ACCOUNTANCY EUROPE.

¿QUÉ IMPLICACIONES TIENE LA NUEVA NORMATIVA DE PROTECCIÓN DE DATOS SOBRE EXPERTOS CONTABLES Y AUDITORES?

El Reglamento General de Protección de Datos

FACTS.

ABRIL 2017

DESTACADO

Las nuevas normas de la UE sobre protección de datos que entrarán en vigor el 25 de mayo de 2017 serán de aplicación sobre todos aquellos que trabajen con información que contenga datos de carácter personal, sea conservada en línea o en papel. Los expertos contables y auditores se ven afectados de manera directa por esos requerimientos ya que se ven involucrados en la recogida, conservación y tratamiento de datos relativos a sus clientes, empleados y subcontratistas. Estos requerimientos de protección de datos se han de tener en cuenta seriamente ya que las multas pueden alcanzar decenas de millones de euros.

El objetivo de esta nota informativa es ayudar a los profesionales, expertos contables y auditores, a conocer cómo impactará en su trabajo la nueva normativa. Explicamos los cambios legislativos y se proporcionan ejemplos de lo que significa en la práctica: informar al cliente sobre sus derechos sobre los datos, garantizar una correcta ciberseguridad y responder mejor y oportunamente a las violaciones de la seguridad, entre otros aspectos.

INTRODUCCIÓN

Los expertos contables y auditores deberían prepararse con esmero para el *Reglamento General de Protección de Datos* (RGPD)[1] que entra en vigor el 25 de mayo de 2018. Proporciona el marco legal aplicable para la protección de datos personales en la UE. Los profesionales auditores y expertos contables procesan datos personales por lo que se verán afectados directamente por esta norma. El RGPD se desarrolla y reemplaza a la Directiva de Protección de Datos[2] (la Directiva), que fue adoptada hace 21 años.

Desde 1995, las formas en las que se comunican y utilizan los datos personales han cambiado. La nueva legislación tiene, en consecuencia, un doble objetivo: (1) considerar esos cambios en el ámbito de los datos personales e (ii) proporcionar un marco normativo más coherente en la UE. Para ello, el RGPD introduce algunas obligaciones nuevas y onerosas, e incrementa las sanciones por incumplimiento.

Todas aquellas organizaciones que gestionen información de carácter personal deberían revisar sus procedimientos lo antes posible para asegurarse que cumplen con las nuevas disposiciones. Un documento basado en Google estima que, de media, el coste de implementar el nuevo RGPD en una PYME se eleva a 7.200 euros anuales[3].

Esta publicación empieza con un resumen de los conceptos clave en el área de la protección de datos. Sigue con un análisis de los principios fundamentales prescritos por el RGPD para el tratamiento de datos personales. La tercera parte de la publicación incluye aspectos relativos al control e incumplimiento del RGPD. Antes de concluir con los cambios más significativos que conlleva el RGPD, se presta atención a la transferencia de datos a terceros países.

CONCEPTOS CLAVE Y EL PAPEL DE LOS PROFESIONALES EN LA PROTECCIÓN DE DATOS

Los datos personales incluyen toda información relativa a una persona física identificable ("el interesado"). Por ejemplo, su domicilio particular, ingresos o número de teléfono de un individuo en concreto. Los profesionales procesan de manera habitual datos personales de sus clientes o empleados.

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

Por ejemplo, los expertos contables y auditores recogen y conservan información relativa a la identidad de un cliente nuevo para cumplir con los requerimientos de diligencia debida con respecto al cliente de la *Directiva contra el blanqueo de capitales.* Cuando prestan servicios de nómina a sus clientes[4] (o a ellos mismos), también acceden a datos personales relevantes para los empleados. Los auditores, por su parte, tratan datos personales de los empleados de sus clientes.

Los datos pueden ser tratados por responsables del tratamiento de datos (responsables) y por encargados del tratamiento de datos (encargados). Los responsables pueden recurrir a los encargados para tratar datos en su lugar, pero deben tener presente sus responsabilidades al trabajar con un encargado.

Los profesionales expertos contables y auditores pueden actuar tanto de responsables, como de encargados del tratamiento de datos. Por ejemplo, un experto contable o auditor 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 conserva el responsable. Sin embargo, el experto contable o auditor mantiene sus responsabilidades

---

[1] El reglamento (UE) 2016/679 está disponible en http://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&from=ES

[2] La Directiva 95/46/EC está disponible en: http://eur-lex.europa.eu/1egal-content/ES/TXT/HTMU?uri=URISERV:114012&from=ES

[3] L. Christensen, A. Colciago, F. Etro and G. Rafert, *The Impact of the Data Protection Regulation in the E.U* (13 de febrero de 2013), disponible en: http://bit.ly/2iTWy9r

[4] En España, esta prestación de servicios se refiere a los expertos contables

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.

Por poner un ejemplo, los profesionales no están afectados por el RGPD cuando tratan información sobre la ubicación de los negocios de sus clientes (información no personal) o cuando realizan un seguimiento de las notas de sus hijos (actividad doméstica).

PRINCIPIOS DEL TRATAMIENTO DE DATOS PERSONALES

Los responsables del tratamiento tienen muchas responsabilidades y limitaciones cuando tratan datos de carácter personal. Esta sección analiza cuándo pueden tratarse datos personales legalmente; qué es importante tener en cuenta con respecto a los derechos sobre los datos de los interesados y cómo los responsables y encargados del tratamiento de datos debería poder probar que están respetando sus obligaciones.

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 o
- 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

Por ejemplo, los profesionales pueden justificar el tratamiento de información que contenga datos personales de clientes en el contexto del proceso de diligencia debida con respecto al cliente ya que es para salvaguardar el interés público y para cumplir con sus obligaciones según la legislación contra del blanqueo de capitales.

Además de las opciones que se detallan anteriormente, también es posible tratar datos cuando el interesado da su consentimiento. Sin embargo, las condiciones bajo las cuales ello es posible, están reguladas de manera estricta y el responsable del tratamiento deberá poder demostrar que el interesado dio su consentimiento al tratamiento. Es importante indicar que la prestación de un servicio no requiere del consentimiento si el tratamiento no es necesario para la prestación de dicho servicio. Además, el interesado puede retirar su consentimiento en cualquier momento.

EL RGPD también introduce disposiciones para la situación en que los datos son tratados más allá de lo que era su propósito original. Requiere que los responsables del tratamiento documenten correctamente la decisión y que describan los factores que han tenido en cuenta para llegar a ella.

DERECHOS SOBRE LOS DATOS

Los profesionales tendrán que informar al interesado del cual recojan información personal. Por ejemplo, a sus clientes sobre sus derechos sobre los datos, y tomar medidas para facilitar esos derechos. Ello puede requerir la revisión de la información proporcionada al interesado sobre cómo se tratan sus datos personales. Tal revisión debería incluir la revisión del lenguaje utilizado de modo que sea claro y comprensible por el interesado[5].

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. Algunos de estos derechos se describen más adelante. Se urge a los profesionales involucrados en análisis de macrodatos

[5] Hogan Lovells, *Future-proofing privacy: A guide to preparing for the EU data Protection Regulation*

a tomar buena nota de los cambios sobre la creación de perfiles a través de datos, ya que se considera una actividad de alto riesgo[6].

Los profesionales también tendrán que actuar y responder a toda solicitud de un interesado. Por ejemplo, su cliente, para ejercer sus derechos. Ello puede requerir crear nuevos procedimientos para abordar esas solicitudes. Además, a menos que la solicitud del interesado sea manifiestamente infundada o excesiva, los profesionales 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.

Las obligaciones de protección de datos que se describen anteriormente también son aplicables a la información sobre el personal. Los estados miembro o los convenios colectivos entre empleadores y empleados pueden adoptar más normas para el tratamiento de los datos personales de empleados en el ámbito laboral. Ello significa que pueden darse variaciones en los requerimientos entre estados miembro.

EL 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. Los responsables del tratamiento deberían, por tanto, proporcionar al interesado (por ejemplo, al cliente, al empleado, etc.) respuestas sencillas a las siguientes cuestiones clave:

- ¿Quién eres?
- ¿Quién (más) recibe mis datos?
- ¿Por qué tratas mis datos?
- ¿Durante cuánto tiempo vas a conservar mis datos?
- ¿Cuáles son mis derechos sobre los datos?

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. Cuando los datos no se han recogido directamente del interesado, los responsables del tratamiento deberán proporcionar al interesado información similar a la que se daría si se hubiera recogido directamente.

Por ejemplo, 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.

EL DERECHO A LA SUPRESIÓN

El derecho a la supresión o el "derecho al olvido" requiere que los responsables del tratamiento supriman los datos personales a solicitud del interesado en ciertas circunstancias. El derecho a la supresión no es aplicable cuando el tratamiento es necesario para que el responsable del tratamiento cumpla con requerimientos legales o cuando el tratamiento es por el interés público.

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. Las obligaciones pueden cumplirse a través de la adhesión a un procedimiento de certificación o código de conducta. Presumiblemente, también exige que la organización documente los procesos y registre decisiones concretas. Los responsables del

[6] Hogan Lovells, *Future-proofing privacy: A guide to preparing for the EU data Protection Regulation*

tratamiento deben también 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, Para garantizar el correcto cumplimiento del RGPD, será importante ir más allá de "marcar la casilla" y desarrollar una cultura de protección de datos adecuada.

Un nuevo requerimiento que incluye el RGPD es que el responsable del tratamiento está obligado a tomar medidas que lleven a una protección de datos "desde el diseño y por defecto"[7] y garantizar que solo se tratan los datos personales estrictamente necesarios. Por ejemplo, en los procedimientos de diligencia debida con respecto a clientes, los profesionales no deberían tratar datos personales como las preferencias políticas del cliente.

Los responsables están obligados a mantener un registro de las actividades de tratamiento de datos que incluya detalles sobre las medidas técnicas de seguridad sobre datos y su tratamiento. Sin embargo, existe una exención para organizaciones de menos de 250 empleados.

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

El principio de responsabilidad proactiva se extiende, así mismo, a la interacción con los encargados del tratamiento de datos. El RGPD exige que los responsables hagan uso únicamente de encargados del tratamiento de datos que les ofrezcan las garantías suficientes de haber implementado las medidas adecuadas para cumplir con los requerimientos del RGPD. Ello significa que los responsables han de conocer tanto sus propias obligaciones como las de los encargados del tratamiento de datos.

Además de las disposiciones que afectan a responsables y encargados, existen una serie de obligaciones específicas sobre los encargados del tratamiento de datos. Por ejemplo, un encargado del tratamiento no puede contratar a otro encargado sin consentimiento previo del responsable.

El contrato con el encargado del tratamiento debería establecer las bases del trabajo de los encargados del tratamiento. Debe estipular que el encargado del tratamiento ayudará al responsable a cumplir con un número de obligaciones posteriores, como a cumplir con las solicitudes de los interesados, notificar las violaciones de la seguridad o notificar al responsable si cree que alguna instrucción de tratamiento específica infringe el RGPD.

Las nuevas obligaciones aplicables a los responsables y encargados del tratamiento de datos afectarán a las relaciones futuras entre ambos. Como resultado, es probable que los contratos sean más detallados. Las nuevas obligaciones pueden requerir también la revisión de los contratos vigentes[8].

Los profesionales deberían, en consecuencia, ser cuidadosos cuando utilicen los servicios de proveedores, como por ejemplo, proveedores de servicios en la nube. Puede iniciarse durante la selección del proveedor. Por ejemplo, cuando se organice una licitación para servicios en la nube, los profesionales podrían incluir en la convocatoria criterios relativos a la manera en que el proveedor trata la ciberseguridad o si existe un informe de aseguramiento sobre el cumplimiento con las normas internacionales aplicables.

---

7 Para mayor información y orientación, véase ENISA, *Privacy by design*, disponible en https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

8 Hogan Lovells, *Future-proofing privacy: A guide to preparing for the EU data Protection Regulation*

LA PROTECCIÓN DE DATOS TAMBIÉN ES APLICABLE A LOS ARCHIVOS

La Oficina del Comisionado de Información del Reino Unido (UK), la autoridad que respalda los derechos de información en UK, multó al Consejo del Condado de Norfolk (Norfolk) por incumplimiento de las disposiciones sobre protección de datos[9].

Como parte de una mudanza de unas oficinas, Norfolk se deshizo de algunos muebles, incluyendo unos archivadores que se usaban por el equipo social de protección de la infancia. Norfolk no tenía un procedimiento escrito para determinar quién era el responsable de vaciar los archivadores, por lo que quedó sin hacer. Como resultado, una persona que compró posteriormente uno de esos archivadores encontró expedientes con información sensible.

La ICO encontró que Norfolk no tenía las medidas adecuadas contra el tratamiento no autorizado de datos personales ni contra pérdidas accidentales o destrucción de datos personales, Norfolk fue multado con 60.000 libras.

Este caso muestra la importancia de tener procedimientos correctos de protección de datos independientemente de si estás en la nube o utilizas archivos en papel.

SEGURIDAD

Tanto el responsable como el encargado del tratamiento han de implementar las medidas adecuadas para garantizar un adecuado grado de seguridad. Tales medidas deberían estar basadas en una evaluación del riesgo.

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[10] y encriptación como técnicas que podrían ser aplicadas. Ello pondrá más presión sobre las organizaciones para que, al menos, consideren si esas técnicas son necesarias y eficientes en términos de coste y, en su caso, las implementen.

Tales medidas técnicas raramente se pueden aplicar de manera simple. 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.

EL RGPD introduce también nuevas normas con relación a la respuesta a las violaciones de la seguridad. En esa situación, los responsables están obligados a informar de la violación de la seguridad a su autoridad supervisora lo antes posible. Cuando la violación de la seguridad tiene un alto riesgo sobre los derechos y libertados de los interesados, los responsables también han de notificar la violación de la seguridad a los interesados. La obligación del encargado es notificar al responsable de cualquier violación de la seguridad sin retraso no justificado.

Por ejemplo, si alguien piratea el servidor de un profesional y roba información personal del cliente (por ejemplo, una password, domicilio, edad e ingresos), el profesional debe informar de esta violación de la seguridad a la autoridad de control y a los clientes[11]. Si el profesional conserva los datos de los clientes en la nube, el proveedor

[9] ICO disponible en https://ico.org.uk/media/action-weve-taken/mpns/2013720/mpn-norfolk-county-council-20170315.pdf

[10] El proceso de seudonimizar consiste en separar la información original de tal modo que sin volverla a unir o asociarla no es posible identificar a personas físicas. El ejemplo que encajaría en dicho proceso sería el de aplicar un código a una muestra biológica que se envía a analizar a un laboratorio

[11] Puede revisar si tiene una cuenta que se haya visto comprometida por una violación de la seguridad sobre datos en https://haveibeenpwned.com/

de servicios en la nube debería informar al responsable de cualquier violación de la seguridad. Lo último debería ser después notificado a las autoridades de control y al cliente.

GUÍAS SOBRE SEGURIDAD DE DATOS DISPONIBLES PARA PYMES

La Agencia de la Unión Europea para la seguridad en la red y de la información (ENISA por sus siglas en inglés) publicó unas orientaciones (guías) para ayudar a las PYME a adoptar un enfoque basado en el riesgo para la seguridad de los datos que tratan[12].

Las orientaciones tienen como objetivo ayudar a las PYME a conocer el contexto del tratamiento de los datos personales y asesorarlas, a través de un cuestionario, sobre los riesgos de seguridad asociados. ENISA también propone medidas organizativas y técnicas de seguridad que pueden adoptar las PYME para cumplir con el RGPD.

IMPLEMENTACIÓN DEL RGPD

CONTROL

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 (en realidad es una "ventanilla única" para una organización para todos los tratamientos de datos dentro de la UE.

Las autoridades de control de estados miembro distintos al estado miembro en el que se ubica la autoridad de control principal pueden seguir involucradas cuando un estado miembro se ve afectado por el tratamiento de datos de una organización. Esto pasa, por ejemplo, cuando el tratamiento se da exclusivamente dentro de las fronteras nacionales de dicho estado miembro.

Ello puede ser un cambio valioso para responsables o encargados del tratamiento de datos con establecimientos en más de un estado miembro ya que puede simplificar sus obligaciones de registro, normativas y de información. Se les advierte, en consecuencia, a identificar quien es su autoridad de control principal.

Por ejemplo, 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.

Los estados miembro puede emitir normativa adicional respecto a los poderes de las autoridades de control con relación a los responsables y a los encargados del tratamiento de datos, quienes están sujetos al secreto profesional.

INCUMPLIMIENTOS

Algunas violaciones de la seguridad pueden dar lugar a multas de hasta el mayor de los importes entre 20 millones de euros o el 4% del volumen de negocio. Las violaciones de la seguridad menos graves implican multas de hasta el mayor de los importes entre 10 millones de euros y el 2% del volumen de negocio global.

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.

---

[12] ENISA *Guidelines for SMEs on the security of personal data processing (enero de 2017)*, disponible en https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

TRANSFERENCIAS DE DATOS PERSONALES A TERCEROS PAÍSES

Los datos personales solo pueden ser transferidos a países de fuera de la UE cuando se puede garantizar el mismo grado de protección de datos. En la práctica, ello significa que bien en el país existe un marco de protección similar al de la UE o bien que el responsable se asegura de que se adoptan ciertas medidas que garanticen una protección de datos suficiente.

La Comisión Europea evalúa el grado de protección en los terceros países y mantiene una lista de aquellos que cumplen con los criterios. Las transferencias de datos se pueden realizar a cualquier país que esté incluido en la lista sin autorización específica. Hasta ahora solo unos pocos países han mostrado un grado adecuado de protección e integran la lista de la Comisión[13].

Los datos personales pueden seguir enviándose a terceros países no-equivalentes si se incorporan las salvaguardas adecuadas. Dichas salvaguardas pueden adoptar la forma de normas corporativas obligatorias, cláusulas contractuales aprobadas por la Comisión, códigos de conducta o procedimientos de certificación.

Los profesionales no necesitarán autorización para conservar datos en Suiza, que está en la lista de la Comisión. Por otra parte, si una red de firmas de auditoría quiere conservar sus datos en Islandia, podrá hacerlo si adopta normas corporativas obligatorias. Tales normas deberían incluir la aceptación de responsabilidad de las entidades establecidas en la UE por violaciones de la seguridad de cualquier estado de fuera de la UE.

TRANSFERENCIAS A REINO UNIDO: EL IMPACTO DEL BREXIT

Cuando Reino Unido (u otro estado miembro) abandone la UE se considera “tercer país”. Ello significa que los responsables y encargados del tratamiento que tratan datos de carácter personal de interesados de la UE o los responsables del tratamiento de datos de la UE que utilizan encargados que transfieren datos al Reino Unido deberán revisar sus prácticas actuales de tratamiento de datos[14].

TRANSFERENCIAS A LOS ESTADOS UNIDOS DE AMÉRICA EEUU: EL ESCUDO DE PRIVACIDAD

El caso de los EEUU es un caso especial. Está permitido transferir datos de la UE a entidades de los EEUU cuando estas entidades formen parte del Escudo de privacidad[15] Cuando un profesional quiere trasladar datos personales del cliente a los EEUU bajo el Escudo de Privacidad, necesita asegurarse de que las entidades estadounidenses con las que trabaja están en la lista del Escudo de Privacidad y que han tomado todas las medidas necesarias para cumplir con los requerimientos. Alternativamente, pueden transferir datos utilizando otros medios autorizados que ofrecen una adecuada protección de los datos (por ejemplo, mediante cláusulas contractuales).

El Escudo de Privacidad está actualmente cuestionado porque se considera que no ofrece suficiente protección de la privacidad. Cuando el Acuerdo de Puerto Seguro (antecesor del Escudo de Privacidad) se derogó, se generó una incertidumbre legal para auditores y expertos contables que utilizaban servidores ubicados en los EEUU. Es, por lo tanto, aconsejable para aquellos profesionales que conservan sus datos en servidores ubicados en los EEUU, tengan en cuenta lo anterior y que hagan seguimiento de los desarrollos que anuncie la Comisión Europea, así como los cambios normativos en los EEUU.

---

[13] Comisión Europea, Decisiones de la Comisión relativas a la adecuada protección de los datos personales en terceros países http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

[14] El RGPD será aplicable en mayo de 2018. Ello significa que, si las negociaciones para el Brexit no se han finalizado a esa fecha, Reino Unido seguirá estando sujeto al RGPD hasta que se finalice el proceso de salida.

[15] El escudo de privacidad UE-EEUU está disponible en http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

CONCLUSIÓN

En esta publicación hemos analizado algunas de las obligaciones principales que incluye el RGPD que son aplicables a los auditores y a los expertos contables. Estas nuevas normas probablemente requerirán una revisión de los procesos de tratamiento de datos. Se aconseja a los profesionales que se aseguren de que tienen la especialización necesaria en este tema para llevar a cabo esta revisión.

Las instituciones de la UE y las autoridades de protección de datos locales probablemente publicarán orientaciones sobre cómo cumplir con el RGPD, o ya lo habrán hecho ya. Aconsejamos revisar detenidamente cualquier recomendación de la autoridad de tu país.

Por ejemplo, el grupo de trabajo del artículo 29, que está integrado por las autoridades de protección de datos locales, publicó unas guías sobre delegados de protección de datos, portabilidad y sobre cómo identificar a la autoridad de control principal[16]. Además, la Comisión Belga de Privacidad publicó un folleto con 13 pasos para cumplir con el RGPD[17].

LOS CAMBIOS PRINCIPALES QUE CONLLEVA EL RGPD

Los cambios principales en comparación con la Directiva son:

- Inclusión de los responsables y encargados de fuera de la UE que conservan información personal de ciudadanos de la UE.
- Nuevas obligaciones de responsabilidad proactiva para los responsables dl tratamiento
- Nuevos derechos para los interesados
- El tratamiento, basado en el consentimiento del interesado, se regula de manera más estricta.
- Disposiciones más estrictas en el caso de violaciones de seguridad.
- Introducción de la "ventanilla única" para el control
- La necesidad de notificación o aprobación previa de la Agencia de protección de Datos se ha eliminado en muchas circunstancias.
- Introducción de obligaciones directas para los encargados del tratamiento.

[16] En http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083 hay información disponible sobre el Grupo de Trabajo del Artículo 29

[17] El documento: 13 pasos para prepararse para el RGPD está disponible en: https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

Avenue d'Auderghem 22-28, 1040 Brussel

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 50 professional organisations from 37 countries that represent close to **1 million** professional accountants, auditors, and advisors. They make numbers work for people. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.

Accountancy Europe is in the EU Transparency Register (No 4713568401-18).