Expansión | JURÍDICO

Wolters Kluwer

Guía para adaptarse a la nueva norma de protección de datos

La nueva regulación europea impone una serie de obligaciones a las empresas. Todas las compañías que realicen algún tipo de tratamiento de datos deberán ejecutar importantes cambios antes de 2018.

V. Moreno. Madrid

El Reglamento General de Protección de Datos (RGPD), que ha impuesto un nuevo marco normativo para el conjunto de países europeos, ha otorgado un mayor grado de control a los ciudadanos sobre su información privada en el mundo 2.0. Este texto, que entrará en vigor en mayo de 2018, también impone cambios radicales para las empresas y éstas deben ponerse a trabajar desde hoy para adaptar sus protocolos y estructuras a la nueva regulación.

"Sin duda, el RGPD es actualmente una de las normas más importantes de la legislación europea, puesto que se trata de una norma transversal y que afecta a todos los ámbitos", explicaba en la jornada sobre el nuevo reglamento de la UE, organizada por EY, José Luis Piñar, catedrático de derecho administrativo de la Universidad CEU San Pablo y titular de la Cátedra Google de Privacidad, Sociedad e Innovación. "Un abogado no puede dejar de tener en la cabeza el reglamento y tiene que conocer todas sus vertientes".

Dejando de lado los derechos de los ciudadanos –derecho al olvido, restricción del tratamiento, portabilidad de datos o rechazo al *profiling*–, este artículo enumera algunas de las obligaciones que afectarán directamente a las empresas y que impondrán cambios en el seno de las compañías.

Las compañías tienen hasta mayo de 2018, cuando echará a andar la regulación, para adaptarse.

Consentimiento

"Al no permitirse ya el consentimiento tácito, el reglamento obliga a todas las empresas a revisar el conjunto de cláusulas y rehacerlas. Es necesario comunicar de una manera nueva, clara y simple con el usuario. Pasamos a un modelo más amable, en el que se pretende que el usuario se lea los términos y condiciones. El consentimiento debe ser revocable en cualquier momento. Las empresas deben asegurarse de que los datos sólo están siendo empleados para los fines para lo que fueron recabados", apunta Raúl Rubio, socio responsable de tecnologías de la información y comunicaciones de Baker & McKenzie.

El reglamento de la UE es una norma transversal y afecta a todos los ámbitos de los negocios

Estudio de riesgos

"El *privacy impact assesment* (PIA) o estudio de riesgos es una tarea primordial que hay que tener ya pensado para todos los nuevos acuerdos en los que exista un alto riesgo para la protección de datos. Lo mejor que puede hacer una empresa es automatizar este proceso. Deben desarrollar una herramienta eficiente que identifique cuando es necesario hacer un análisis", añade Rubio. "También será positivo verificar todos los acuerdos anteriores al reglamento para que se ciñan a las nuevas obligaciones".

SANCIONES

El reglamento impondrá sanciones muy elevadas por incumplir estas obligaciones. Las **violaciones graves** tendrán multas de hasta 10 millones de euros o el 2% de la facturación mundial. Las muy graves hasta 20 millones o el 4% de la facturación total.

Comunicación de fallos

"Es una nueva obligación impuesta por el RGPD. El encargado de tratamiento deberá notificar los fallos de seguridad a la Agencia Española de Protección de Datos (AGPD) en un plazo de 72 horas", explica Rosario Álvarez, letrada asociada de tecnologías de la información y comunicaciones de Baker & McKenzie. "El encargado debe contar con un sistema efectivo para realizar el reporte a la AGPD o para comunicar el fallo a los afectados si existe algún riesgo para sus derechos".

Las empresas deben realizar campañas de sensibilización y formación para sus trabajadores

DPO

"El *data protection officer* o delegado de protección de datos es una figura esencial en el reglamento. Tendrá que identificar los riesgos y buscar soluciones para solventarlos. Las empresas deberán contar con este delegado, interno o externo, otorgarle total independencia y aportarle las herramientas que necesite cuando las solicite", dice Rodrigo González, asociado sénior del departamento mercantil de EY Abogados y coordinador de proyectos en materia de protección de datos.

"El RGPD no especifica el perfil del DPO y sólo apunta que debe tener una formación adecuada, dejando en manos de la empresa encontrar la persona idónea. Éste es un rol esquizofrénico, porque debe actuar en dos ámbitos: por un lado, ayudar a la empresa que le contrata para que cumpla sus obligaciones y, al mismo tiempo, ser auditor interno en comunicación constante con la AGPD", concluye Rubio.

Formación

"Educación y sensibilización, esto es lo que debe hacer una compañía respecto a la protección de datos. Habitualmente, en casos de tratamientos inadecuados, lo que falla no son las propias tecnologías, sino el ser humano, ya sea por no seguir las reglas, por negligencia o, en ciertos casos, intencionalmente. El factor humano es el eslabón débil y, por eso, la única medida adecuada es la formación y que la empresa genere actividades para tomar conciencia de la importancia de la protección de datos", comenta Álvarez.

Sector sanitario y los datos relativos a la salud

El sector sanitario es uno de los ámbitos más expuestos y afectados por la nueva normativa de protección de datos europea. Los datos especiales, hasta ahora conocidos como datos sensibles –salud, origen racial, religión–, cuentan con obligaciones reforzadas. Además, el Reglamento General de Protección de Datos amplía al listado de datos especiales los genéticos y los biométricos.

"Las entidades cuya actividad principal consista en el tratamiento a gran escala de categorías especiales de datos personales –hospitales, clínicas, aseguradoras médicas, mutuas y, eventualmente, laboratorios y empresas farmacéuticas– estarán obligadas a nombrar un delegado de protección de datos", explica Norman Heckh, socio del área de Tecnologías de la Información de Ramón y Cajal Abogados. "En lo que se refiere a las medidas de seguridad, las empresas del sector sanitario deberán, al menos, aplicar medidas de seudonimización, cifrado, garantía de confidencialidad, integridad, disponibilidad y acceso a los datos en caso de incidente", añade. Por último, Heckh insiste en el protagonismo que otorga el reglamento a los códigos de conducta y la importancia de elaborar estudios de riesgo (PIA).

LABORAL

Negarse a reincorporar a un trabajador expresidiario es discriminatorio

Almudena Vigil. Madrid

Negarse a reincorporar a la plantilla a un trabajador expresidiario es discriminatorio. Así lo afirma una sentencia del juzgado de lo social número 33 de Madrid que ha declarado nulo el cese de un trabajador que fue despedido mientras cumplía prisión. La empresa le envió la carta de despido certificada a su domicilio, lo que le impidió acceder a ella, no pudiendo tampoco acudir a recogerla a Correos donde quedó depositada.

Según la sentencia, la reinserción social es un derecho fundamental de todo ciudadano privado de libertad por el cumplimiento de una condena penal, tal y como contempla el artículo 25.2 de la Constitución. En este sentido, explica que "se impone el derecho del trabajador a ser reintegrado en sus derechos de ciudadanía, sin que los antecedentes penales puedan en ningún caso ser motivo de discriminación social o jurídica". Señala que, precisamente, "uno de estos derechos, esencial además para alcanzar efectivamente su socialización y su dignidad personal, es el derecho al trabajo (artículo 35.1 de la Constitución)".

Por ello, explica que "no incorporar al trabajo a quien fue condenado y ya cumplió por el delito cometido, constituye una conducta discriminatoria por tal circunstancia o condición, que es incompatible con el artículo 14 de la Constitución y con el 17.1 del Estatuto de los Trabajadores".

Carta de despido

El juzgado recuerda que diversas sentencias del Tribunal Supremo han sostenido que, si bien la condena penal no es por sí misma causa de despido, de la ausencia al trabajo por esta causa sí sería responsable el trabajador porque fue condenado por un delito determinante de su privación de libertad, pudiendo aplicarse el artículo 54.1.a) del estatuto, que considera infracción muy grave las actividades contrarias a la seguridad nacional o el orden público. Sin embargo, la sentencia del juzgado señala que "sorprendentemente" la empresa no imputó al trabajador ausencias injustificadas.