PUNTOS A APLICAR Y CONTROLAR PARA CUMPLIR CON LA PROTECCIÓN DE DATOS

El nuevo marco europeo, vigente desde el 25 de mayo, otorga más derechos y control a los usuarios y exige una responsabilidad proactiva a las empresas en su tratamiento. Las sanciones en caso de incumplimiento pueden alcanzar 20 millones de euros o el 4 por ciento de la facturación anual

O. FONTANILLO

El Reglamento General de Protección de Datos, por el que se deroga la Directiva 95/46/CE (RGPD), entra en vigor el 25 de mayo en todos los Estados miembros de la Unión Europea, una regulación que se completará, en breve, con el futuro Reglamento de ePrivacy, que se está debatiendo en la Comisión Europea. El nuevo marco otorga más derechos a los usuarios y mayor control de sus datos y exige una responsabilidad proactiva a las empresas en su tratamiento. Un complejo escenario que incluye posibles sanciones de hasta 20 millones de euros o el 4 por ciento de la facturación anual en caso de incumplimientos, y al que muchas empresas aún no se han adaptado.

En este sentido, Ignacio Aparicio, socio de Andersen Tax & Legal, advierte de que "las compañías deben adoptar medidas necesarias para cumplir con el Reglamento y estar en disposición de demostrar que se están aplicando". El experto, que participó en la jornada *¿Estamos preparados para la inminente aplicación del RGPD? Nuevos retos ante la normativa europea de protección de datos*, organizada por Andersen Tax & Legal y la Fundación de Estudios Bursátiles y Financieros (FEBF) -celebrada en la Bolsa de Valencia-, detalló que "el diseño de las medidas debe ser adecuado al volumen de datos que se gestionan, a la sensibilidad de los mismos y al tratamiento que se hace de ellos".

Rafael Ripoll, Of Counsel de la firma; Isabel Martínez Moriel, responsable del área de Privacy, IT & Digital Business del despacho, y María García Zarzalejos, abogada de este área, profundizaron en algunos de los puntos clave que deben cumplir las empresas para adaptarse al nuevo contexto legal.

Isabel Martínez Moriel, responsable del área de Privacy, IT & Digital Business de Andersen Tax & Legal; Rafael Ripoll, Of Counsel de la firma; María García Zarzalejos, abogado, e Ignacio Aparicio, Socio de Andersen Tax & Legal. G. LUCAS

¿Quién está obligado? Cualquier empresa, europea o no, que dirija sus servicios a ciudadanos de la Unión Europea y tenga acceso a datos de carácter personal y metadatos. En algunos casos, los operadores de fuera de esta zona deberán nombrar a un representante para que actúe en ella. Cualquier empresa de fuera de la UE solo tendrá que tratar con una única Autoridad de Protección de Datos como interlocutora.

Recogida de datos. Isabel Martínez Moriel subrayó que el Reglamento Europeo de Protección de Datos refuerza el derecho del usuario sobre sus datos y recoge el consentimiento expreso de su uso, mediante una acción libre, inequívoca, precisa y con la información suficiente sobre el tratamiento que se va a hacer de los mismos. Se crearán bases de datos específicas para las distintas funcionalidades.

Registro de ficheros. Ya no existe la obligación de registrar ficheros en la Agencia Española de Protección de Datos, pero se debe llevar a cabo un registro de actividades de tratamiento interno en la empresa, donde consten los datos tratados, los encargados de tratamiento, las transferencias internacionales… Es obligatorio para empresas de más de 250 empleados o aquellas que lleven a cabo tratamientos de gran volumen.

Actualización de los datos. Martínez Moriel apunta que es necesaria una evaluación de los datos personales tratados por la empresa para aplicar medidas adaptadas a aquellos que han estado activos o sobre los que se tiene un interés legítimo en base a una relación contractual. Se define la obligación de revisar y actualizar el consentimiento del usuario, explicando de forma clara y concisa la finalidad de utilización de sus datos.

Nuevos derechos de los usuarios. Entre ellos, se contemplan el derecho de portabilidad, limitación del tratamiento, a no ser objeto de decisiones automatizadas y, sobre todo, el derecho al olvido.

Gestión del riesgo. El nuevo modelo de privacidad está basado en la gestión del riesgo, en función de si se trata de riesgo alto o estándar, el cual se atiende mediante el diseño de medidas concretas para que el tratamiento de los datos sea seguro en función de su volumen y uso. En este sentido, "pese a que en muchos casos no se trate de datos muy privados, el uso a gran escala de datos personales nos puede llevar a tener que realizar una evaluación de impacto", advierte Martínez Moriel. Se recomienda, asimismo, la elección de encargados de tratamiento -gestoría de nóminas, empresas de destrucción de información confidenciales, servicios de *hosting*, etcétera- que estén adheridos a códigos de conducta o certificaciones del sector.

Jornada sobre la protección de datos en Bolsa de Valencia. G. LUCAS

Responsabilidad y nuevos protocolos de seguridad. Se definen nuevas obligaciones para los encargados del tratamiento de los datos, 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.

El Delegado de Protección de Datos. El Reglamento General de Protección de Datos introduce la figura del Delegado de Protección de Datos (DPO por sus siglas en inglés), obligado para autoridades y organismos públicos, entidades que traten datos de forma sistemática a gran escala y para empresas que traten datos sensibles -por ejemplo, financieros, de salud, afiliación sindical o política- o sobre infracciones penales. María García Zarzalejos señaló que "debe ser una persona que no sea susceptible de incurrir en conflictos de interés, por lo que no podría ser un miembro de la directiva o aquellos que decidan sobre el tratamiento de los datos directamente, como puede ser el responsable del departamento de tecnologías de la información o de marketing". Esta figura puede ser tanto una persona interna de la organización o un experto externo, mediante un contrato de prestación de servicios. El DPO no puede llevar a cabo la auditoría en materia de protección de datos.

Otras medidas recomendables. Los expertos que intervinieron en la jornada expusieron otras medidas "recomendables" para cumplir con las exigencias de privacidad, como la minimización de datos; la elaboración de evaluaciones de impacto en materia de protección, o la transparencia. Además, Ignacio Aparicio hizo referencia a la "pseudominización", que implica "anonimizar los datos personales tras el periodo legal de conservación, de forma que no se puedan vincular con una persona, pero se puedan utilizar para finalidad distinta para la que habían sido recabados, como podrían ser para finalidades analíticas o estadísticas".