



Las actividades de Marketing y los servicios Cloud, ante el desafío de GDPR

Tras el éxito de los workshops sobre GDPR organizados por AUSAPE en Madrid, Barcelona, Zaragoza y en las diferentes delegaciones, la Asociación ha querido abordar en dos sesiones específicas cómo afectará el nuevo Reglamento General de Protección de Datos a las actividades de Marketing y también a aquellos clientes que opten por Cloud para la prestación de servicios.

Consciente de la inquietud que suscita entre las empresas asociadas la aplicación de la normativa europea a partir del próximo 25 de mayo, AUSAPE ha organizado dos nuevos workshops, uno en Madrid y otro en Barcelona, para abordar cómo impacta la norma en dos ámbitos concretos de la empresa: Marketing y Cloud. Y, como ponentes, ha vuelto a recurrir a los expertos legales de Marzo & Abogados, Ana Marzo y Gonzalo M. Flechoso, especialistas en derecho y nuevas tecnologías que asesoran de forma habitual a la Asociación.

La primera parte de cada una de las sesiones estuvo dedicada al tratamiento de los datos por parte del departamento de Marketing, bloque en el que se trataron temas como la licitud de los tratamientos de marketing (consentimiento, información y derechos), la procedencia de los datos (de terceros, redes sociales, cookies, seguimiento de emails, fuentes accesibles al público), segmentación, perfilados y listas de exclusión, así como las campañas con agencias de publicidad (regulación y responsabilidad).

La segunda parte, que abordó como impacta el GDPR en la contratación de servicios Cloud y el tratamiento de los datos, se centró en las siguientes temáticas: quién es el responsable y quién el encargado del tratamiento; responsabilidades del responsable y del encargado del tratamiento; la elección del prestador del servicio de Cloud; subcontrataciones (el contratista y el prestador); el contrato de servicios en la nube y el contrato de encargo de tratamiento, y las transferencias internacionales, con sus requisitos y responsabilidades.

MARKETING

Actualmente hay una serie de normativas vigentes que protegen al ciudadano como destinatario o receptor de comunicaciones comerciales publicitarias, entre ellas, la Ley de Competencia Desleal, la LGDCU (que regula las comunicaciones comerciales a distancia), la LOPD (la Ley Orgánica de Protección de Datos que aborda en su articulado los tratamientos de datos con fines publicitarios y

de promoción comercial) y la LSSICE (que legisla sobre las comunicaciones comerciales por medios electrónicos que, en caso de colisión, prevalece sobre la LGDCU en algunas materias).

Estas normas establecen derechos de los usuarios a la hora de que se traten sus datos como, por ejemplo, los de identificación del responsable del tratamiento de los datos, consentimiento para tratar los datos o el de oposición. En definitiva, definen la forma en la que se pueden ejercer determinados derechos, o las medidas que deben poner en marcha las empresas para garantizar que se cumplen.

Los expertos de Marzo & Abogados hicieron un repaso exhaustivo de toda esta legislación para ofrecer el contexto en el que España está intentando establecer un marco jurídico a nivel nacional porque, pese a que GDPR es directamente aplicable en todos los Estados miembros y se aplicará con independencia de cualquier norma nacional, se hace necesaria una adaptación legislativa mediante la derogación y modificación de las leyes existentes, concretamente de la LOPD, que será sustituida previsiblemente por el Proyecto de Ley Orgánica de Protección de Datos (PLOPD) que, al cierre de esta edición de la revista, está en aprobación en el Parlamento.

EL NUEVO REGLAMENTO Y EL PLOPD

El nuevo Reglamento General de Protección de Datos europeo no hace un gran mención explícita a las actividades de marketing en su articulado que, simplemente, aparecen en varios considerandos, el texto que precede y sirve de apoyo al precepto de una ley. En éstos se dice que el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo, y que si los datos personales se tratan con fines de mercadotecnia directa, el interesado debe tener derecho a oponerse, sin coste al-

guno, a que se traten sus datos personales y a que se elaboren perfiles que vayan a ser utilizados para esa finalidad.

Este derecho de oposición debe comunicarse explícita y claramente al interesado, y al margen de cualquier otra información. Además, cuando se oponga al tratamiento de datos con esta finalidad, éstos tienen que dejar de ser tratados.

En su articulado, el Proyecto de LOPD recuerda que, en cumplimiento de GDPR, los responsables y encargados del tratamiento deberán designar un Delegado de Protección de Datos cuando desarrollen actividades de publicidad y prospección comercial, lleven a cabo tratamientos basados en las preferencias de los interesados o realicen actividades que impliquen la elaboración de perfiles de los mismos.

Respecto a este último punto, GDPR define elaboración de perfiles como toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos a su rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos.

Para poder realizarlos, hay que buscar una base jurídica que haga legítimo el tratamiento, y las empresas tienen el deber de informar al interesado, así como de incluir información sobre la lógica aplicada en los perfilados y las consecuencias previsibles de dicho tratamiento para él.

Por otro lado, el PLOPD contempla que el derecho de supresión del tratamiento de los datos se ejercerá también según lo establecido también en el Reglamento europeo y que, cuando la supresión, se derive del derecho de oposición de esta norma, se podrán conservar los datos identificativos del afectado necesarios con el fin de impedir tratamientos futuros para fines de mercadotecnia directa.

Los ponentes: Ana Marzo, en Barcelona; Gonzalo M. Flechoso, en Madrid...



ANA MARZO

Licenciada en Derecho con formación ampliada que combina los aspectos legal y técnico. Ana es socia-directora de la consultora especializada en tecnologías de la información y comunicación EQUIPO MARZO con una amplia experiencia en propiedad intelectual, protección de datos, administración electrónica, publicidad digital y consultoría y auditoría en

seguridad de la información.

Es autora de numerosas publicaciones y profesora en másters, cursos y seminarios en las citadas áreas. Puedes encontrarla en nuestra sección 'Rincón legal' y en @AnaMarzoP y www.equipomarzo.com

GONZALO M. FLECHOSO

Licenciado en derecho y Auditor Cisa (ISACA), con una larga experiencia en asesoramiento en Tecnologías de la Información y la comunicación, a través de MARZO ASESORES, sobre comercio electrónico, redes sociales, contratación informática, compliance y protección de datos.

Profesor en distintos masters y cursos, y colaborador en publicaciones especializadas en TI. Puedes encontrarle en nuestro "Rincón Legal", en LinkedIn y en www.marzoasesores.com



Finalmente, respecto a las actividades de marketing, también hay que tener muy en cuenta la LSSICE, la Ley de Servicios de la Sociedad de la Información y Comercio Electrónico, que recoge el derecho de consentimiento y prohíbe comunicaciones comerciales por medios electrónicos si antes no hubieran sido solicitadas o expresamente autorizadas, salvo que exista una relación contractual previa. Esta normativa exige que se ofrezca la oposición, de forma sencilla y gratuita, en cada comunicación y que el interesado pueda revocar el consentimiento en cualquier momento.

La LSSICE regula también el uso de cookies, los derechos de información y consentimiento del usuario y las obligaciones de los prestadores de servicios, y extiende su alcance a cualquier otro Dispositivo de Almacenamiento y Recuperación de Datos (DARD).

EL IMPACTO EN CLOUD

Cloud computing trae consigo un nuevo modelo de prestación de servicios y, en consecuencia, una nueva forma de tratar la información. Con la modalidad de computación en la nube, el proveedor del servicio puede encontrarse en cualquier lugar del mundo y su objetivo será proporcionar los servicios optimizando sus propios recursos.

Ya ahora, como expusieron los expertos de Marzo & Abogados, cuando se opta por Cloud hay que tener en cuenta una serie de consideraciones desde el punto de vista de los derechos de los ciudadanos y del ejercicio de las responsabilidades del cliente de dichos servicios.

Al igual que ocurrirá cuando se aplique GDPR, desde la perspectiva de la normativa de protección de datos, el cliente que contrata los servicios en la nube sigue siendo el responsable del tratamiento de los datos personales, incluso si las dos partes incorporan una cláusula en el contrato con el fin de traspasar la responsabilidad. Por su parte, el prestador del servicio es el encargado del tratamiento.

En este modelo la AEPD considera importantes los siguientes aspectos: las medidas de seguridad del prestador y la confidencialidad de su personal, las actuaciones frente a incidentes de seguridad, si hay transferencias de datos internacionales o no, la posibilidad de cambios unilaterales en el contrato por parte del prestador y, por supuesto, es fundamental que el cliente responsable del tratamiento tenga garantizada la recuperación de los datos personales de los que es responsable, es decir, la portabilidad de los datos. Esto significa que que el proveedor Cloud está obligado, una vez terminado el contrato, a entregar al cliente directamente o a otro proveedor todos los datos en el formato acordado en el menor plazo posible y con las garantías de integridad, sin incurrir en costes adicionales.

Con GDPR, y como es lógico, las dos partes deben firmar un contrato de encargo del tratamiento, y el responsable de éste tendrá que elegir un encargado que ofrezca garantías suficientes para aplicar las medidas técnicas y organizativas necesarias para cumplir con el reglamento y garantizar la protección de los derechos del ciudadano o interesado.

El contrato debe establecer el objeto, la duración, la naturaleza y finalidad del tratamiento, el tipo de datos personales a tratar, las

categorías de interesados, y las obligaciones y derechos del responsable. Además, deberá estipular claramente que el encargado tratará los datos personales siguiendo solo instrucciones documentadas del responsable, incluidas las relacionadas con transferencias de datos personales excepto en contadas ocasiones, por ejemplo, cuando tengan que ver con obligaciones legales del encargado de los datos. El prestador de servicios deberá garantizar que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad y estará obligado a tomar las medidas de seguridad adecuadas al nivel de riesgo.

GDPR también le obliga a asistir al responsable, según qué tratamiento, para atender el ejercicio de derechos y a ayudarle a garantizar el cumplimiento de sus obligaciones de seguridad como, por ejemplo, las relativas con la realización de la evaluación de impacto, la notificación de brechas, ayuda en las inspecciones y auditorías, etc.

Sus obligaciones no acaban ahí, ya que también debe informar al responsable si, en su opinión, una instrucción infringe el RGPD u otra norma de protección de datos y no puede subcontratar sin la autorización previa por escrito, específica o general, del responsable, etc. Este punto es importante porque, además, tiene que firmarse otro contrato con las mismas obligaciones que las de Responsable-Encargado, ya si el subcontratado incumple sus obligaciones, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento.

Ambos abogados mencionaron más aspectos a tener en cuenta, pero prestaron especial atención al cambio que introduce GDPR a la hora de contratar los servicios de proveedores Cloud que no están localizados dentro del Espacio Económico Europeo (EEE) o en países con los que la Unión Europea mantiene acuerdos por

entender que garantizan el nivel adecuado de protección de datos.

En este caso se simplifica el procedimiento ya que, actualmente, para realizar una transferencia internacional de datos es necesaria la autorización previa de la Directora de la AEPD, que podrá otorgar si hay garantías suficientes de que se van a garantizar una serie de derechos y libertades de los ciudadanos. A partir de ahora, las transferencias no se inscribirán en la AEPD, sino en el registro de las actividades, y no hará falta autorización cuando los contratos incluyan cláusulas contractuales tipo.

Por otro lado, SAP también presentó el 7 de marzo en Madrid para los asociados su propuesta para dar cobertura a los requisitos de la normativa. En la sesión, a la que asistieron 41 personas, se realizó una introducción a GDPR y se profundizó el proceso de adaptación a éste sobre la base de tres principios en torno a los que gira la normativa: el de protección de los datos, el de transparencia y el de responsabilidad activa. En la jornada intervinieron Víctor Artola, experto en soluciones de GRC de SAP; Miguel Ángel Gómez, especialista en soluciones OpenText, y Antonio Vergara, arquitecto SAP que escribe un artículo sobre este tema en las siguientes páginas.

Las presentaciones, con toda la información ampliada, están disponibles en la web de AUSAPE.

Cloud computing trae consigo un nuevo modelo de prestación de servicios y, en consecuencia, una nueva forma de tratar la información.