N/REF: 008531/2019

I

Tal y como resulta de su Exposición de Motivos, el proyecto de Real Decreto tiene por objeto dar cumplimiento a la previsión recogida en la disposición final octava de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, por la que se autoriza al Gobierno para que, a propuesta del Ministro de Economía y Competitividad (hoy Ministro de Economía y Empresa, dicte las normas necesarias para el desarrollo de lo dispuesto en esta Ley. A su vez, dicha ley 22/2015, de 20 de julio, de Auditoría de Cuentas (en adelante, ley 22/2015) tiene como objetivo principal adaptar la legislación interna española a los cambios incorporados por la Directiva 2014/56/UE del Parlamento Europeo y del Consejo, de 16 de abril de 2014, por la que se modifica la Directiva 2006/43/CE del Parlamento Europeo y del Consejo, de 17 de mayo de 2006, relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, en lo que no se ajusta a ella. Junto a dicha Directiva, se ha aprobado el Reglamento (UE) n.º 537/2014, del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre los requisitos específicos para la auditoría legal de las entidades de interés público y por el que se deroga la Decisión 2005/909/CE de la Comisión.

Es en dichas normas europeas, por lo tanto, donde habrá que fijarse para determinar cuál es la regulación que realizan en la materia específica a que este informe ha de ceñirse, que es la regulación de la protección de los datos personales que de una u otra manera se ven afectados por la actividad de la Auditoría de cuentas.

Así las cosas, es de ver cómo la Directiva citada 2014/56/UE contiene menciones expresas a la necesidad de compatibilizar ambas regulaciones, la específica en materia de auditoría legal y la general en materia de protección de datos. En concreto, su considerando (9) dice así:

> *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,* ***siempre que se cumpla lo dispuesto en la Directiva 95/46/CE del Parlamento***

> ***Europeo y del Consejo.*** *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.*

Se observa, por lo tanto, una primera conclusión, y es que la existencia de unas normas específicas en materia de auditoría no impide el cumplimiento, además, en su integridad, de la normativa en materia de protección de datos personales siempre que, en el devenir de la actividad auditora, ya sea por los auditores o sociedades de auditoría, o como luego veremos, por las propias autoridades reguladoras en materia de auditoría, se vean afectados datos personales. Ello incluye incluso los casos de cooperación internacional en los que se planteen intercambios de información sobre papeles de trabajo de los auditores entre las autoridades competentes de un Estado miembro o de terceros países. Así, el considerando (26) de la Directiva 2014/56/UE establece:

> *Con el fin de preservar los derechos de las partes interesadas en los casos en que las autoridades competentes de un Estado miembro cooperen con las de terceros países intercambiando papeles de trabajo de auditoría u otros documentos pertinentes para la evaluación de la calidad de las auditorías realizadas, los Estados miembros deben velar por que los acuerdos de cooperación suscritos por sus autoridades competentes y que sirvan de base para ese intercambio de documentación incluyan salvaguardias suficientes para proteger los secretos empresariales y los intereses comerciales, incluidos los derechos de propiedad industrial e intelectual, de las entidades auditadas.* ***Los Estados miembros deben velar por que dichos acuerdos cumplan y sean compatibles con las disposiciones de la Directiva 95/46/CE****.*

Es decir, tal y como se pone de relieve en estos preceptos, no es suficiente con que la actividad de los auditores o sociedades de auditoría, y de las autoridades competentes de supervisión, (en España el Instituto de Contabilidad y Auditoría de cuentas -ICAC-) se ajuste a las normas concretas de auditoría, sino que ello no excluye que las actuaciones que lleven a cabo hayan de cumplir igualmente, en todo caso, con la normativa de protección de datos personales. Como veremos, esta necesidad es una constante en la regulación para cuyo desarrollo se dicta el proyecto de Real Decreto sometido a informe, y que, por lo tanto, este habrá de respetar.

Ello se pone de manifiesto igualmente en el Reglamento (UE) nº 537/2014 del Parlamento Europeo y del Consejo, de 16 de abril de 2014, sobre

los requisitos específicos para la auditoría legal de las entidades de interés público y por el que se deroga la Decisión 2005/909/CE de la Comisión, igualmente desarrollada por la ley 22/2015, y en consecuencia por el Proyecto de Real Decreto sometido a Informe. El considerando (11) dice así:

> *La Directiva 95/46/CE del Parlamento Europeo y del Consejo 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.*

El Reglamento citado, específico en materia de auditoría de entidades de interés público, plasma dichos principios en los artículos 23.6, 35 y 36:

> *23.6 El tratamiento de datos de carácter personal en el ejercicio de las facultades de supervisión e investigación estipuladas en el presente artículo se llevará a cabo de conformidad con 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.*
>
> *Artículo 36*
> *1. Las autoridades competentes podrán celebrar acuerdos de cooperación para el intercambio de información con las autoridades competentes de terceros países, siempre y cuando la información comunicada esté sujeta, en los terceros países en cuestión, a garantías de secreto profesional equivalentes al menos a las establecidas en los artículos 22 y 34. Las autoridades competentes comunicarán dichos acuerdos de inmediato a la COESA y los notificarán a la Comisión.*
> *Solo se intercambiará información al amparo del presente artículo cuando ese intercambio sea necesario para que las autoridades competentes de que se trate puedan ejercer las funciones que les asigna el presente Reglamento.* ***Cuando el intercambio de información implique la transferencia de datos personales a un tercer país, los Estados miembros deberán respetar la Directiva 95/46/CE****, y la COESA deberá respetar el Reglamento (CE) nº 45/2001.*

Estas circunstancias -esto es, el hecho de que el marco jurídico específico de la auditoría podría afectar, en determinados casos, a los

derechos de las personas en cuanto a sus datos personales- ya fue puesto de manifiesto igualmente por el Supervisor Europeo de Protección de Datos (SEPD) en su Dictamen sobre las propuestas de la Comisión relativas a una Directiva por la que se modifica la Directiva 2006/43/CE relativa a la auditoría legal de las cuentas anuales y de las cuentas consolidadas, y al Reglamento sobre los requisitos específicos para la auditoría legal de las entidades de interés público (Dictamen cuyo resumen se publicó en el DOUE C 336, de 6 de noviembre de 2012). Así, entre las recomendaciones de su Dictamen, en el apartado 47, el SEPD sostuvo:

> *- dar una nueva redacción al artículo 56 de la propuesta de Reglamento e incorporar una disposición en la Directiva 2006/43/CE que la que se subraye la* ***plena aplicabilidad de la legislación existente en materia de protección de datos y sustituir las múltiples referencias en diferentes artículos de la propuesta de Reglamento por una disposición general que remita tanto a la Directiva 95/46/CE*** *como al Reglamento (CE) nº 45/2001. El SEPD sugiere clarificar la referencia a la Directiva 95/46/CE, especificando que las disposiciones se aplicarán conforme a las normas nacionales en virtud de las cuales se transpone dicha Directiva,*

II

La Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos fue derogada por el ya citado 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 (Reglamento General de Protección de Datos, RGPD).

Esta norma, el RGPD, es de aplicación transversal, aplicable a todos los tratamientos de datos, salvo en aquellos casos expresamente excluidos de su aplicación por el propio RGPD. Su artículo 2 establece su ámbito de aplicación material:

> *1. El presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero".*
> *2. El presente Reglamento no se aplica al tratamiento de datos personales:*

a) en el ejercicio de una actividad no comprendida en el ámbito de aplicación del Derecho de la Unión;
b) por parte de los Estados miembros cuando lleven a cabo actividades comprendidas en el ámbito de aplicación del capítulo 2 del título V del TUE;
c) efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas;
d) por parte de las autoridades competentes con fines de prevención, investigación, detección o enjuiciamiento de infracciones penales, o de ejecución de sanciones penales, incluida la de protección frente a amenazas a la seguridad pública y su prevención.

Ninguna de estas circunstancias excluyentes del apartado 2 puede entenderse que aplica en los tratamientos que se realizan en el ámbito de la auditoría legal, por lo que, siempre que existan tratamientos de datos personales en el ejercicio de la actividad auditora o supervisora, dichos tratamientos estarán sujetos al RGPD.

El art. 4 RGPD define, entre otros términos, "datos personales" y "tratamiento de datos".

«datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

«tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

Será sobre estas bases -y ciertamente sobre el resto del contenido del RGPD- que se examinarán los distintos tratamientos de datos que se puedan contener en el proyecto de Real Decreto sometido a informe para determinar su adecuación a la normativa de protección de datos personales.

Pero es necesario hacer desde ya una precisión: los auditores legales y sociedades de auditoría, así como el ICAC en tanto que autoridad supervisora, en cuanto que personas y/o entidades que tratan datos personales, están

sometidos, como “responsables de los tratamientos” -y a continuación ahondaremos un poco en este concepto- al RGPD en su integridad en los tratamientos de datos personales que realizan. En consecuencia, los auditores y sociedades de auditoría y el ICAC deberán de tener en cuenta la regulación que contiene el RGPD en cualesquiera tratamientos de datos personales, de modo que, con independencia de la normativa propia de la Auditoría (Directiva 2006/43/CE, Directiva 2014/56/UE, Reglamento (UE) 537/2014, Ley 22/2015, de 20 de julio, de Auditoría de Cuentas o el Real Decreto presentado a Informe), su actividad está sujeta igualmente a esta parcela del derecho.

Lo anterior puede verse con claridad, a modo de ejemplo, -sin perjuicio de que más adelante nos referiremos también a ella-, en la Decisión de Ejecución (UE) 2016/1010, de la Comisión, de 21 de junio de 2016 sobre la adecuación de las autoridades competentes de determinados terceros países y territorios con arreglo a la Directiva 2006/43/CE del Parlamento Europeo y del Consejo. Como establece el considerando (1) de dicha Decisión de ejecución:

> *Con arreglo al artículo 47, apartado 1, de la Directiva 2006/43/CE, las autoridades competentes de los Estados miembros únicamente pueden permitir el envío a las autoridades competentes de un tercer país de papeles de trabajo de auditoría u otros documentos que obren en poder de auditores legales o sociedades de auditoría autorizados por ellos, así como de informes de inspección o investigación relativos a las auditorías de que se trate, cuando dichas autoridades cumplan requisitos que la Comisión haya declarado adecuados y existan* ***acuerdos de trabajo basados en la reciprocidad*** *entre tales autoridades y las de los Estados miembros correspondientes*

Pues bien, el considerando (9) de la misma reconoce que para la transferencia de datos a estos países reconocidos de acuerdo con la Directiva 2006/43/CE no es suficiente que existan dichos acuerdos de trabajo basados en la reciprocidad propios de la normativa de auditoría, sino que habrán de cumplirse los requisitos que para dicha transferencia internacional de datos a terceros países (no miembros de la UE) exige la normativa de protección de datos.

> *(9) Cuando el envío de papeles de trabajo de auditoría u otros documentos en poder de auditores legales o sociedades de auditoría y de informes de inspección o investigación a las autoridades competentes del tercer país o territorio de que se trate suponga la divulgación de datos personales,* ***tal divulgación únicamente es lícita si cumple asimismo los requisitos para las transferencias internacionales de datos establecidos en la Directiva 95/46/CE del Parlamento Europeo y del Consejo****. Por consiguiente,* ***el artículo 47, apartado 1, letra e), de la Directiva 2006/43/CE obliga a los Estados miembros a garantizar que el intercambio de datos personales***

entre sus autoridades competentes y las del tercer país o territorio de que se trate se atenga a lo dispuesto en el capítulo IV de la Directiva 95/46/CE*. Los Estados miembros deben velar por que existan salvaguardias adecuadas para la protección de los datos personales transmitidos, en caso necesario establecidas mediante acuerdos vinculantes, y que a su vez las autoridades competentes del tercer país o territorio no divulguen los datos personales incluidos en los documentos enviados sin el acuerdo previo de las autoridades competentes de los Estados miembros de que se trate.*

III

El RGPD distingue entre responsables y encargados del tratamiento.

Es «responsable del tratamiento» o «responsable» la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros. Y «encargado del tratamiento» o «encargado» es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento. (art. 4.7 y 4.8 RGPD).

El artículo 28.3 del citado Reglamento regula dicha figura y exige en su número tercero la existencia de un contrato u otro acto jurídico con arreglo al derecho de la Unión o de los Estados miembros que vincule al encargado respecto del responsable. Entre las determinaciones que debe contener dicho contrato se recoge en primer lugar la estipulación de que el encargado "*tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público*"

De este modo, teniendo en cuenta las definiciones de responsable y encargado del tratamiento contenidas en el artículo 4 del RGPD, así como la regulación que del encargado del tratamiento se efectúa en su artículo 28, debe considerarse que el criterio definidor de la condición de responsable del tratamiento viene dado por la potestad de determinar los fines y los medios del tratamiento, en tanto que el encargado debe limitar su actuación a seguir las instrucciones del responsable.

La determinación de si los auditores legales o las sociedades de auditoría han de ser consideradas responsables o encargados del tratamiento ya se planteó en el Informe de esta AEPD 258043/2011 en relación con el Proyecto de Real Decreto por el que se aprobó el Reglamento de desarrollo de la Ley 19/1988, de 12 de julio de Auditoría de Cuentas.

El referido informe señalaba lo siguiente:

<<Antes de entrar en el análisis detallado del contenido del Proyecto sometido a informe debe igualmente efectuarse una consideración previa en relación con la naturaleza del auditor de cuentas en el ejercicio de su actividad en lo que se refiere a la aplicación de las normas de protección de datos de carácter personal.

En este sentido, el artículo 3 d) de la Ley Orgánica 15/1999 define al responsable del fichero o tratamiento como "Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento". Por su parte, conforme al artículo 3 g) es encargado del tratamiento "La persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento".

La delimitación entre una y otra figura se fundamenta en el hecho de que mientras el responsable lleva a cabo el tratamiento en nombre propio, manteniendo, en su caso, una relación directa con el afectado al que se refieren los datos, el encargado del tratamiento se limita a tratar los datos en cumplimiento del encargo expresamente conferido por el responsable, no manteniendo dicha relación directa con el afectado y limitando su actividad a las instrucciones en virtud de las cuales el encargado es conferido de esta condición.

Pues bien, en el presente supuesto podría plantearse la hipótesis de que el auditor de cuentas mantiene en relación con la entidad auditada la condición de encargado del tratamiento, dado que la actividad desarrollada por el auditor se deriva de la existencia de un contrato celebrado con dicha entidad, regulado por el artículo 8 del Proyecto sometido a informe, cuyo apartado 1 señala en su segundo párrafo que "el contrato de auditoría de cuentas anuales ha de formalizarse por escrito e incluirá, de conformidad con la normativa reguladora de la actividad de auditoría de cuentas, al menos, la identificación de las cuentas anuales objeto de auditoría y los aspectos relevantes del trabajo de auditoría a realizar, referidos al período de contratación, los honorarios, finalidad o razón por la que se realiza el encargo y plazo de entrega del informe de auditoría".

No obstante, cabe considerar que el régimen establecido a lo largo del Texto refundido y del Proyecto sometido a informe pone de manifiesto que la actividad de auditoría de cuentas no puede sin más ser considerada como la propia de un encargado, asumiendo el auditor funciones que le identifican en mayor medida con las de un responsable del tratamiento.

En particular, el artículo 12.2 de la Ley Orgánica 15/1999 establece que "La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas".

Además, según el artículo 12.3 "una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento".

Pues bien, las normas reguladoras del ejercicio de la actividad de auditoría de cuentas vienen a contradecir las obligaciones derivadas de los preceptos citados, por cuanto el auditor deberá, por un lado, mantener una absoluta independencia de la entidad auditada y, por otra, conservar la información y papeles de trabajo obtenidos, manteniéndolos a disposición de las autoridades competentes para el control y supervisión, en los términos que se analizarán a lo largo del presente informe.

Así, respecto de la independencia, el artículo 22.1 de la Directiva 2006/43/CE dispone que "Los Estados miembros se asegurarán de que, cuando se realice una auditoría legal, el auditor legal y/o la sociedad de auditoría sean independientes de la entidad auditada y no participen en el proceso de toma de decisiones de la misma", indicando el considerando 11 de su Exposición de Motivos que "Los auditores legales y las sociedades de auditoría deben ser independientes cuando realicen auditorías legales. Podrán informar a la entidad auditada de los asuntos derivados de la auditoría, pero deben abstenerse de participar en los procesos de toma de decisiones internos de la entidad auditada. Si se encontraran en una situación en la que la importancia de las amenazas para su independencia, incluso tras la aplicación de salvaguardias para mitigarlas, fuera demasiado grande, deben renunciar al contrato de auditoría o abstenerse de ejecutarlo".

Del mismo modo, el artículo 25 de la Directiva añade que "Los Estados miembros se asegurarán de que existan las normas adecuadas que establezcan que los honorarios para las auditorías legales: a) no están influidos o determinados por la prestación de servicios adicionales a la entidad auditada; b) no puedan basarse en ningún tipo de contingencia".

Así, el artículo 12.1 del Texto Refundido añade en su primer párrafo que "Los auditores de cuentas y las sociedades de auditoría deberán ser independientes, en el ejercicio de su función, de las entidades auditadas, debiendo abstenerse de actuar cuando su independencia en relación con la revisión y verificación de las cuentas anuales, los estados financieros u otros documentos contables pudiera verse comprometida".

Por este motivo, concluye el artículo 8 del texto sometido a informe que en el contrato no será posible "que puedan establecerse limitaciones al desarrollo del trabajo de auditoría ni estipulaciones contrarias a lo establecido en la citada normativa ni restricciones a la distribución o utilización del informe de auditoría".

A la vista de todo ello, cabe considerar que los auditores de cuentas tendrán, desde la perspectiva de la aplicación de las normas de protección de datos, la condición de responsables del tratamiento de datos de carácter personal que lleven a cabo en el ejercicio de su actividad. Ello conllevará que los mismos queden sometidos a la totalidad de las disposiciones de la Ley Orgánica 15/1999, debiendo proceder a la notificación de los ficheros generados en el ámbito de su actividad al registro General de Protección de Datos.

En el mismo sentido, los auditores de cuentas se encontrarán obligados por los principios contenidos en la Ley Orgánica 15/1999 y por los deberes impuestos en la misma, debiendo, en su caso, atender las solicitudes de ejercicio de los derechos de acceso, rectificación, cancelación y oposición, así como implantar en el tratamiento de los datos las medidas de seguridad establecidas en el Título VIII del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre.>>

Aunque parece clara, en principio, la distinción entre encargado y responsable del tratamiento, en la práctica no es así en todos los casos. Lo esencial es que el encargado actúa en nombre y por cuenta del responsable en el tratamiento de los datos, de modo que el RGPD establece la ficción jurídica de que, dado que el encargado no decide los fines y medios del tratamiento, la cesión de datos que en realidad se realiza mediante el encargo (el tratamiento), no es tal jurídicamente. En definitiva, la relación entre el encargado y el responsable es consecuencia de la existencia de una relación jurídica que le

vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio.

No obstante, en el caso presente, no se produciría una actuación del auditor o sociedad de auditoría como encargado del tratamiento, sino que este incorpora los datos personales recabados para sus propios fines, y es él, el auditor o sociedad de auditoría, quien decide la forma de llevar a cabo el servicio de auditoría encomendado de conformidad con el elenco de normas por las que han de regirse la actividad de auditoría, que no se aplica a la sociedad auditada. En definitiva, el auditor emplea la información obtenida (entre ello, los datos personales) para sus propios fines, integrándola finalmente para la prestación del servicio. Si bien el auditor es cesionario de los datos personales necesarios para el ejercicio de su actividad, no trata estos de conformidad a las "instrucciones" recibidas del cliente, sino que los integra en su propia actividad, que por definición es *independiente* de la del cliente, y dicha utilización es en nombre propio (como auditor) y por cuenta propia (pues la actuación del auditor se sujeta a las leyes y reglamentos propios así como a las normas de auditoría, de ética e independencia y de control de calidad interno de los auditores de cuentas y sociedades de auditoría -art. 2 ley 22/2015-) normas a las que no está sujeto el cliente (la sociedad auditada) sino el propio auditor, quien como resultado final deberá emitir un informe de auditoría a la sociedad auditada, informe este que la sociedad auditada no puede emitirse a sí misma.

En la actualidad, el artículo 14.1 de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, relativo al principio general de independencia al que resulta obligado todo auditor, reproduce lo señalado en el derogado Texto Refundido de la Ley de Auditoría de Cuentas, aprobado por el Real Decreto Legislativo 1/2011, de 1 de julio, y dispone que, *"Los auditores de cuentas y las sociedades de auditoría deberán ser independientes, en el ejercicio de su función, de las entidades auditadas, debiendo abstenerse de actuar cuando su independencia en relación con la revisión y verificación de las cuentas anuales, los estados financieros u otros documentos contables se vea comprometida.*" Esta obligación de independencia, junto con la necesidad de que el auditor pueda tener acceso en todo caso a la información (lo que puede incluir datos personales) necesaria para el ejercicio para realizar los trabajos de auditoría de cuentas, y, es más, la obligación que los auditores tienen de requerir cuanta información precisen para la emisión del informe de auditoría de cuentas (art. 6 ley 22/2015), para integrarse como resultado de su trabajo en un informe de auditoría cuyos métodos de obtención son propios del trabajo de auditoría e independiente de las instrucciones del cliente, hacen que no pueda considerarse al auditor de cuentas como un encargado del tratamiento.

En efecto, entre otros, el art. 28 de la ley 22/2015 establece los requisitos que han de cumplir los auditores o sociedades de auditoría como

procedimientos de trabajo para llegar al informe de auditoría, todo lo cual es independiente del cliente (la sociedad auditada).

> ***Artículo 28. Organización interna.***
> *1. Los auditores de cuentas y las sociedades de auditoría dispondrán de* ***procedimientos administrativos y contables fiables, de procedimientos de valoración de riesgo eficaces, de mecanismos operativos que permitan asegurar el control y la protección de sus sistemas informáticos, así como de los mecanismos internos de control de calidad, que garanticen el cumplimiento de las decisiones y procedimientos en el seno de la estructura funcional del auditor de cuentas*** *y en todos los niveles de la sociedad de auditoría.*
> *2. Los auditores de cuentas y las sociedades de auditoría implantarán un sistema de* ***control de calidad interno*** *que garantice la calidad de la auditoría de cuentas de conformidad con lo establecido en las normas de control de calidad interno a las que se refiere el artículo 2. (…)*

En definitiva, dado que es el auditor legal quien verdaderamente determina los fines y los medios del tratamiento, no puede considerarse al auditor como un encargado del tratamiento de la sociedad auditada.

IV

Antes de pasar a los comentarios sobre los artículos del proyecto de Real Decreto, cabe resaltar que en el seno de las relaciones de auditoría se producen una multitud de tratamientos de información, que pueden incluir datos personales: sociedad auditada-auditor; auditor-afectado (persona física cuya información -datos personales- son/pueden ser tratados por el auditor en el ejercicio de sus funciones); auditor-auditor (por ejemplo, de grupo consolidado, o sustituto del anterior); autoridad supervisora (ICAC)-entidad auditada; ICAC-auditor; ICAC-persona afectada, (pues esos datos personales que quizás se hayan recogido en los papeles de trabajo de los auditores pueden ser revisados por la autoridad supervisora); ICAC-autoridad supervisora de otro Estado miembro de la UE, o de un tercer país; auditor-autoridad supervisora de otro Estado miembro de la UE, o de un tercer país, que solicita información, por ejemplo sobre auditorías consolidadas, etc.

En todas estas relaciones, como ya se ha manifestado, es esencial el cumplimiento de la normativa de protección de datos personales. Dado que la actividad de auditoría puede abarcar un amplísimo abanico de empresas y sectores, no es de descartar que los datos personales que hayan de ser auditados puedan incluir datos cuyos tratamientos quepa incluirlos en **categorías especiales de datos personales**. Ello supone que, en esos casos,

el tratamiento de dichos datos habrá de contar no sólo con la base jurídica correspondiente del art. 6 RGPD, sino que al menos también deberá concurrir alguna de las circunstancias previstas en el art. 9.2 RGPD.

La actividad de auditoría, tal y como resulta de la Directiva 2014/56/UE, del Reglamento (UE) 537/2014 y por último por la ley 22/2015, (véase la Exposición de motivos de esta última)

> *(…) por su* ***contribución a la transparencia y fiabilidad de la información económico financiera de las empresas y entidades auditadas, constituye un elemento consustancial al sistema de economía de mercado*** *recogido en el artículo 38 de la Constitución. Así, se configura como aquella que, mediante la utilización de determinadas técnicas de revisión, tiene por objeto la emisión de un informe acerca de la fiabilidad de la información económica financiera auditada, sin que se limite a la mera comprobación de que los saldos que figuran en sus anotaciones contables concuerdan con los ofrecidos en las cuentas que se auditan, ya que las técnicas de revisión y verificación aplicadas permiten, con un alto grado de certeza, dar una opinión técnica e independiente sobre la contabilidad en su conjunto y, además, sobre otras circunstancias que, afectando a la vida de la empresa, no estuvieran recogidas en dicho proceso.*
>
> *La actividad de auditoría de cuentas se caracteriza por* ***la relevancia pública que desempeña al prestar un servicio a la entidad revisada y afectar e interesar no sólo a ésta, sino también a los terceros que mantengan o puedan mantener relaciones con la misma****, habida cuenta de que todos ellos, entidad auditada y terceros, pueden conocer la calidad de la información económica financiera auditada sobre la cual versa la opinión de auditoría emitida.*

Nos encontramos por lo tanto con una actividad regulada en el Derecho de la UE, y nacional, en este último caso mediante una ley. Los datos personales que pudieran estar incluidos en dichas categorías especiales reguladas en el art. 9 RGPD podrían ser tratados para los fines de auditoría siempre que, y sólo en el caso de que, dicho tratamiento sea necesario por razones de un *interés público esencial*, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser *proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos* y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado (art. 9.2.g) RGPD). Cabe considerar que, siempre que se cumplan dichos requisitos de necesidad y proporcionalidad, y estableciéndose en la norma medidas adecuadas y específicas para proteger intereses y derechos fundamentales del interesado, cabría el interés público como circunstancia que permitiría, dentro de las previstas por el art. 9.2 RGPD, el tratamiento de categorías especiales de datos personales. Por ello, se considera conveniente que en el **art. 74 del Reglamento objeto del Proyecto**

de Real Decreto -que es la norma ahora informada- se contemplen las **medidas "adecuadas y específicas"** (sic: **art. 9.2.g) RGPD**) para proteger los intereses y derechos fundamentales del interesado a que hace referencia el citado art. 9.2.g) RGPD que permita al auditor o sociedad de auditoría el tratamiento de categorías especiales de datos personales, y no limitarse a remitirse genéricamente al RGPD y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD). Dichas medidas podrían ser, entre otras sin carácter exhaustivo a considerar para dar cumplimiento al art. 9.2.g) RGPD, las de no reutilización de la información fuera del ámbito específico de la auditoría que se está llevando a cabo, el establecimiento de medidas de seguridad específicas para categorías especiales de datos cuando estos sean objeto de tratamiento por los auditores etc.

V

Los artículos 16 a 18 del proyecto de reglamento sometido a informe tratan sobre la auditoría de las cuentas consolidadas.

Si se observa el texto de la Directiva 2006/43/CE, modificada por la Directiva 2014/56/UE, y la ley 22/2015, vemos que esta última establece unas obligaciones de supervisión para el auditor de las cuentas consolidadas mayores que la que establece la propia Directiva en su artículo 27.1, por cuanto la ley establece la obligación en todo caso para el auditor del grupo consolidado, no sólo de asumir la plena responsabilidad respecto del informe de auditoría de cuentas consolidado, sino que las obligaciones que la Directiva en los apartados b) y c) del artículo 27.1 les impone respecto de la revisión y evaluación de los trabajos de auditoría realizados por auditores de terceros países a efectos de la auditoría del grupo, la ley 22/2015 no lo restringe a los trabajos realizados por auditores de dichos terceros países, sino que la evaluación y revisión del trabajo de auditoría realizado por otros auditores de cuentas se extiende a todos ellos, incluso a los llevados a cabo en el propio Estado, y no sólo a los trabajos que se realicen por un auditor en un Estado de la Unión Europea o en un tercer país (ver art. 7.4 ley 22/2015).

El reglamento sometido a informe es consistente con la visión legal y regula en detalle los aspectos y documentación que los auditores del grupo consolidado han de reflejar en sus papeles de trabajo respecto de las labores realizadas por los auditores de las compañías del grupo consolidable.

La ley, en su artículo 7.4, regula la necesidad de un acuerdo previo entre el auditor de las cuentas consolidadas y los auditores de las sociedades del grupo para que el primero pueda disponer de toda la documentación necesaria para la realización de la auditoría de las cuentas consolidadas, y ello también

para permitir en su caso la revisión y el control del trabajo realizado por el auditor de las cuentas consolidadas por parte del ICAC.

El art. 18 del proyecto sometido a informe regula el caso de la inexistencia de acuerdo para el intercambio de información con los auditores de un tercer país.

Se trata en definitiva de tratamientos de datos específicos, que en algunos casos podrán proceder de terceros países (esto es, no miembros de la UE), en cuyo caso se aplicarán además las previsiones establecidas en la Directiva 2014/56/UE y en la ley 22/2015 -que remiten al RGPD- para los supuestos de cooperación internacional. Así, el artículo 23.5 de la Directiva 2006/43/CE, en su redacción dada por la Directiva 2014/56/UE, dice: *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.* Hoy día, la referencia al capítulo IV de la Directiva 95/46/CE, que llevaba por título “Transferencia de datos personales a países terceros” hay que entenderla sustituida por una referencia a la regulación contenida en el capítulo V del RGPD, que lleva por título “Transferencias de datos personales a terceros países u organizaciones internacionales”.

Respecto de los tratamientos de datos en sí mismo considerados, mediante los cuales el auditor de una empresa incluida en el grupo consolidado transmite datos personales al auditor de las cuentas consolidadas, -prescindiendo en este momento del aspecto de transferencia internacional, que, siempre que sea aplicable habrá de cumplirse igualmente- el acceso por el auditor del grupo consolidado a la información a la que hubieran accedido los auditores de la sociedad que forma parte de dicho grupo consolidado se consideran tratamientos de datos que, como con carácter general cabe predicar en el presente sector de auditoría, la base jurídica para licitud de su tratamiento podría encontrarse en el apartado e) del art. 6.1 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”, dada la configuración que de la auditoría legal han realizado tanto las Directivas y Reglamentos comunitarios, como la ley 22/2015. La base de dicho tratamiento, de conformidad con lo establecido en el art. 6.3 RGPD, ha sido establecida por el Derecho de la Unión (Directivas y Reglamento 537/2014), y el grupo normativo que regula el sector de la auditoría contiene disposiciones específicas que regulan los plazos de conservación de datos, las operaciones y los procedimientos del tratamiento, medidas que han de cumplir los auditores en materia de control de calidad, normas de ética, escepticismo profesional etc. que influyen en los tratamientos de datos personales. De todas maneras, y, en cualquier caso, la normativa se remite igualmente a la regulación de protección

de datos personales contenida en las normas generales RGPD, a las que habrá de estarse en todo caso.

VI

La sección 1ª del capítulo II (arts. 20 a 26) hace referencia al Registro Oficial de Auditores de Cuentas (ROAC).

Ya en el informe 258043/2011 emitido por esta AEPD se tuvo la oportunidad de examinar estos apartados desde la perspectiva de la normativa entonces en vigor, LOPD 15/1999. La ley 22/2015 ha dado nueva redacción a los preceptos del ROAC, en coordinación con las modificaciones introducidas por la Directiva 2014/56/UE en la Directiva 2006/43/CE.

En este caso, el tratamiento de datos se produce al inscribir los datos correspondientes, y posteriormente al ser público el Registro (art. 8.2 ley 22/2015), al permitir su examen por el público en general, por medios electrónicos.

Se considera que los tratamientos de datos personales que resultan de la publicidad registral están amparados igualmente por el interés público, previsto en el art. 6.1.e) del RGPD al que se ha hecho referencia.

Ahora bien, hay que hacer una mención específica al artículo 25 apartado 3 del proyecto de reglamento sometido a Informe, que dice así:

> *El Instituto de Contabilidad y Auditoría de Cuentas pondrá a disposición del Registro Mercantil Central, de la Dirección General de los Registros y del Notariado, y del Decanato de los Juzgados, las relaciones de auditores de cuentas y sociedades de auditoría a los efectos de lo establecido en los artículos 355 y 356, respectivamente, del Reglamento del Registro Mercantil, aprobado por Real Decreto 1784/1996, de 19 de julio y en el artículo 40 del Código de Comercio.*
>
> *Dichas listas, que podrán consultarse por medios telemáticos, incluirán, además de las sociedades de auditoría, a aquellos auditores de cuentas inscritos en situación de ejercientes* ***que no hayan manifestado*** *expresamente su voluntad de estar excluidos de las citadas relaciones****,*** *y que estén en situación que les permita ejercer la actividad de auditoría de cuentas.*
>
> *En dichas listas figurarán las direcciones de las oficinas abiertas en las que los auditores de cuentas o sociedades de auditoría efectivamente ejerzan su actividad.*

La Memoria de Análisis de Impacto Normativo (MAIN) aportada con la documentación correspondiente a la solicitud de informe señala que este artículo se corresponde con el artículo 31 del vigente reglamento, y hace una serie de precisiones de las que cabe destacar ahora la de que se ha suprimido del texto del proyecto de reglamento el apartado 5 del artículo 31 del reglamento vigente ya que por la modificación del artículo 27 de la ley concursal por la ley 17/2014 ya no se hace referencia a la remisión de la lista de auditores por parte del ICAC puesto que ya nos exige que el líquido sea un auditor de cuentas.

Pues bien, si bien es cierto que el texto transcrito del art. 25.3 es similar al existente en el reglamento vigente, su apreciación ha de ser diferente a la que en su momento se tuvo en cuenta con la LOPD 1999.

La base jurídica del tratamiento de datos previstos en dicho apartado es, como puede observarse, el *consentimiento tácito* de los auditores de cuentas, en cuanto que la transmisión de los datos personales al Registro Mercantil Central, DGRN y Decanato del Juzgado, o la posibilidad de consulta a través de medios informáticos, se realiza respecto de aquellos que **no** hayan manifestado expresamente su voluntad de estar excluidos de dichas listas. Si bien la redacción original del reglamento actualmente vigente podría encontrar acomodo en la regulación anterior (art. 14.2 del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre, RLOPD) que permitía el consentimiento que se denominó “tácito”, el RGPD no considera dicha posibilidad, ya que requiere que el consentimiento se preste mediante una “declaración o clara acción afirmativa” (art. 4.11, RGPD). El Considerando (32) del RGPD dice:

> *El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. Esto podría incluir marcar una casilla de un sitio web en internet, escoger parámetros técnicos para la utilización de servicios de la sociedad de la información, o cualquier otra declaración o conducta que indique claramente en este contexto que el interesado acepta la propuesta de tratamiento de sus datos personales. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. (…)*

En consecuencia, y dado que la normativa de protección de datos personales se aplica exclusivamente a las personas físicas (art. 1.2 RGPD), no se considera conforme al RGPD la redacción del segundo párrafo del apartado tercero del art. 25 del proyecto de reglamento sometido a informe, ya que no

puede basarse dicho tratamiento de datos en que consiste la cesión de los datos personales de los auditores, en el hecho de que estos no hayan manifestado expresamente su voluntad de estar excluidos. Debería preverse, al menos por lo que hace a los auditores personas físicas, que dicho consentimiento se exprese de manera positiva, tal y como de manera similar, por ejemplo, constaba en el apartado 5 del artículo 31 del reglamento de auditoría actualmente vigente, que ha sido suprimido en el proyecto sometido a informe, y que decía lo siguiente, y que actualmente sigue en el proyecto sometido a informe, con carácter transitorio, en la Disposición Transitoria sexta:

> *Hasta que entre en vigor el desarrollo reglamentario del artículo 27 de la Ley 22/2003, de 9 de julio, Concursal, el Instituto de Contabilidad y Auditoría de Cuentas remitirá al Decanato de los Juzgados, las relaciones de las personas físicas, en situación de ejercientes, y jurídicas inscritas en el Registro Oficial de Auditores de Cuentas* ***que hayan manifestado su disponibilidad para ser nombrados*** *administradores concursales.*

VII

Los artículos 27 a 36 desarrollan la ley 22/2015 en lo relativo a los requisitos de formación -entendida en sentido amplio- que han de reunir los auditores para el ejercicio de su profesión. Así, han de seguir programas de enseñanza teórica previos a la autorización para el ejercicio, también han de seguir una determinada formación práctica, y un examen de aptitud, que se regulan el artículo 29 del proyecto de reglamento sometido a informe. Con posterioridad, y en desarrollo de lo dispuesto en el artículo 8.7 de la ley 22/2015, se requiere que los auditores sigan con una determinada formación continuada que les mantenga al tanto de las novedades y que en general garanticen el correcto cumplimiento de la normativa reguladora de la actividad de auditoría de cuentas.

Estas obligaciones de los auditores de seguir una determinada formación implican a su vez unas obligaciones de las entidades que proveen dicha formación de comunicarla a la autoridad supervisora, el ICAC, para la debida constancia y en su caso revisión examen, de la misma. Ello supone un tratamiento de datos, una cesión, de los propios auditores o sociedades de auditoría o desde las entidades que proporcionan dicha formación al ICAC. Así, el art. 28.3 del proyecto de reglamento establece:

> *Los auditores de cuentas y sociedades de auditoría deberán rendir información anual al Instituto de Contabilidad y Auditoría de Cuentas de la formación práctica que hayan realizado las personas a su servicio,*

con el detalle y distribución, y en el plazo que se determinen mediante resolución del Instituto de Contabilidad y Auditoría de Cuentas.

O el art. 36:

Las corporaciones de derecho público representativas de auditores de cuentas, las Universidades, así como las sociedades de auditoría, agrupaciones de sociedades de auditoría y grupos de auditores individuales ejercientes y los centros de formación reconocidos por el Instituto de Contabilidad y Auditoría de Cuentas que realicen las actividades de formación continuada, conforme a lo previsto en el artículo anterior, remitirán, al Instituto de Contabilidad y Auditoría de Cuentas, en el mes de noviembre de cada año, una declaración anual de las actividades finalizadas en los doce meses anteriores al 30 de septiembre de cada año.

Asimismo, las corporaciones de derecho público representativas de auditores de cuentas, en el plazo previsto en el apartado 1, remitirán al Instituto de Contabilidad y Auditoría de Cuentas la relación de actividades comunicadas por los auditores pertenecientes a las mismas. (…)

Estas obligaciones establecidas en la norma derivan directamente de la Directiva 2006/43/CE, y del Reglamento europeo, y de la ley 22/2015, y suponen un requisito indispensable tanto para que el auditor pueda entrar a formar parte de la profesión y ejercer como tal, como, asimismo, en lo que respecta a la formación continuada, pueda seguir ejerciendo y realizando auditorías legales. Por lo tanto, puede considerarse, al igual que ya se hizo en el informe relativo de esta AEPD 258043/2011 citado, sobre la base de la Directiva 95/46 y la LOPD entonces vigente, que dichas comunicaciones -tratamientos de datos personales- tienen una base jurídica en el artículo 6.1, letra b) RGPD en cuanto que constituyen un tratamiento necesario para la ejecución de un contrato por cuanto constituye una comunicación necesaria para la adecuado desarrollo de la relación jurídica del auditor con las sociedades o entidades, toda vez que la finalidad última de la realización de las acciones formativas es, precisamente, la acreditación del cumplimiento de los requisitos mínimos exigibles para el desempeño de la actividad de auditoría de cuentas.

Podría añadirse asimismo que dicho tratamiento puede ser también necesario para cumplimiento de una misión realizada en interés público (art. 6.1, letra e) RGPD), por cuanto dicho interés se predica, tal y como resulta de las Directivas europeas al respecto, de la actividad de los auditores en cuanto éstos han de demostrar una formación suficiente para que tanto la sociedad auditada como los terceros que pueda relacionarse con ésta, tengan la confianza en que la opinión de auditoría recoge la imagen fiel, lo que se debe

tanto a los métodos de trabajo de la auditoría como a la formación del auditor, por cuanto, como describe la Exposición emotivos de la ley 22/2015.

> *La actividad de auditoría de cuentas se caracteriza por la relevancia pública que desempeña al prestar un servicio a la entidad revisada y afectar e interesar no sólo a ésta, sino también a los terceros que mantengan o puedan mantener relaciones con la misma, habida cuenta de que todos ellos, entidad auditada y terceros, pueden conocer la calidad de la información económica financiera auditada sobre la cual versa la opinión de auditoría emitida. Con la finalidad de regular y establecer las garantías suficientes para que las cuentas anuales o cualquier otra información económica financiera que haya sido verificada por un tercero independiente sea aceptada con plena confianza por los terceros interesados, en la Ley 19/1988, de 12 de julio, de Auditoría de Cuentas, se definió la actividad de auditoría y se establecieron, entre otras disposiciones, las condiciones que se deben cumplir para acceder al Registro Oficial de Auditores de Cuentas y poder así ejercer tal actividad, las normas que regulan su ejercicio, el contenido mínimo del informe de auditoría de cuentas anuales, el régimen de incompatibilidades y de responsabilidad de los auditores de cuentas, el régimen de infracciones y sanciones y la atribución al Instituto de Contabilidad y Auditoría de Cuentas del control de la actividad y de la potestad disciplinaria de los auditores de cuentas*

--- *** ---

Dentro de este apartado, y como muestra de la importancia y la relación que tienen las actividades de auditoría con las normas de protección de datos personales, cabe destacar el artículo 29 del proyecto sometido a informe, que regula el examen de aptitud al que deben someterse los aspirantes a auditores legales, "*que irá encaminado a la comprobación rigurosa de la capacitación del candidato para el ejercicio de la actividad de auditoría de cuentas*", y que consta de dos fases: una primera de comprobación del nivel de conocimientos teóricos, y una segunda fase que consistirá en determinar la capacidad de aplicar los conocimientos teóricos a la práctica de la actividad de auditoría de cuentas.

Pues bien, no está de más recordar aquí la sentencia del TJUE de 20 de diciembre de 2017, C-434/16, Peter Nowack. El Sr. Peter Nowack, como contable en prácticas, aprobó la primera parte de los exámenes de contabilidad y tres de las pruebas de la segunda parte organizados por el Institute of Chartered Accountants of Ireland (Instituto de Auditores Públicos de Irlanda). Sin embargo, suspendió el examen de «contabilidad de gestión y finanzas estratégicas». A raíz del resultado desfavorable de este examen, en el otoño del año 2009 el Sr. Nowack, en un primer momento, presentó una reclamación contra la nota obtenida. Al ver desestimada su reclamación, presentó una

solicitud de acceso a todos los datos de carácter personal que le afectaban, en poder el Instituto de Auditores Públicos. En 2010, dicho Instituto remitió al Sr. Nowack 17 documentos, pero se negó a remitirle su ejemplar del examen, al considerar que no contenía datos personales.

En dicha sentencia C-434/16, el TJUE ha considerado que las *respuestas escritas de un aspirante en un examen profesional* son datos relacionados con su persona, es decir, datos personales del aspirante. El contenido de esas respuestas refleja el nivel de conocimientos y competencia del aspirante en un área determinada y, en ocasiones, sus procesos de reflexión, su discernimiento y su capacidad de análisis. Además, mediante la obtención de las respuestas se pretende valorar la capacidad profesional del aspirante y su aptitud para ejercer el oficio de que se trate. Finalmente, la utilización de esos datos, que se traduce, en particular, en el éxito o el fracaso del aspirante en el examen en cuestión, puede tener efectos en sus derechos e intereses, ya que puede condicionar o alterar, por ejemplo, sus oportunidades de acceder a la profesión o al empleo deseados. El Tribunal de Justicia señala que, al igual que las respuestas proporcionadas por ese aspirante durante el examen, las *anotaciones del examinador* sobre las respuestas del aspirante son datos que le afectan. El contenido de esas anotaciones expresa la opinión o valoración del examinador acerca del rendimiento individual del aspirante en el examen y, en particular, sobre sus conocimientos y competencias en el área de que se trate.

VIII

El art. 28 de la ley 22/2015, de 20 de julio, de Auditoría de Cuentas, respecto de la organización interna, dispone que *los auditores de cuentas y las sociedades de auditoría dispondrán de procedimientos administrativos y contables fiables, de procedimientos de valoración de riesgo eficaces, de mecanismos operativos que permitan asegurar el control y la protección de sus sistemas informáticos, así como de los mecanismos internos de control de calidad, que garanticen el cumplimiento de las decisiones y procedimientos en el seno de la estructura funcional del auditor de cuentas y en todos los niveles de la sociedad de auditoría.*

Igualmente establece en su apartado 2 que *los auditores de cuentas y las sociedades de auditoría implantarán un sistema de control de calidad interno que garantice la calidad de la auditoría de cuentas de conformidad con lo establecido en las normas de control de calidad interno a las que se refiere el artículo 2.*

Establece, por lo tanto, la necesidad de que los auditores legales tengan una organización interna con políticas y procedimientos apropiados a la

actividad de auditoría, y que cuenten además con un sistema de control de calidad que cumpla una serie de criterios, todo ello como consecuencia de lo establecido en el artículo 24 bis y en el artículo 29 de la Directiva 2006/43/CE, modificada por la Directiva 2014/56/UE.

El proyecto de reglamento desarrolla estos preceptos en los artículos 66 a 71.

El artículo 66.1, párrafo segundo, del proyecto dice que: *Esta organización interna incluirá procedimientos administrativos contables y* ***procedimientos de identificación, valoración, y respuesta a los riesgos significativos que afecten a la actividad de auditoría de cuentas****, de acuerdo con lo indicado en este artículo, así como el sistema de control de calidad interno regulado en el artículo Sistema de control de calidad interno.*

Y el párrafo 4 de dicho artículo precisa que:

> *Los procedimientos administrativos relativos a la identificación, valoración y respuesta a los* ***riesgos que puedan afectar a la actividad de la auditoría de cuentas****, incluirán los relativos al control y la protección de los sistemas informáticos, así como, en el caso de los auditores de entidades de interés público, aquellos que permitan asegurar la continuidad y regularidad de la actividad de auditoría de cuentas.*
>
> *Los citados procedimientos deberán ser eficaces para asegurar razonablemente la adecuada gestión de los riesgos que puedan afectar a la actividad de auditoría de cuentas. Estos procedimientos incluirán la obtención de información necesaria derivada de actuaciones de la red a la que pertenezcan, así como de las personas y entidades contempladas en el artículo 19.1 y 20.1 de la Ley 22/2015, de 20 de julio, en tanto en cuanto afecte, de alguna forma, al funcionamiento del auditor de cuentas o sociedad de auditoría o al cumplimiento de la normativa aplicable a éstos, que comprenderá la información sobre la propuesta o prestación de servicios u otras operaciones o transacciones realizadas durante el ejercicio con entidades auditadas o vinculadas a estas.*

La identificación de los riesgos es una actividad compleja, y ha de ser considerada desde un punto de vista amplio, puesto que incluye necesariamente (entre otros aspectos) los riesgos derivados de la cualidad del auditor como responsable del tratamiento de datos personales.

Los artículos 24 y 32 del RGPD regulan la responsabilidad del responsable del tratamiento de datos personales en relación con dichos tratamientos y con las medidas de seguridad adecuadas para el riesgo que los tratamientos de datos suponen para los derechos e intereses de los afectados

(las personas físicas), estableciendo la obligación de que adopten medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado a los riesgos.

Si bien el artículo 74 del proyecto hace referencia a que los tratamientos de datos de carácter personal que lleven a cabo los auditores de cuentas se encuentran sometidos al RGPD y a la Ley orgánica 3/2018, de Protección de Datos Personales y garantía de derechos digitales (LOPDGDD), se considera recomendable que dentro de los procedimientos administrativos relativos a la identificación, valoración y respuesta de los riesgos que puedan afectar a la actividad de auditoría de cuentas se incluyan expresamente, como riesgo a tener en cuenta y por tanto **mencionándolo expresamente en el artículo 66**, junto con los relativos al control y prevención de los sistemas informáticos (apartado 4 del art. 66), los relativos a los tratamientos de datos personales, de manera que los sistemas de organización interna de los auditores de cuentas regulados en el art. 66 del proyecto de reglamento hayan de incluir necesariamente dentro de los procedimientos administrativos relativos a la identificación, valoración y respuesta de riesgos el riesgo ya citado de protección de datos.

Por supuesto, los auditores legales o sociedades de auditoría habrán de considerar siempre como uno de los riesgos relativos al ejercicio de su profesión el de la protección de datos personales. Entre otras circunstancias habrá de estarse al RGPD para verificar, por ejemplo, si el auditor legal necesita hacer una evaluación de impacto de materia de protección de datos/análisis de riesgos, y en general para llevar a cabo las medidas de responsabilidad proactiva requeridas de los responsables de los tratamientos de datos personales.

IX

Los artículos 24.bis.1 y 24 ter.3, último párrafo, de la Directiva 2006/43/CE, en la redacción dada por la Directiva 2014/56/UE, establecen la posibilidad de que el auditor legal solicite asesoramiento de expertos externos o lleve a cabo externalización de funciones en el ejercicio de sus actividades de auditoría. Ello sin embargo no puede dar lugar a que se perjudique el control interno de la calidad del auditor legal o de la sociedad de auditoría, y además la externalización de las funciones de auditoría mencionadas no afectará a la responsabilidad asumida por el auditor legal o la sociedad de auditoría frente a la entidad auditada.

Los artículos 67.9 y 70 del proyecto de reglamento, en desarrollo del art. 28.2.b) 4º de la ley 22/2015, hacen referencia a la posibilidad de los auditores legales de llevar a cabo la externalización de actividades (i) de auditoría de

cuentas o (ii) actividades de control de calidad, y el 74 lo extiende también a la posibilidad de externalizar los servicios de (iii) conservación y custodia de la documentación. En este último caso el art. 74, último párrafo, del proyecto de reglamento establece que "*deberá darse cumplimiento a lo dispuesto en la Ley Orgánica 3/2018 de 5 de diciembre, de protección de datos de carácter personal y garantía de los derechos digitales*".

Pues bien, de la redacción de los apartados anteriores, y, sobre todo, de lo dispuesto en el párrafo segundo del artículo 74 del proyecto, parecería entenderse que sólo en el supuesto de que los auditores legales externalizasen los servicios de conservación y custodia de la documentación (apartado (iii) según la numeración expuesta en el párrafo anterior) debería darse cumplimiento a la Ley Orgánica 3/2018, de 5 de diciembre (LOPDGDD). Sin embargo, parece que no se exigiría que se dé cumplimiento a dicha ley orgánica en los supuestos (i) y (ii). Sin perjuicio de que no es posible una interpretación en tal sentido, que se deje de cumplir la ley de protección de datos personales para determinadas actividades externalizadas, lo cierto es que de la redacción del artículo 74, segundo párrafo, del proyecto de reglamento parece desprenderse la idea de que en el supuesto (iii) nos encontraríamos ante un encargado del tratamiento y en los supuestos (i) y (ii) no.

Si ésta fuera la intención del redactor del proyecto, no se comparte la misma. Entendemos que, en todos estos supuestos, (i), (ii) y (iii), nos encontraríamos ante un verdadero encargado del tratamiento, en el sentido establecido en el artículo 4.8 del RGPD: "encargado del tratamiento" o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento, que es quien determina los fines y medios del tratamiento. Así como hemos sostenido que los auditores legales no son encargados del tratamiento respecto de las sociedades o entidades auditadas, en el presente caso son los propios auditores legales los que recurren a la externalización de determinadas funciones por trabajos relacionados con dicha actividad de auditoría de cuentas. Acertadamente, y siguiendo lo dispuesto en el artículo 28 de la ley y en la Directiva, el art. 67.9. 3º, cuarto párrafo, dice:

> *El auditor de cuentas o la sociedad de auditoría serán* ***plenamente responsables de todas las actividades externalizadas,*** *tanto en relación con la realización de trabajos de auditoría de cuentas como de actividades de control de calidad, no eximiéndole de sus obligaciones y de sus responsabilidades. Los acuerdos de externalización no podrán impedir las facultades de supervisión referidas en el artículo 49 de la Ley 22/2015, de 20 de julio.*

Por ello, el artículo 74, último párrafo, de acuerdo con el precepto transcrito, no debería hacer mención tan sólo a una de las actividades

externalizadas cuya externalización de lugar a la necesidad de cumplimiento de la LOPDGDD, sino que debería suprimirse dicha mención explícita a una de las actividades externalizadas de modo que la obligación de cumplimiento de la LOPDGDD por los auditores legales se extienda a **todas** las actividades que hubiesen decidido externalizadas, ya que se considera que todas ellas son encargos del tratamiento, con la necesidad y obligaciones de cumplir lo dispuesto en art. 28 y concordantes del RGPD y de la LOPDGDD.

X

El art. 30 sexies de la de la Directiva 2006/43/CE, en la redacción dada por la Directiva 2014/56/UE, establece:

> *Denuncia de las infracciones*
> *1. Los Estados miembros se asegurarán de que se establezcan mecanismos eficaces para fomentar la denuncia a las autoridades competentes de las infracciones de la presente Directiva o del Reglamento (UE) nº 537/2014.*
> *2. Los mecanismos contemplados en el apartado anterior incluirán, como mínimo:*
> *a) los procedimientos específicos para la recepción de denuncias de infracciones y para su seguimiento;*
> *b) la protección de los datos personales tanto del denunciante como del presunto responsable de haber cometido esa infracción, con arreglo a los principios establecidos en la Directiva 95/46/CE;*
> *c) las medidas apropiadas para garantizar el derecho de la persona acusada a defenderse y a ser oída antes de que se adopte una decisión a su respecto, además del derecho a un recurso efectivo ante un órgano jurisdiccional contra cualquier decisión o medida que le pueda concernir.*
> *3. Los Estados miembros se asegurarán de que las sociedades de auditoría establezcan los procedimientos oportunos para que sus* ***empleados puedan denunciar internamente*** *las infracciones potenciales o reales de la presente Directiva o del Reglamento (UE) nº 537/2014 a través de un canal específico*

El art. 28 de la ley 22/2015 establece la necesidad para los auditores legales de disponer e implantar un sistema de control de calidad interno que garantice la calidad de la auditoría de cuentas. Dicho sistema de control de calidad interno debe incluir políticas y procedimientos apropiados para la realización de los trabajos de auditoría de cuentas, y entre otras cuestiones, establecer apropiadamente el seguimiento de dichos procedimientos. El apartado 5º del art. 28.2, letra b) de la ley 22/2015 señala que entre dichos procedimientos habrán de incluirse:

5.º Políticas y procedimientos para comprobar y analizar la idoneidad y eficacia de sus sistemas de organización interna y del sistema de control interno, así como las medidas a adoptar para corregir cualquier posible deficiencia.
Dichos procedimientos incluirán, entre otros, los medios para que el personal del auditor de cuentas y de las sociedades de auditoría pueda ***denunciar internamente los hechos que pudieran ser constitutivos de infracciones de la normativa reguladora de la actividad de auditoría de cuentas****.*

El art. 67.10 del proyecto de reglamento sometido a informe viene a permitir, de conformidad con la normativa expuesta más arriba, la posibilidad de que el sistema de seguimiento pueda considerar la información obtenida a través de una denuncia.

Sin embargo, hay que tener en cuenta en su integridad la regulación contenida en el artículo 24 LOPDGDD de los sistemas de información de denuncias internas, que igualmente, y dado que la normativa específica de auditoría (Directiva, ley y reglamento) establece la obligación de que el sistema de seguimiento cuente con un sistema de denuncias internas, éste deberá cumplir con la regulación establecida en el citado art. 24.

Por ello parece conveniente que, bien directamente en el artículo 67.10, bien en el propio artículo 74 del proyecto, se haga referencia al citado artículo 24 LOPDGDD como norma que deberá regular, desde la perspectiva de la normativa de protección de datos personales, la regulación de las denuncias internas en los sistemas de seguimiento del control de calidad interno de los auditores legales. También podría aprovecharse para actualizar en el reglamento sometido a informe la referencia a normativa ya derogada que se contiene en el párrafo tercero del art. 89 de la ley 22/2015 respecto al tratamiento de los datos de carácter personal del denunciante, que deberá referirse no a la LOPD 15/1999, sino al RGPD y a la LOPDGDD.

XI

El art. 32 de la Directiva 2006/43/CE, en la redacción dada por la Directiva 2014/56/UE, establece que *los Estados miembros organizarán un sistema efectivo de supervisión pública para auditores legales y sociedades de auditoría basado en los principios establecidos en los apartados 2 a 7 y designarán una autoridad competente responsable de dicha supervisión*.

Dicha autoridad competente en España es el Instituto de Contabilidad y Auditoría de Cuentas (ICAC), (art. 46.2 ley 22/2015). El art. 48.1 de la ley

22/2015 establece que *[e]l Instituto de Contabilidad y Auditoría de Cuentas podrá recabar cuanta información estime necesaria para el adecuado cumplimiento de las competencias de supervisión que tiene encomendadas (…)*

El art. 88.7 del proyecto de reglamento presentado a informe a su vez establece que *[e]l Instituto de Contabilidad y Auditoría de Cuentas podrá requerir a los auditores de cuentas y sociedades de auditoría de cuentas, en cualquier momento, cuanta información venga exigida legal o reglamentariamente a éstos, así como cuanta información de carácter público respecto de las entidades auditadas se considere necesaria para el adecuado cumplimiento de las competencias que tiene atribuidas.*

Como ya hemos mencionado anteriormente, todas las actuaciones del ICAC en el ejercicio de sus funciones están sujetas a la normativa de protección de datos (art. 89.1, ley 22/2015), por lo que estas solicitudes de información habrán de acomodarse a los dispuesto por dicha normativa, y de ello en primer lugar cabe resaltar que dichos requerimientos de información estarán sujetos en todo caso a los principios relativos al tratamiento de datos contenidos en el art. 5 RGPD, fundamentalmente en este caso al principio de minimización (los datos solicitados habrán de ser sólo los "*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados*" y en segundo lugar, y tal y como ha establecido el Tribunal Constitucional (TC), ello conlleva limitaciones en la actuación administrativa, que ha de coordinarse con el derecho fundamental a la protección de datos personales.

Así, la sentencia del TC 17/2013, de 31 de enero, con citra de otras como la STC 292/2000, de 30 de noviembre, dice, lo que sería exactamente aplicable a nuestro informe:

> *Ahora bien, dicha previsión legal ha de ser entendida de forma acorde con las exigencias de proporcionalidad que nuestra doctrina exige en la limitación de un derecho fundamental como es el aquí concernido, relativo la protección de datos de carácter personal. Eso significa que la cesión de datos que el acceso regulado por el precepto supone ha de venir* ***rodeado de una serie de garantías específicas****, garantías que, cumplimentadas por el órgano administrativo al que el precepto hace referencia, son, evidentemente,* ***susceptibles de control****. Entre ellas se encuentra la necesidad de* ***motivar y justificar expresamente t****anto la concreta atribución de la condición de usuario para el acceso telemático a los datos del padrón que el precepto prevé, como los concretos accesos de que se trate,* ***evitando*** *—en cuanto que la exigible motivación de tales decisiones facilita su correspondiente control mediante los mecanismos previstos en el ordenamiento jurídico, en especial, a través del control jurisdiccional contencioso-administrativo—*

*que se produzca tanto un uso torticero de dicha facultad **como accesos indiscriminados o masivos**. Límites al contenido del acceso que también resultan de determinadas previsiones de la legalidad ordinaria, las cuales han de ser aplicadas teniendo presente, en todo caso, la necesaria unidad del ordenamiento jurídico, tales como el art. 16.3 LBRL, que ya hemos examinado o, incluso, otras regulaciones específicas de la Ley Orgánica de protección de datos, en especial su art. 22.2. Resulta de ello que el acceso solamente será posible, en las condiciones antes dichas, cuando el concreto dato en cuestión resulte **pertinente y necesario** en relación con la **finalidad** que ha justificado el acceso, quedando garantizada la posibilidad de analizar si, en cada caso concreto, el acceso tenía amparo en lo establecido en la ley pues, en caso contrario, no resultará posible su uso. Con tales garantías el acceso regulado en la disposición cuestionada resulta ser proporcionado en relación con la finalidad perseguida, ya que, en tanto que el dato resultante solo puede ser utilizado para la finalidad establecida en el precepto, ha de realizarse de forma puntual por quien se encuentre expresamente habilitado para ello y en relación a datos concretos cuya necesidad ha de ser también justificada de forma expresa y, por tanto, sometida a control, en los términos que acabamos de exponer.*

En definitiva, en lo que respecta a la posibilidad de solicitud de información por el ICAC en el ejercicio de sus funciones cabe, desde la perspectiva de la normativa de protección de datos, considerar que la base jurídica de los tratamientos que realiza sería la del art. 6.1.e) RGPD (cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos) pero está siempre sujeta a los límites inherentes al derecho fundamental a la protección de datos que hemos mencionado.

XII

El art. 55 de la ley 22/2015 prevé que el ICAC podrá utilizar los servicios de profesionales y expertos para la realización únicamente de labores meramente instrumentales o para verificaciones o funciones específicas. El apartado 4 de dicho precepto establece que quienes participen en dichas labores meramente instrumentales podrán acceder a la documentación que sea necesaria referente a los auditores o sociedades de auditoría siempre y cuando así lo determinen expresamente los funcionarios inspectores del ICAC. Estas personas quedarán sujetas al deber de secreto.

Se produce en estos casos un tratamiento de datos por personal al servicio (mediante un contrato de servicios) del ICAC, que cabe considerar que se lleva a cabo a través de un encargado del tratamiento por cuenta del ICAC, para lo cual, y tal y como ya se ha hecho hincapié, deberá suscribirse el

correspondiente contrato de encargo de tratamiento (disposición adicional vigésima quinta de la ley 9/2017, de 8 de noviembre, de Contratos del Sector Público).

> *2. Para el caso de que la contratación implique el acceso del contratista a datos de carácter personal de cuyo tratamiento sea responsable la entidad contratante, aquel tendrá la consideración de encargado del tratamiento.*

XIII

Los artículos 111 y siguientes del proyecto de reglamento de auditoría regulan los intercambios de información, en cumplimiento del deber de colaboración previsto en la Directiva, entre las autoridades competentes de los Estados miembros de la Unión Europea. Como tal, al ser miembros de la UE, no nos encontramos, desde la perspectiva de la normativa de tratamiento de datos personales, ante una transferencia internacional ya que el art. 1.3 RGPD establece que *la libre circulación de los datos personales en la Unión no podrá ser restringida ni prohibida por motivos relacionados con la protección de las personas físicas en lo que respecta al tratamiento de datos personales.*

A estos efectos cabe mencionar en primer lugar que este intercambio con autoridades competentes de Estados miembros de la Unión Europea puede incluir información acerca de procesos sancionadores que se estén llevando a cabo o hayan finalizado.

El artículo 27 de la LOPDGDD contiene una regulación específica acerca de los tratamientos de datos relativos a infracciones y sanciones administrativas. El apartado 1 establece los requisitos necesarios para que sea lícito un tratamiento de datos relativos a infracciones y sanciones administrativas, incluido el mantenimiento de registros relacionados con las mismas. El primero de dichos requisitos, letra a), es que los responsables de dichos tratamientos sean los órganos competentes para la instrucción del procedimiento sancionador, la declaración de infracción o la imposición de sanciones. Y, en segundo lugar, letra b), que el tratamiento se limita los datos estrictamente necesarios para la finalidad perseguida por aquel. Si tenemos en cuenta el régimen de supervisión aplicable a los auditores legales, en los cuales, y de acuerdo con la Directiva 2006/43/CE, deberán publicarse las sanciones impuestas (art. 30 quater de la Directiva 2006/43/CE, modificada por la Directiva 2014/56/UE) cabe considerar que dicho tratamiento de datos consistente en la transferencia a la autoridad competente de otro Estado miembro de la información que consta en el registro público de la autoridad competente tiene una base lícita en el interés público (art. 6.1, letra e) RGPD).

En segundo lugar, y respecto a la letra g) del citado artículo 111, que hace referencia a la posibilidad de transferir información mediante intercambio de "*cualquier información que pueda resultar de utilidad para el ejercicio de las funciones de supervisión*", de acuerdo con los principios ya citados reiteradamente de proporcionalidad y minimización previstos en la normativa de protección de datos, dicha posibilidad de intercambio de información ha de venir restringida a la que sea *estrictamente necesaria* para las funciones propias de las autoridades de supervisión. Sin embargo, no se considera que este apartado g) sea en sí mismo excesivo por cuanto en los artículos 112 y 113 y siguientes del proyecto de reglamento se establecen una serie de cautelas que han de tenerse en cuenta a la hora de determinar la bondad del precepto, como es que la solicitud de intercambio de información debe incluir una explicación de las razones que justifican la solicitud, de la finalidad para que la que se va a utilizar la información, y debe referirse en todo caso a la información *necesaria* para el cumplimiento de sus funciones y que no pueda obtenerse por otros medios. Por ello, habida cuenta de las cautelas previstas en los artículos 112 y 113, que determinan que la expresión "cualquier información que pueda resultar de utilidad" ha de entenderse en realidad como que fuese necesaria para cumplimiento de las funciones y que no pueda obtenerse por otros medios, se considera que dicho apartado g) del art. 111 es conforme a la normativa de protección de datos personales.

También constituye un intercambio de información, esto es, un tratamiento de datos personales, la posibilidad prevista en la norma de colaboración entre las autoridades supervisoras para la realización de actuaciones de control en un determinado estado miembro, ya que por el hecho de permitir a miembros de una autoridad supervisora de un Estado miembro acompañar al personal de la autoridad competente en España, el ICAC, la autoridad competente en otro Estado miembro podrá adquirir información que contenga datos personales.

Esta posibilidad está expresamente prevista en la Directiva 2006/43/CE en su art. 36.6:

> *Una autoridad competente de un Estado miembro también podrá pedir que la autoridad competente de otro Estado miembro realice una investigación en el territorio de este último.*
> *Podrá pedir, además, que se permita que algunos miembros de su propio personal* ***acompañen al personal de la autoridad competente de ese otro Estado miembro en el transcurso de la investigación.***
> *La investigación estará completamente sujeta al control general del Estado miembro en cuyo territorio se lleve a cabo.*

En desarrollo de dicho precepto, la ley 22/2015 regula dichas posibilidades en art. 63.

Se considera que estos tratamientos de datos pueden englobarse, al igual que con carácter general hemos establecido, en la base de licitud contenida en el art. 6.1 letra e) del RGPD, esto es, en el cumplimiento de una misión de interés público, establecida además directamente en una norma de derecho de la Unión Europea.

XIV

El art. 117 integra la sección 3ª del capítulo II del Título III, referente a la coordinación con autoridades competentes de terceros países, en desarrollo del art. 67 de la ley 22/2015, y del art. 47 de la Directiva 2006/43/CE, con las modificaciones introducidas por la Directiva 2014/56/UE.

En primer lugar, y comenzando por el artículo 67 de la ley, hay que mencionar que su apartado 1 establece que, atendiendo al principio de reciprocidad, podrán celebrarse acuerdos de intercambio de información con las autoridades de terceros países que sean declaradas adecuadas por la Comisión de la Unión Europea. Este acuerdo de intercambio de información (que el reglamento denomina “acuerdo de cooperación”, si bien es requisito necesario para la mencionada posibilidad de intercambio de la información, con el contenido que se establece en la ley 22/2015, no cabe considerarlo requisito suficiente por cuanto en todo caso (art. 47.1, letra e) de la Directiva 2006/43/CE) *la transferencia de datos personales al tercer país habrá de ser conforme con el capítulo IV de la Directiva 95/46/CE* -Directiva de protección de datos personales-. Hoy día dicha referencia a la Directiva 95/46/CE ha de considerarse realizada al RGPD, que regula en su capítulo V esta materia.

Sin necesidad de entrar ahora en un análisis de las diferentes posibilidades que prevé el RGPD para considerar la transferencia de datos personales a terceros países como conforme a la normativa de protección de datos, basta citar en este momento que dicha transferencia puede basarse en una “decisión de adecuación” de la Comisión (art. 45 RGPD), en una transferencia mediante garantías adecuadas (art. 46 RGPD) -incluyendo en ellas a las normas corporativas vinculantes (art. 47 RGPD) – o por medio de excepciones para situaciones específicas (art. 49 RGPD), es lo cierto que en principio cualquiera de estas causas de legitimación de la transferencia de datos personales a un tercer país sería suficiente, siempre que se cumplan los requisitos establecidos en dichos preceptos, para permitir dicha transferencia -ello exclusivamente considerado desde la perspectiva de la normativa de protección de datos personales-. Por ello cabe concluir que será necesaria en todo caso una base de legitimación de las previstas en la normativa de protección de datos personales para transferir dichos datos a un tercer país, *y además* habrán de cumplirse los requisitos propios de la normativa de auditoría, como el que exista en primer lugar una declaración de adecuación

por la Comisión de que un tercer país es adecuado en materia de autorización, registro, control de calidad, investigación y régimen disciplinario de auditoría, y en segundo lugar, que exista un acuerdo de intercambio de información con el contenido que se prevé en el artículo 67.1 de la ley 22/2015.

XV

Continuando con la exposición comenzada en el ordinal anterior acerca de la cooperación con autoridades competentes de terceros países, cabe poner de manifiesto una circunstancia a la que ya se hizo referencia cuando esta AEPD emitió sus informes 258043/2011, 364906/2011 y 364906/2011 en relación con el proyecto de reglamento de desarrollo de la ley 19/1988, de 12 de julio, de Auditoría de cuentas. Y es que entonces, el reglamento, como el actual sometido a informe, establecía una posibilidad que se considera no prevista por la Directiva 2006/43/CE, ni por la ley 22/2015, que transpone en las modificaciones introducidas en dicha Directiva por la Directiva 2014/56/UE.

El proyecto de reglamento sometido a informe (como ya contemplaba el anterior, vigente en la actualidad) introduce la posibilidad de que dichos acuerdos de cooperación con las autoridades supervisoras de un tercer país contemplen que se puedan llevar a cabo “actuaciones de control conjuntas” o “permitir al personal de la autoridad competente de un tercer país participar en una actuación de control junto con el personal del ICAC” en España, “siempre que así lo prevea la correspondiente Decisión de la Unión Europea y en los términos contenidas en la misma”.

Si se observa la regulación contenida en la Directiva 2006/43/C, modificada por la Directiva 2014/56/UE, la cooperación con autoridades competentes **de terceros países** parece centrarse en la posibilidad de permitir el envío a las autoridades competentes de un tercer país de los papeles de trabajo de auditoría en poder de los auditores legales (art. 47.1 Directiva) bien por la autoridad competente del país de origen, bien, excepcionalmente, directamente por el auditor legal o la sociedad de auditoría. Parece que dicha norma concibe la Decisión de adecuación de la Comisión exclusivamente como medio de determinar la posibilidad de intercambio de papeles de trabajo de auditoría u otros documentos que obran en poder de auditores legales y sociedades de auditoría (art. 47.3 Directiva). No se hace mención en ningún momento en la Directiva a que dicha Decisión de adecuación de la Comisión respecto de un tercer país no miembro de la UE pueda referirse a supuestos distintos del intercambio de papeles de trabajo u otros documentos (actuaciones conjuntas). Se establece así en la Directiva una diferencia clara entre el régimen de cooperación entre los Estados miembros de la UE y el régimen de cooperación con terceros países. Lo anterior se reafirma aún más si se observan los artículos 31 y 36 del Reglamento (UE) 537/2014, sobre los

requisitos específicos para la auditoría legal de las entidades de interés público, norma esta que también se traspuso al ordenamiento jurídico español por la ley 22/2015. El mismo razonamiento cabe hacer respecto de la regulación que se contiene en el artículo 67 de la ley 22/2015, que no menciona en ningún momento la posibilidad de realizar “actuaciones conjuntas” con autoridades de terceros países.

Por eso la conclusión del Informe de la AEPD nº 258043/2011 fue que ni la Directiva ni el Texto Refundido de Auditoría de cuentas (entonces vigente) se refieren al supuesto de realización de actuaciones conjuntas de inspección en territorio español con autoridades de terceros países no miembros de la UE, a los que sí se refería el proyecto sometido entonces a informe, al igual que se refiere en el que ahora se somete a informe en la actualidad. Igualmente, el artículo 117 del proyecto de reglamento sometido a informe en desarrollo de la ley 22/2015, por lo que hace a dicho tratamiento de datos (la cesión a las autoridades de terceros países que participasen conjuntamente con el ICAC en la actuación conjunta de control) carecería de base legal. La base jurídica de un tratamiento de datos personales por razón de interés público necesita ser establecida por una norma de Derecho de la Unión o del Derecho del Estado miembro que se aplique al responsable del tratamiento (art. 6.4 RGPD), y en España, dicha base ha de estar constituida por una ley, conforme reiteradamente ha mantenido el Tribunal Constitucional, y recoge hoy el art. 8 LOPDGDD, y un reglamento de desarrollo de una ley no sería suficiente.

En respuesta a dichos informes emitidos por la AEPD en 2011, en los que se puso de manifiesto esta objeción, el Jefe de Gabinete de la Subsecretaría del Ministerio de Economía y Hacienda puso de relieve y envió documentación haciendo referencia a que Decisiones de la Comisión Europea dictadas en ejecución de la normativa referente a cooperación con terceros países en materia de auditoría habían establecido la posibilidad de llevar a cabo actuaciones de control conjuntas con autoridades de terceros países, haciendo referencia expresa a la Decisión de la Comisión 2010/485/UE, de 1 de setiembre de 2010, sobre la adecuación de las autoridades competentes de Australia y los Estados Unidos de América. Con posterioridad a dicha Decisión, y ya con la Directiva 2014/56/UE de plena aplicación (entrada en vigor, 17 junio 2016) la Comisión ha dictado otras Decisiones de adecuación, entre la que cabría destacar la Decisión de Ejecución (UE) 2016/1010 de la Comisión, de 21 de junio de 2016, sobre la adecuación de las autoridades competentes de determinados terceros países y territorios con arreglo a la Directiva 2006/43/CE del Parlamento Europeo y del Consejo; o la Decisión de Ejecución (UE) 2016/1156 de la Comisión, de 14 de julio de 2016, sobre la adecuación de las autoridades competentes de los Estados Unidos de América con arreglo a la Directiva 2006/43/CE del Parlamento Europeo y del Consejo. En la primera de estas, Decisión 2016/1010, la Comisión reconoce que determinadas autoridades competentes de terceros países o territorios (Dubai, Brasil, Sudáfrica etc.) cumplen requisitos que se considerarán adecuados a efectos

del artículo 47, apartado 1, letra c), de la Directiva 2006/43/CE a los fines del envío de papeles de trabajo de auditoría u otros documentos y de informes de inspección e investigación con arreglo al artículo 47, apartado 1, de dicha Directiva, *pero no establece ninguna previsión respecto de "actuaciones conjuntas*". En la segunda de ellas, Decisión 2016/1156, reconoce a determinadas autoridades de Estados Unidos a los efectos del art. 47.1, letra c) de la Directiva 2006/43/CE, pero añade, al igual que en la Decisión ya mencionada 2010/485/UE, de 1 de setiembre de 2010, que "[*l*]*os Estados miembros garantizarán que* ***toda inspección conjunta*** *que sus autoridades competentes lleven a cabo en la Unión con las autoridades competentes de los Estados Unidos cumpla las condiciones establecidas en el artículo 47 de la Directiva 2006/43/CE y que se realice, en general, bajo la dirección de las autoridades competentes del Estado miembro de que se trate*". El Considerando (11) de dicha Decisión expone:

> *Los Estados miembros pueden aceptar que, en circunstancias excepcionales, sus autoridades competentes realicen sus* ***inspecciones conjuntamente*** *con las autoridades competentes de los Estados Unidos cuando sea necesario para garantizar una supervisión efectiva. Los Estados miembros pueden autorizar que la cooperación con las autoridades competentes de los Estados Unidos se lleve a cabo a través de* ***inspecciones conjuntas o mediante observadores*** *que no tengan facultades de inspección o investigación ni acceso a los papeles de trabajo de auditoría u otros documentos confidenciales que obren en poder de los auditores legales o de las sociedades de auditoría, ni a informes de inspección o investigación. Resulta oportuno que dicha cooperación se desarrolle siempre en las condiciones establecidas en el artículo 47, apartado 2, de la Directiva 2006/43/CE y en la presente Decisión, en particular por lo que respecta a la necesidad de respetar la soberanía, la confidencialidad y la reciprocidad. Es preciso que los Estados miembros velen por que toda inspección conjunta que sus autoridades competentes lleven a cabo en la Unión con las autoridades competentes de los Estados Unidos al amparo del artículo 47 de la Directiva 2006/43/CE se realice, en general, bajo la dirección de las autoridades competentes del Estado miembro de que se trate*

En conclusión, no corresponde a esta AEPD determinar la validez de las Decisiones u otros actos jurídicos de la Comisión, competencia esta reservada al Tribunal de Justicia de la UE bien mediante recurso de anulación (art. 263 TFUE) bien a través de un recurso prejudicial (art. 267 TFUE), sino constatar que en la actualidad existen Decisiones que permiten actuaciones conjuntas con determinadas autoridades competentes de terceros países (no con todas), por lo que mientras dichas Decisiones se mantengan vigentes se considera que existe base jurídica suficiente conforme al art. 6.1. letra e) RGPD en relación con el art. 6.4 RGPD para los tratamientos de datos personales que puedan darse en las actuaciones conjuntas con las autoridades competentes de

terceros países autorizados mediante Decisión de la Comisión conforme al art. 47.1, letra c) de la Directiva 2006/43/CE, por lo que las previsiones contenidas en el art. 117.1 y en el art. 117.6 del proyecto de reglamento sometido a informe es conforme a derecho.

---***---

Aún en las Decisiones de adecuación citadas, la Comisión hace hincapié en que estas no agotan el espectro de requisitos necesarios para el envío de información a las autoridades competentes de terceros países, sino que es necesario el cumplimiento, entre otros requisitos que sean necesarios, de la normativa de transferencias internacionales de datos contenidas en la regulación de protección de datos personales. Así, por ejemplo, el Considerando (2) de la Decisión de Ejecución (UE) 2016/1010 de la Comisión, de 21 de junio de 2016, dice:

> *"Las decisiones sobre la adecuación adoptadas con arreglo al artículo 47, apartado 3, de la Directiva 2006/43/CE no abarcan los demás requisitos específicos para el envío de papeles de trabajo de auditoría u otros documentos o de informes de inspección o investigación en poder de auditores legales o sociedades de auditoría, como la celebración, entre las autoridades competentes, de acuerdos de trabajo sobre una base de reciprocidad según lo establecido en el artículo 47, apartado 1, letra d), de dicha Directiva,* ***o los requisitos para la transferencia de datos personales que se contemplan en la letra e) de dicho artículo****".*

O el Considerando (10) de la Decisión de Ejecución (UE) 2016/1156 de la Comisión, de 14 de julio de 2016:

> *Cuando el envío de papeles de trabajo de auditoría u otros documentos en poder de auditores legales o sociedades de auditoría y de informes de inspección o investigación a las autoridades competentes de los Estados Unidos suponga la divulgación de datos personales, tal divulgación únicamente es lícita* ***si cumple asimismo los requisitos para las transferencias internacionales de datos establecidos en la Directiva 95/46/CE*** *del Parlamento Europeo y del Consejo. Por consiguiente, el artículo 47, apartado 1, letra e), de la Directiva 2006/43/CE obliga a los Estados miembros a garantizar que el intercambio de datos personales entre sus autoridades competentes y las de los Estados Unidos se atenga a lo dispuesto en el capítulo IV de la Directiva 95/46/CE. Los Estados miembros deben velar por que existan salvaguardias adecuadas para la protección de los datos personales transmitidos, en especial mediante acuerdos vinculantes entre sus autoridades competentes y las autoridades competentes de los Estados Unidos, y que a su vez las autoridades competentes de los*

Estados Unidos no divulguen los datos personales incluidos en los documentos enviados sin el acuerdo previo de las autoridades competentes de los Estados miembros de que se trate.

Tal y como se ha expuesto con anterioridad en este informe, la referencia a la Directiva 95/46/CE ha de entenderse hoy realizada al RGPD.

XVI

Sobre la publicidad de las sanciones durante un plazo de 7, 6 o 5 años, desde la publicación, según sea muy grave, grave o leve, prevista en el art. 141 del texto, cabe mencionar que en la MAIN se contiene una explicación al respecto, en relación con el art. 30 quater de la Directiva, que se considera acertada.

Cabe mencionar igualmente que dicho art. 30 quater, en su apartado 3, hace referencia a que la publicación de sanciones y medidas habrá de respetar en todo caso el derecho a la protección de datos de carácter personal.

XVII

Artículo 144; el texto sometido a informe dice así:

A los efectos de lo dispuesto en el artículo [143]*.3, letras f) y g) anterior, las corporaciones de derecho público representativas de auditores de cuentas podrán acceder a la documentación referente a cada auditoría, quedando sujetas a la obligación establecida en el artículo 32.e) de la Ley 22/2015, de 20 de julio.*

Dicha referencia a las letras f) y g) no parece correcta. Más parece que debería referirse a las "letras g) y h)" del artículo 143. Véase la respuesta en la MAIN al comentario "U" presentado por el Instituto de Censores Jurados de Cuentas al borrador de texto, en el que se menciona que se retoma el apartado f) y se desdobla el g) en g) y h) (ejemplar enviado sin numeración de páginas).

Por otro lado, la mención al art. 32 e) que se hace en dicho precepto es incorrecta, ya que el apartado e) del art. 32 de la ley 22/2015 no establece que en sí mismo una obligación de secreto, sino que debería remitirse al artículo 31 de la ley, que es el que establece dicha obligación.

En cualquier caso, se propone una nueva redacción que ponga de manifiesto que las competencias para acceder a la documentación correspondiente a cada auditoría por cada una de las corporaciones de derecho público representativas de auditores de cuentas lo son a los exclusivos efectos de verificar las prácticas de sus miembros. Podría ser la siguiente:

A los exclusivos efectos de verificar la observancia de las prácticas y procedimientos internos de actuación de sus miembros en el ejercicio de su actividad de auditoría de cuentas referidas en las letras g) y h) del artículo anterior, las corporaciones de derecho público representativas de auditores de cuentas podrán acceder a la documentación referente a cada auditoría, quedando sujetas a la obligación de secreto establecida en el artículo 31 de la ley 22/2015, de 20 de julio, de Auditoría de Cuentas.

XVIII

La disposición adicional quinta del texto reglamentario sometido a informe desarrolla lo establecido en la disposición adicional séptima de la ley 22/2015. El texto reglamentario, en primer lugar, establece un mecanismo de coordinación, de acuerdo con el párrafo primero de la disposición adicional séptima de la ley, que consiste en que el auditor de cuentas deberá enviar un informe complementario al de auditoría de cuentas anuales a los órganos o

instituciones públicas que tengan atribuida legalmente la competencia de control y supervisión sobre empresas y entidades que sometan sus cuentas anuales a auditoría de cuentas. El apartado segundo del texto reglamentario desarrolla la obligación de comunicar a los organismos reguladores en el plazo de tres días hábiles cualquier hecho o decisión sobre la entidad o institución auditada de que hayan tenido conocimiento que pudiera constituir una violación grave de las normas, perjudicar la continuación de la explotación de la entidad auditada o implicar una opinión con salvedades, desfavorable o denegada. Y por último el apartado tercero desarrolla la obligación de enviar copia del informe de auditoría de las cuentas anuales a las autoridades supervisoras en caso de haber transcurrido una semana desde la fecha de la entrega de dicho informe a la entidad auditada por parte del auditor sin este haberlo realizado.

El apartado 4 de dicha disposición adicional establece que:

Los datos, informes, antecedentes y demás información obtenida por los Órganos e Instituciones Públicas en virtud de lo dispuesto en esta disposición adicional, sólo podrán utilizarse para los fines de control y supervisión encomendados a dichas Instituciones. Las informaciones que los Órganos e Instituciones Públicas, para el cumplimiento de sus funciones, tengan que facilitar a los auditores de cuentas de las empresas y entidades sujetas a su supervisión y control, quedarán exceptuadas del deber de secreto al que, en su caso, dichos Órganos e Instituciones se encuentren sujetos, conforme a su respectiva normativa legal.

Se recuerda que, en el caso de que entre la información o los datos obtenidos se encuentren datos personales, la utilización de dichos datos, incluso para los fines de control y supervisión encomendados a dichas instituciones, estará sujeto en todo caso a la normativa de protección de datos personales, lo que podrá conllevar, por ejemplo, y entre otras, obligaciones en materia de información a los afectados cuyos datos no se hubieran obtenido directamente de estos. Véase al respecto, como ejemplo, la Sentencia del TJUE, Sala Tercera, de 1 de octubre de 2015, Smaranda Bara y otros, Asunto C-201/14.

XIX

Reiterando lo que ya se expuso por esta AEPD en nuestro informe 258043/2011, en lo relativo a la entonces disposición adicional novena del texto reglamentario aún vigente, que se corresponde con lo establecido en el último párrafo del apartado 5 de la disposición adicional sexta del texto reglamentario sometido a informe, se recomienda que la referencia contenida en este último párrafo tenga la siguiente redacción:

La publicación de dichas resoluciones o consultas ***está en todo caso sujeta a la normativa de protección de datos personales****, y, además,*

no contendrá, en ningún caso, los datos referentes a las personas jurídico privadas, empresarios individuales o profesionales afectados por la resolución o consulta.