borrador de Reglamento de Privacidad Electrónica.

En general, el proveedor del DMP integrará *third party data* para alimentar o ampliar el *first party data* o *second party data* y para permitir una segmentación más escalable de las personas implicadas.

Igual que con los *second party data*, la empresa que utilice el DMP deberá asegurarse que su tratamiento de los datos se ajusta a la ley.

[1]Esta noción de corresponsabilidad podrá tener una función más importante si el Tribunal Europeo de Justicia siguiera el consejo de su Abogado General en el caso **Fashion ID**.

Caso de estudio

1

FIRST PARTY DATA

Yolanda compra ropa a tienda de la empresa MAS, que vende todo tipo de prendas además de protección solar. En ocasiones anteriores, Yolanda había utilizado el sitio web de MAS para comprar protección solar (con un índice de protección de entre 30 y 50 SPF). Al comprar en la tienda física, se suscribe a la *newsletter* de MAS dejando su dirección de correo electrónico (yola@gmail.com) y aceptando el tratamiento de sus datos personales

2

SECOND PARTY DATA

MAS tiene un socio, una empresa llamada Birthdaytop, que se dedica a la organización de eventos y, para el 35 cumpleaños de una mujer, preparó una fiesta en un club de solteros; esta mujer confirmó el evento a través de la misma dirección de correo electrónico que había facilitado a MAS unos días antes a través de su *app* (disponible en Android).

3

THIRD PARTY DATA

Yolanda está buscando en Internet, desde su portátil, cruceros para solteros en el Caribe, y llega a la página web www.caraibestropcool.com. Una vez más, esta deja una serie de *cookies* y píxeles en su portátil.

Caso de estudio

4

MAS incorpora los datos a su CRM (onboarding), pide a Birthdaytop que le transfiera los datos de mujeres solteras (o probablemente solteras) que tiene en su base de datos y compra datos a www.caraibestropcool.com para tener información sobre las nuevas tendencias en salidas hacia el Caribe para mejorar su oferta en ropa de baño.

5

MAS integra y anonimiza los datos que están en su poder, recibidos y adquiridos a www.caraibestropcool.com, y los sincroniza con un DMP.

6

Durante el proceso de sincronización, se crea un identificador único (AABR0976). Corresponde a una mujer de entre 25 y 35 años, soltera, a la que le gusta viajar y que necesita un nivel de protección solar alto. En base a este identificador, MAS podrá personalizar las ofertas comerciales que proponga a Yolanda.

Caso de estudio

El consentimiento para procesar los datos de Yolanda probablemente se fundamente en la información que dio al realizar una compra en la tienda física. MAS recabó esta información directamente de Yolanda. Además, Yolanda había comprado protección solar a través de la página web de MAS: Es decir, mediante la integración de datos (*onboarding*), MAS puede integrar información recabada tanto en su tienda física como en su página web.

Los datos de la edad y la fecha de cumpleaños de Yolanda no estaban incluidos en la *first party data*. Por lo tanto, MAS, antes de incorporar estos datos, debería obtener el consentimiento explícito de Yolanda como fundamentación legal para el tratamiento de datos personales.

En el ejemplo anterior, la información de que a Yolanda le gusta viajar podría obtenerse a través de cookies. Por lo tanto, es necesario comprobar que esta información se ha obtenido de forma legal de conformidad con la ley del 13 de junio de 2005.

A MAS, en tanto que responsable del tratamiento, le corresponderá demostrar que el tratamiento del perfil que ha creado, que, en el ejemplo anterior, contiene muchos puntos de datos personales (identificación, datos financieros, identificación electrónica, etc.) está basado en el consentimiento otorgado en virtud del RGPD.

Conclusión

Dado el enorme volumen y diversidad de los datos que procesa, incluyendo la incorporación (*onboarding*) y enmascaramiento de datos personales, los **DMP' s no están exentas de los requisitos y del alcance del RGPD**, ni de los de la Directiva de Privacidad Electrónica.

La verdadera complicación de usar una DMP en este momento seá evaluar y garantiza el consentimiento de conformidad con los requisitos que el RGPD establece para el responsable de datos. Esto no es baladí, teniendo en cuenta la posible variedad de actores y fuentes de datos implicadas en un DMP:

No obstante, aunque la principal responsabilidad corresponde al responsable del tratamiento, tanto el responsable como el encargado del tratamiento deberán asegurar la validez legal del consentimiento si quieren evitar sanciones graves, que han sido objeto de debate desde el 25 de mayo de 2018.

Sobre los autores

Frédéric Dechamps está colegiado en el Colegio de Abogados de Bruselas como abogado ejerciente ante los Tribunales desde 1997, además de miembro de la Comisión de Nuevas Tecnologías del Colegio de Abogados de Bruselas..

Participa habitualmente en conferencias y simposios sobre sus temas predilectos:

- derecho mercantil (prácticas comerciales, derecho societario, etc.);
- propiedad intelectual (derechos de copia (copyright), derechos de marca, etc.);
- nuevas tecnologías.

Frédéric también es responsable de la gestión de contratos de **Lawbox**.

Nathan Vanhelleputte está colegiado en el Colegio de Abogados de Bruselas como abogado ejerciente ante los Tribunales desde 2018.

Después de dos años trabajado para la empresa de seguros AIG; abandonó esta empresa estadounidense para colaborar en la creación de una firma de consultora especializada en cuestiones de regulación y cumplimiento.

Tras esta experiencia, decidió integrarse en **Lex4u** para trabajar en el ámbito del derecho mercantil, derecho contractual, derecho de protección de datos personales y derecho de las nuevas tecnologías.

Nathan es un delegado de protección de datos (*Data Protection Officer* o DPO) titulado por la Solvay Brussels School.

qualifio

Sobre Qualifio

Qualifio es el SaaS líder en Europa en marketing interactivo y recopilación de datos. Te permite crear y publicar fácilmente contenidos interactivos (cuestionarios, tests de personalidad, encuestas y más de 50 formatos innovadores) en todos tus canales y recopilar datos de tu audiencia para poder cualificar, segmentar y monetizarla.

¿Cómo funciona?

CREAR

Elige tu campaña interactiva entre más de 50 formatos, totalmente personalizables y sin desarrollo extra

PUBLICAR

Fácil de publicar en tu página web, aplicaciones móviles y redes sociales

RECOPILAR DATOS

Lanza campañas de recopilación de datos en regla con el RGPD gracias a una serie de funcionalidades especiales.

OBTENER RESULTADOS

Se pueden visualizar y extraer los perfiles generados y los resultados de campañas a tiempo real

SEGMENTAR Y MONETIZAR

Puedes integrar la plataforma a tus herramientas de marketing y datos (CRM, DMP, SSO, Analytics, etc.)

¿Quieres recibir más contenido como esto?

SUSCRÍBETE A NUESTRA NEWSLETTER

¿Necesita más información?

HABLA CON UN EXPERTO

www.qualifio.com

Referencias

[1] La Directiva sobre Privacidad Electrónica llevaba bastante tiempo vigente en Bélgica a través de su transposición a la ley del 13 de junio de 2005 sobre comunicaciones electrónicas. Con el fin de unificar las distintas regulaciones, se trató de adoptar un Reglamento Europeo, previsto para el 25 de mayo de 2018 (Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre el respeto de la vida privada y la protección de los datos personales en el sector de las comunicaciones electrónicas y por el que se deroga la Directiva 2002/58/CE («Propuesta de Reglamento sobre la Privacidad Electrónica»)).

[2] C.J.E.U (2nd Ch.), *19 de octubre de 2016, P. Breyer c. Bundesrepublik Deutschland* , ***C-582/14***.

[3] Si bien existen seis fundamentaciones que pueden justificar legalmente el tratamiento de datos personales, no nos detendremos en LAS que se refieren al cumplimiento de una obligación legal, a la necesidad de proteger intereses vitales o a la necesidad de realizar una misión de servicio público, dado que serán las que se presenten con menos frecuencia en el contexto de una empresa privada.

[4] Artículo 9 de la Propuesta para un Reglamento sobre la Privacidad Electrónica.

[5] En este sentido, la Opinión WP260 del Grupo 29, *Pautas sobre la transparencia de conformidad con el Reglamento 2016/679* pág. 18 punto 33.

[6] Pasó a ser el ***Comité Europeo de Protección de Datos***.

[7] Opinión WP260 del Grupo 29, *Pautas sobre la transparencia de conformidad con el Reglamento 2016/679* pág. 23 punto 45.

[8] Por citar un caso reciente, ver **Sentencia del Tribunal Europeo de Justicia del 10 de juilo de 2018** relativo a los Testigos de Jehová (C-25/17) sobre los criterios para evaluar la condición de subcontratista o gestor conjunto.

[9] Artículo 28(3) del RGPD.