PROTECCIÓN DE DATOS, UN DESAFÍO PARA LA INDUSTRIA

La nueva normativa europea, que entra en vigor en mayo, contempla sanciones que pueden alcanzar los 20 millones de euros o el 4% de la facturación anual para las empresas que no cumplan con las obligaciones establecidas

EL ECONOMISTA

Mayor protección del usuario en el tratamiento de los datos, nuevos requerimientos en el consentimiento, notificaciones sobre brechas de seguridad y la nueva figura del Delegado de Protección de Datos (DPO) son cuestiones que están encima de la mesa de todas las empresas para la adaptación de su política al nuevo Reglamento General de Protección de Datos, que entrará en vigor el 25 de mayo de 2018 y prevé sanciones que alcanzan los 20 millones de euros o el 4 por ciento de la facturación anual a las empresas que no cumplan con lo establecido en esta norma. Una regulación que se completará, en breve, con el futuro Reglamento de ePrivacy, que se está debatiendo en la Comisión Europea.

Isabel Martínez Moriel, asociado senior y responsable del área de Privacy, IT & Digital Business de Andersen Tax & Legal, destaca que la norma sobre *ePrivacy* necesita "una puesta en común de todos los agentes implicados que impida volver atrás en el uso y posibilidades que ofrece Internet. La industria tiene que dar un paso adelante en autorregulación de servicios generales y propuestas que permitan a los usuarios entender qué datos se tratan y con qué finalidad".

Andersen Tax & Legal ha elaborado un informe sobre los puntos a tener en cuenta en la empresa de cara a la entrada en vigor del RGPD y está llevando a cabo una serie de jornadas sobre las implicaciones del cambio normativo. La próxima se celebrará el 6 de marzo en Valencia, junto al Club para la Innovación de la Comunidad Valenciana, con 50 asistentes.

ISTOCK

Cualquier empresa, europea o no, que preste sus servicios a residentes en la Unión Europea y que tenga acceso a cualquier tipo de datos personales, deberá implementar las medidas técnicas y organizativas necesarias para el cumplimiento de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (RGPD). Martínez Moriel explica que el RGPD será de aplicación a responsables y encargados de tratamiento situados fuera de la UE que traten datos de carácter personal de residentes europeos con destino dentro o fuera de la UE. En algunos casos, los operadores situados fuera de esta zona deberán nombrar a un representante para que actúe en ella.

Además, requiere del consentimiento expreso de los titulares de datos y atribuye al responsable la obligación de demostrar que lo ha recabado correctamente, así como de notificar previamente y de forma transparente al interesado si se recaban datos de carácter personal.

Recoge, de esta forma, nuevos derechos en favor de los titulares de datos, entre los que destaca "la minimización en la recogida de datos", el "derecho a la portabilidad" o el "derecho al olvido", e incluye nuevas obligaciones para los encargados de tratamiento, como el mantenimiento de registros de actividades de procesamiento bajo su propia responsabilidad, la cooperación con la autoridad correspondiente y la puesta a disposición de la información, en caso de solicitud, y la notificación por parte del responsable de cualquier brecha de seguridad, algo que debe realizarse ante la autoridad competente en un plazo no superior a 72 horas desde que se tenga conocimiento de ella.

Una de las cuestiones más controvertidas es la del Delegado De Protección De Datos. La mayoría de empresas con un volumen de tratamiento de datos o tamaño significativo, así como instituciones públicas, deberán designar un delegado de protección de datos (DPO). Podrá ser un trabajador de la empresa o podrá externalizarse a un tercero.

El RGPD reconoce, además, las Normas Corporativas Vinculantes como un medio para la legitimación de transferencias internacionales dentro de un grupo de empresas y establece el sistema de ventanilla única, de forma que cualquier empresa situada fuera de la Unión Europea solo tendrá que tratar con una única Autoridad de Protección de Datos como interlocutora.

En cuanto al futuro Reglamento de ePrivacy, Martínez Moriel sostiene que afecta de forma más directa a las empresas, ya que se aplica a todos los datos de comunicaciones electrónicas e introduce un consentimiento más estricto para la publicidad digital, al que se debe someter cualquier empresa, europea o no, que preste sus servicios a residentes en la UE y tenga acceso a cualquier tipo de datos, sean personales o no.

Isabel Martínez Moriel, asociado senior de Andersen Tax & Legal y responsable del área de Privacy, IT & Digital Business; José Luis Piñar, catedrático de Derecho Administrativo, delegado de Protección de Datos del Consejo General de la Abogacía Española y titular de la Cátedra Google sobre Privacidad, Sociedad e Innovación, y Jesús Aspra, Managing Director de Weborama. EE

La normativa incluye más obligaciones en consentimiento y notificaciones sobre brechas de seguridad

La experta hace hincapié en las adaptaciones que va a experimentar el tratamiento de metadatos, es decir, cualquier información relativa al contenido intercambiado o transmitido en una comunicación electrónica y los datos utilizados para rastrear e identificar el origen y el destino de una comunicación. En concreto, los metadata y los datos obtenidos para la elaboración de perfiles a través de *cookies* y de identificadores en línea pasan a considerarse datos personales.

También se refiere a la necesidad de consentimiento explícito del usuario, que es más riguroso en el Reglamento de ePrivacy que en el Reglamento Europeo de Protección de Datos. Las empresas deben recabarlo para cada uno de los usos que se vaya a hacer de los datos.