Consulta de auditoría 2- BOICAC 120/DICIEMBRE 2019
(Publicada en la página web del ICAC el 20 de diciembre de 2019)

Sobre la aplicación de la normativa reguladora de la protección de datos personales en el ámbito de un trabajo de auditoría de cuentas.

Respuesta

Situación planteada

La cuestión planteada se refiere a si los auditores de cuentas en la realización de sus trabajos de auditoría de cuentas se ven afectados por lo dispuesto en la normativa reguladora de la protección de datos de carácter personal.

Consideraciones:

1.- La protección de datos de carácter personal se encuentra regulada 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 físicas 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 sobre esta materia (Reglamento general de protección de datos, en adelante RGPD), y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDP).

Dicha regulación es aplicable al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a incluir en un fichero, de conformidad con el ámbito de aplicación de dicha normativa establecida en el artículo 2 del RGPD y en las definiciones que a tal efecto se establecen en el artículo 4, apartados 1 y 2, de dicho Reglamento.

2.- Por otra parte, tanto la Directiva 2014/56/UE, de 16 de abril de 2014, por la que se modifica la Directiva 2006/43/CE, relativa a la auditoría legal de las cuentas anuales, como el Reglamento (UE) nº 537/2014, de 16 de abril de 2014, sobre los requisitos específicos para la auditoría legal de las entidades de interés público, contienen menciones expresas a que en el ejercicio de la actividad de auditoría de cuentas debe tenerse en cuenta y aplicarse lo dispuesto en la normativa reguladora de la protección de datos de carácter personal, de forma que resulta necesario compatibilizar ambas regulaciones, la específica en materia de auditoría de cuentas y la general en materia de protección de datos. Así:

La Directiva citada, en su considerando 9 y en su artículo 23, establece:

> *"Considerando (9)*
> *Es importante que los auditores legales y las sociedades de auditoría respeten la vida privada y la protección de los datos de sus clientes. Deben, por lo tanto, regirse por unas normas estrictas de confidencialidad y secreto profesional que, sin embargo, no deben impedir la correcta aplicación de la presente Directiva y del Reglamento (UE) no 537/2014 ni la cooperación con el auditor del grupo durante la auditoría de los estados financieros consolidados cuando la empresa matriz esté domiciliada en un tercer país,*

C/ HUERTAS, 26
28014 MADRID
TEL.: 91 389 56 00
FAX: 91 429 94 86

siempre que se cumpla lo dispuesto en la Directiva 95/46/CE del Parlamento Europeo y del Consejo (1). No obstante, dichas normas no deben permitir que el auditor legal o la sociedad de auditoría coopere con las autoridades de terceros países fuera de los canales de cooperación previstos en el capítulo XI de la Directiva 2006/43/CE. Dichas normas de confidencialidad deben aplicarse asimismo a todo auditor legal o sociedad de auditoría que deje de participar en una tarea de auditoría específica."

Artículo 23

Confidencialidad y secreto profesional

1. Los Estados miembros se asegurarán de que toda la información y documentos a los que tenga acceso el auditor legal o la sociedad de auditoría al realizar una auditoría legal estén protegidos por normas adecuadas de confidencialidad y secreto profesional.

2. Las normas de confidencialidad y secreto profesional relativas a los auditores legales o las sociedades de auditoría no impedirán la aplicación de las disposiciones de la presente Directiva o del Reglamento (UE) n o 537/2014.

(..)

5. …(párrafo final) La transmisión de información al auditor del grupo radicado en un tercer país deberá hacerse en cumplimiento de lo dispuesto en el capítulo IV de la Directiva 95/46/CE y de las normas nacionales aplicables en materia de protección de datos personales.

El citado Reglamento (UE), en su considerando 11 y en el artículo 35 establecen lo siguiente:

"Considerando (11)
La Directiva 95/46/CE del Parlamento Europeo y del Consejo (1) debe regular el tratamiento de los datos personales realizado en los Estados miembros en el marco del presente Reglamento y dicho tratamiento de los datos personales tiene que estar sujeto a la supervisión de las autoridades competentes de los Estados miembros, y en particular de las autoridades públicas independientes designadas por estos. Todo intercambio o transmisión de información efectuado por las autoridades competentes debe cumplir las disposiciones sobre transferencia de datos personales establecidas en la Directiva 95/46/CE."

"Artículo 35. Protección de datos personales

1. Los Estados miembros aplicarán la Directiva 95/46/CE al tratamiento de los datos de carácter personal que se efectúe en los Estados miembros en virtud del presente Reglamento.
2. Se aplicará lo dispuesto en el Reglamento (CE) no 45/2001 al tratamiento de los datos de carácter personal realizado por la COESA, la AEVM, la ABE y la AESPJ en el marco del presente Reglamento y de la Directiva 2006/43/CE.

Por su parte, el artículo 59 del Reglamento de desarrollo del texto refundido de la Ley de Auditoría de Cuentas, aprobado por el Real Decreto 11517/2011, de 31 de octubre, también recoge el sometimiento a la normativa reguladora de la protección de datos personales del tratamiento de dichos datos llevados a cabo por el auditor de cuentas como consecuencia del ejercicio de su actividad. Así:

"Artículo 59. Protección de datos de carácter personal.

El tratamiento de datos de carácter personal llevado a cabo por los auditores de cuentas y sociedades de auditoría como consecuencia del ejercicio de su actividad, incluido el de los datos contenidos en los documentos o papeles de trabajo utilizados para tal fin, se encuentra sometido a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal y sus disposiciones de desarrollo.

En la conservación de los datos a la que se refiere el artículo anterior, los auditores de cuentas y sociedades de auditoría implantarán las medidas de seguridad previstas en la normativa de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre.

En el supuesto en que los auditores de cuentas y sociedades de auditoría externalizase los servicios de conservación y custodia de la documentación deberá darse cumplimiento a lo dispuesto en el artículo 12 de la Ley Orgánica 15/1999."

Es decir, desde la perspectiva de la normativa reguladora de la actividad de auditoría de cuentas se impone a los auditores de cuentas la obligación de aplicar lo establecido en la normativa de protección de datos personales cuando, en el desarrollo de un trabajo de auditoría de cuentas, se traten datos personales, sin que, por otra parte, dicha normativa de protección de datos personales pueda impedir la aplicación de lo exigido por la normativa de auditoría de cuentas.

La base de legitimación para el tratamiento de datos personales se encuentra en el artículo 6.1, apartado e), del RGPD, por cuanto dicho tratamiento de datos personales, en el caso de que la información auditada los contuviese, podría entenderse como necesario para el cumplimiento de una misión realizada en "interés público" o "función de interés público", dada la configuración que de la auditoría de cuentas han realizado tanto las Directivas y Reglamentos comunitarios, como la LAC. Adicionalmente, la base de legitimación podría encontrarse también en lo dispuesto en el artículo 6.1.b) del RGDP, por cuanto hay tratamientos de datos personales necesarios para la ejecución del contrato de auditoría o a las actividades de formación continuada. A estos efectos, la base de dicho tratamiento, de conformidad con lo establecido en el artículo 6.3 RGPD, vendría establecida por el Derecho de la Unión Europea (Directiva 2006/46/UE y Reglamento 537/2014), y la normativa reguladora nacional de la actividad de auditoría de cuentas de desarrollo, que contienen disposiciones específicas que regulan deberes de secreto y confidencialidad, de conservación y custodia, plazos de conservación de datos, limitaciones de uso, etc. En cualquier caso la citada normativa reguladora de la actividad de auditoría de cuentas se remite igualmente a la regulación de protección de datos personales contenida en el RGPD y en la LOPDP, a las que habrá de estarse en todo caso.

3.- En este mismo sentido se ha pronunciado la Agencia Española de Protección de Datos (autoridad supervisora de esta materia en España), indicando que los auditores de cuentas, como cualquier otra persona física o jurídica, están sometidos a la normativa reguladora de protección de datos cuando, en la realización de sus trabajos de auditoría de cuentas, traten datos de carácter de personal, de conformidad con las definiciones de "datos personales" y "tratamiento" establecidas en el artículo 4, apartados 1 y 2, del RGPD, respectivamente. Y en estos casos, la sujeción de los auditores de cuentas a la normativa reguladora de protección de datos lo será en calidad de "**responsables de tratamiento**", dado que determinan los fines y medios del tratamiento de los datos personales en el transcurso de su trabajo de auditoría de cuentas y son independientes de la entidad auditada en la realización de su trabajo, sin que dicho tratamiento se efectué de ningún modo por cuenta de la entidad auditada, cumpliendo así los términos de la definición establecida en el artículo 4.7 del RGPD.

En consecuencia, hay que entender que en el desarrollo de los trabajos de auditoría de cuentas los auditores de cuentas en la medida en que traten datos de carácter personal, en el tratamiento de dichos datos, incluido el de los datos contenidos en los documentos o papeles de trabajo utilizados para tal fin, se encontrarán sometidos a lo dispuesto en el RGPD y la LOPDP, y tal sujeción lo será en calidad de "responsable del tratamiento", por los motivos indicados anteriormente.

4. En este sentido, de acuerdo con lo establecido en los artículos 24 y 25 del RGPD y los artículos 28 y siguientes de la LOPD, referentes a las obligaciones generales y responsabilidad de los responsables de tratamiento de datos, los auditores de cuentas deberán adoptar las medidas técnicas y organizativas apropiadas, atendiendo a la naturaleza, ámbito, contexto y fines del tratamiento.

A este respecto, deben establecerse las medidas de seguridad necesarias, habida cuenta del estado de la tecnología, los costes de aplicación, la naturaleza, alcance, contexto y fines del tratamiento y los riesgos para los derechos y libertades de las personas físicas, a fin de respetar y proteger los intereses y derechos fundamentales del interesado, de conformidad con lo establecido en el RGPD y la LOPDP, y sin olvidar la implantación de las medidas apropiadas para atender, en tiempo y forma, las posibles peticiones de ejercicio de derechos que formulen los interesados.

Las medidas organizativas serán las que, a juicio del auditor, resulten más apropiadas en el contexto de su propia organización y los trabajos de auditoría que realice. Debe tenerse en cuenta que el tratamiento de los datos debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas para proteger los intereses y derechos de los interesados.

Hay que advertir, por otra parte, de que las obligaciones como responsable de tratamiento se basan en un principio de responsabilidad proactiva que debe documentarse para ser capaz de demostrarla, según el artículo 5.2 el RGPD. Dicha responsabilidad proactiva incluye un abanico de medidas tales como la elaboración de un registro de actividades de tratamiento, la realización de un análisis de riesgos, la revisión de las medidas de seguridad a la luz de los resultados del análisis de riesgos, el establecimiento de mecanismos y procedimientos para notificar quiebras de seguridad, la realización, en su caso, de una evaluación de impacto en la protección de datos y la designación, en su caso, de un Delegado de protección de datos. Adicionalmente, deberán actualizarse los formularios informativos sobre el tratamiento de datos a las previsiones del RGPD, así como los mecanismos y procedimientos para el ejercicio de los derechos reconocidos en dicha norma y, elaborar una política de privacidad.

Asimismo, en el supuesto en que los auditores de cuentas externalizasen alguno o algunos de los aspectos de un trabajo de auditoría de cuentas, en su condición de "responsable de tratamiento", deberán establecerse los procedimientos oportunos para dar cumplimiento a lo dispuesto en el RGPD y en la LOPDP en relación con dichos agentes externos y la custodia y conservación de la documentación correspondiente, los cuales tendrán la condición de encargados de tratamiento. A este respecto, debe tenerse en cuenta que el RGPD exige un deber específico de diligencia en la selección de los encargados del tratamiento en lo que respecta al tratamiento de datos personales y que dichas prestaciones de servicios han de vincularse a través de un contrato que establezca garantías suficientes, debiendo adaptarse los contratos ya existentes en los plazos previstos en la Disposición transitoria quinta de la LOPDP. En dicha disposición se prevé que dichos contratos mantendrán su vigencia hasta la fecha de vencimiento señalada en los mismos y, en caso de haberse pactado de forma indefinida, hasta

el 25 de mayo de 2022. En la hoja de ruta señalada a continuación se incluye un enlace para facilitar la adaptación de los contratos al RGPD.

5. Conviene advertir que la Agencia Española de Protección de Datos en su página web facilita información sobre la hoja de ruta a seguir para la adaptación al RGPD, a través de este enlace:

https://www.aepd.es/media/infografias/infografia-adaptacion-rgpd-sector-privado.pdf

Asimismo, en dicha hoja de ruta se recogen enlaces adicionales a guías prácticas e informaciones útiles para la aplicación de diversas medidas de cumplimiento.

Esta Agencia ha publicado en su página web numerosas guías, tanto generales como sectoriales, que indican los criterios a seguir en los distintos aspectos de la aplicación de la normativa de protección de datos para su adecuado cumplimiento entre las que se encuentra la "Guía del RGPD para responsables del tratamiento" que podría facilitar al auditor el cumplimento de la normativa de protección de datos en su calidad de responsable. Asimismo, en esta página web, se ofrecen diferentes herramientas, entre las que se encuentra el canal INFORMA_RGPD, que tiene como finalidad prestar soporte en aquellas dudas y cuestiones que puedan derivarse de la aplicación del RGPD.

6. Por último, debe advertirse que, tal y como se prevé en la normativa reguladora de la actividad de auditoría de cuentas, las obligaciones derivadas de las normas de confidencialidad y secreto profesional, así como de las de protección de datos, no podrán ser argumentadas como justificativas de la no aplicación de lo exigido por las citadas normas de auditoría de cuentas en la realización del trabajo de auditoría. En este sentido y a tales efectos, debe recordarse que la citada normativa reguladora ya prevé las actuaciones a realizar por el auditor en los supuestos en que se pudieran producirse impedimentos o limitaciones a la realización de pruebas o procedimientos de auditoría en el desarrollo de cualquier trabajo de auditoría de cuentas, entre las que se incluirían las que hipotéticamente surgieran de las citadas normas de confidencialidad o de protección de datos. como por ejemplo las Normas Técnicas de Auditoría, resultado de la adaptación de las Normas Internacionales de Auditoría para su aplicación en España (NIA-ES), sobre Informes, integrantes de la serie NIA-ES 700 a 720, y en particular la NIA-ES 705 "Opinión Modificada en el Informe Emitido por un Auditor Independiente".

Conclusiones

7.- Atendiendo a las consideraciones anteriores, este Instituto entiende que **si los auditores de cuentas en el desarrollo de los trabajos de auditoría de cuentas tratan o pueden tratar datos de carácter personal, el tratamiento de dichos datos, incluido el de los datos contenidos en los documentos o papeles de trabajo utilizados para tal fin, se encuentra sometido a lo dispuesto en el RGPD y la LOPDP, actuando los auditores en calidad de "responsable del tratamiento**".

A estos efectos, los auditores de cuentas deberán adoptar las medidas de organización interna necesarias para dar cumplimiento a las obligaciones derivadas de la aplicación de la normativa sobre protección de datos en el desarrollo de sus trabajos de auditoría de cuentas para proteger los intereses y derechos de los interesados, y sin que lo dispuesto en la normativa de protección de datos, o en la de confidencialidad y secreto profesional, pueda aducirse como impedimento a la aplicación de lo exigido por la normativa reguladora de la actividad de auditoría de cuentas.

8.- Conforme a lo establecido en la Disposición Adicional Novena del Real Decreto 1517/2011, de 31 de octubre, por el que se aprueba el Reglamento que desarrolla el texto refundido de la Ley de Auditoría de Cuentas, la presente contestación tiene carácter de información, no pudiéndose entablar recurso alguno contra la misma.