elEconomista.es

Los auditores se preparan para la nueva legislación de protección de datos... ¿cómo afectará a su sector?

ELECONOMISTA.ES

24/05/2018 - 13:22

- *La nueva ley entra en vigor este viernes 25 de mayo*

Los auditores se enfrentan a un nuevo reto, la nueva normativa de protección de datos, según asegura el informe '¿Qué implicaciones tiene la nueva normativa de protección de datos sobre expertos contables y auditores? El Reglamento General de Protección de Datos', elaborado por Accountancy Europe (antes Federación Europea de Expertos Contables), entidad de la que forma parte el Instituto de Censores Jurados de Cuentas de España (ICJCE).

El informe pretende ayudar a los auditores y expertos contables a conocer cómo impactará en su trabajo la nueva normativa del Reglamento General de Protección de Datos (RGPD), que entra en vigor este viernes, 25 de mayo de 2018.

Algunas violaciones de la seguridad en la protección de datos pueden conllevar multas de entre 20 millones de euros, la más alta, o el 4% del volumen de negocio de la firma. Las violaciones de la seguridad menos graves implican multas de entre 10 millones de euros y el 2% del volumen de negocio global a los actuales.

Los interesados tendrán derechos adicionales como el derecho a presentar una reclamación ante una autoridad de control para recurrir judicialmente contra un responsable o encargado del tratamiento de datos y de obtener compensación del responsable.

El papel de los profesionales

El tratamiento de datos es cualquier operación realizada sobre datos personales de una persona. Incluye la recogida, registro, estructuración, conservación, adaptación, consulta, utilización, comunicación, supresión o destrucción de datos.

Los datos pueden ser tratados por responsables del tratamiento de datos (responsables) y por encargados del tratamiento de datos (encargados). Los auditores y expertos contables pueden actuar tanto de responsables como de encargados del tratamiento de datos.

Un auditor o experto contable que conserva datos personales de sus clientes en la nube es un responsable.

El proveedor de servicios en la nube es, en este caso, un encargado que trata los datos que conservan los profesionales. Sin embargo, estos mantienen sus responsabilidades cuando externaliza el tratamiento de datos, lo que incluye garantizar una seguridad adecuada sobre los datos personales.

El RGPD no cubre el tratamiento de datos personales por una persona física en el ejercicio de una actividad personal o doméstica. Tampoco incluye información relativa a empresas u otras entidades jurídicas, es decir, información no personal.

Bases del tratamiento de datos

El tratamiento de datos personales es legal cuando es necesario para:

- La ejecución de un contrato en el que el interesado es parte

- El cumplimiento de una obligación legal

- Proteger intereses vitales del interesado

- El cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

- La satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado.

Derecho sobre los datos

Los profesionales tendrán que informar al interesado del cual recojan información personal. Los derechos sobre los datos incluyen el derecho de rectificación, objeción, supresión, acceso del

interesado, portabilidad de datos, restricciones al tratamiento y ciertos derechos respecto a la creación de perfiles.

También tendrán que actuar y responder a toda solicitud de un interesado y deberán llevar a cabo las medidas relativas a los derechos del interesado de manera gratuita. Si no se lleva a cabo acción alguna con relación a una solicitud, el profesional deberá asesorar al interesado sobre sus derechos de reclamación.

Derecho a la información

Cuando se recogen datos directamente del interesado, el responsable del tratamiento deberá proporcionar información tal como sus datos de contacto, la duración de la retención de los datos, el objeto del tratamiento y la base legal. El responsable del tratamiento también deberá informar al interesado cuando tenga intención de llevar a cabo tratamientos adicionales con unos propósitos distintos a los que motivaron la recogida inicial de datos.

Durante los procedimientos de diligencia debida con respecto al cliente, los profesionales necesitan dar a sus clientes los datos de contacto y explicarles que la información se recoge para llevar a cabo una tarea de interés público. Cuando un profesional utiliza un proveedor de servicios en la nube cuyos servidores están fuera de la UE, también necesitarán informar al cliente acerca de las salvaguardas listas para garantizar la protección de los derechos sobre los datos.

Responsabilidad proactiva

Los responsables del tratamiento deben implementar las medidas necesarias para garantizar y ser capaces de demostrar que el tratamiento de datos cumple con los requerimientos del RGPD. También deben llevar a cabo un análisis de impacto antes de embarcarse en algún proceso que probablemente conlleve un alto riesgo contra los derechos y libertades de los interesados.

Además, tanto responsables como encargados del tratamiento tienen obligación de designar a un delegado de protección de datos en ciertos casos. Por ejemplo, es necesario un delegado de protección de datos cuando las actividades principales de la organización requieran el seguimiento habitual y sistemático de interesados a gran escala o consista en el tratamiento a gran escala de datos especiales relativos a condenas criminales.

El delegado de protección de datos debe ser un experto en protección de estos y debe controlar el cumplimiento del RGPD. Puede ser un empleado de la organización, pero debe ser independiente en el ejercicio de sus responsabilidades.

Seguridad

Tanto el responsable como el encargado del tratamiento han de implementar las medidas adecuadas para garantizar un adecuado grado de seguridad. El RGPD obliga tanto al responsable como al encargado a considerar el actual "estado de la técnica" al implementar las

medidas de seguridad y específicamente nombra la seudonimización y encriptación como técnicas que podrían ser aplicadas.

Tales medidas técnicas raramente se pueden aplicar de manera sencilla. Por ejemplo, la encriptación no es probable que sea efectiva cuando los datos se transmiten a un servicio en línea (como por ejemplo un paquete contable), mientras que la seudonimización puede ser adecuada pero solo después de una personalización. Implementar tales medidas tendrá, por lo tanto, implicaciones de coste.

Implementación del RGPD

El RGPD introduce el concepto de "autoridad de control principal". Es el organismo del estado miembro en el que está ubicado el establecimiento principal del responsable o encargado del tratamiento de datos dentro de la UE. Esta autoridad liderará todo el tratamiento transfronterizo realizado por la organización.

Una red de firmas de auditoría tendrá que tratar principalmente con la autoridad de control de su sede en la UE. Cuando un profesional de una red adopta medidas para cumplir con una decisión emitida por la autoridad de control principal, solo han de notificar esas medidas a la autoridad reguladora. Esta última deberá notificarlo a la otra autoridad de control implicada.