N/REF: 200574/2018

La consulta plantea si, de conformidad con lo establecido en la normativa de protección de datos, y, en concreto, de acuerdo con lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos -**RGPD**-), la entidad consultante -cuando realiza actividades de auditoria de tercera parte (esto es, auditorias de certificación realizadas a clientes, como terceros independientes y bajo un esquema estándar de certificación)-, tiene la condición de encargada o de responsable del tratamiento.

Según se expone en la consulta, en el supuesto sometido a informe los fines y medios del tratamiento no los determina el cliente, sino la propia empresa auditora, quien -siguiendo el criterio del auditor y basándose en esquemas estándar de certificación-, procede al tratamiento de datos de carácter personal incorporados a los sistemas de información de su cliente auditado.

I

El artículo 4.7 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, define al responsable del tratamiento o responsable como *"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."*

Asimismo, el citado Reglamento se refiere -en el apartado 8 de su artículo 4-, al encargado del tratamiento o encargado como "*la persona física o*

jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento". En este sentido cabe recordar que la figura del encargado del tratamiento obedece a la necesidad de dar respuesta a fenómenos como la externalización de servicios por parte de las empresas y otras entidades, de manera que en aquellos supuestos en que el responsable del tratamiento encomiende a un tercero la prestación de un servicio que requiera el acceso a datos de carácter personal por éste, dicho acceso no pueda considerarse como una cesión de datos por parte del responsable a quien le presta tal servicio, sino que el tratamiento de los datos se realiza por el encargado en nombre y por cuenta del responsable como si fuera este mismo quien lo lleva a cabo.

El artículo 28.3 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, 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. Dicho contrato o acto jurídico deberá constar por escrito, incluso en formato electrónico, como señala el número 9 de dicho artículo. 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".* Asimismo, el número 10 del artículo 28, establece que *"Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento."*

Por su parte, y en idéntico sentido, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, se refiere en su artículo 33 al encargado del tratamiento, disponiendo que:

"" Artículo 33. Encargado del tratamiento.

1. El acceso por parte de un encargado de tratamiento a los datos personales que resulten necesarios para la prestación de un servicio al responsable no se considerará comunicación de datos siempre que se cumpla lo establecido en el Reglamento (UE) 2016/679, en la presente ley orgánica y en sus normas de desarrollo.

2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.

Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades.

3. El responsable del tratamiento determinará si, cuando finalice la prestación de los servicios del encargado, los datos personales deben ser destruidos, devueltos al responsable o entregados, en su caso, a un nuevo encargado.

No procederá la destrucción de los datos cuando exista una previsión legal que obligue a su conservación, en cuyo caso deberán ser devueltos al responsable, que garantizará su conservación mientras tal obligación persista.

4. El encargado del tratamiento podrá conservar, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.

5. En el ámbito del sector público podrán atribuirse las competencias propias de un encargado del tratamiento a un determinado órgano de la Administración General del Estado, la Administración de las comunidades autónomas, las Entidades que integran la Administración Local o a los Organismos vinculados o dependientes de las mismas mediante la adopción de una norma reguladora de dichas competencias, que deberá incorporar el contenido exigido por el artículo 28.3 del Reglamento (UE) 2016/679.""

De este modo, teniendo en cuenta las definiciones de responsable y encargado del tratamiento contenidas tanto en el Reglamento General de Protección de Datos, como en la Ley Orgánica 3/2018, de 5 de diciembre, 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, reputándosele responsable en caso de que determine fines y medios, esto es, si utiliza para fines propios los datos personales que el responsable le haya comunicado para que lleve a cabo el tratamiento objeto de encargo, sin perjuicio de que pueda incurrir en una infracción del Reglamento con dicha actuación.

II

Así las cosas y con base en la normativa de protección de datos, hay que aclarar si la entidad consultante es, dentro del ámbito que se está exponiendo y respecto de los datos personales necesarios para realizar su labor de "auditoria de tercera parte", **un encargado** del tratamiento que -de acuerdo con las definiciones transcritas en el Punto anterior de este informe-, actué por cuenta del responsable accediendo a los datos personales que resulten necesarios para la prestación de un servicio, o si, por el contrario, actúa en calidad de **responsable** del tratamiento.

En relación con la *"auditoría de cuentas",* la cuestión sometida a consulta fue analizada en el informe 272/2011, de 28 de julio, emitido por el Gabinete Jurídico de esta Agencia con ocasión del análisis, de conformidad con lo dispuesto en los artículos 37 h) de la Ley Orgánica, de 13 de diciembre, de Protección de datos de Carácter Personal, referente al Proyecto de Real

Decreto por el que se aprobaba el Reglamento de desarrollo de la entonces vigente, Ley 19/1998, de 12 de julio, de Auditoría de Cuentas.

En el referido informe se concluye:

"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."
(…)

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 este mismo sentido, en nuestro reciente Informe 27/2019, de 26 de julio de 2019, emitido en relación con el proyecto de Real Decreto dictado en desarrollo de la Ley 22/2015, de 20 de julio, de Auditoría de Cuentas, viene a reiterarse la misma tesis mantenida en nuestro informe de 28 de julio de 2011, en similares términos. En dicho Informe se hace especial mención al principio de ***independencia*** en la actividad del auditor de cuentas en el tratamiento de los datos personales obtenidos de su cliente para el ejercicio de sus funciones, encontrándose estas establecidas en la normativa aplicable.

Así, se señala que no procede considerar un cambio de criterio con la entrada en vigor y aplicación práctica del RGPD, entendiendo que la actividad *de los auditores de cuentas o sociedades de auditoría* en el ejercicio de sus funciones se desarrolla en calidad de responsables de los tratamientos, en atención al carácter ***independiente*** de su actividad respecto de las entidades auditadas.

En lo que atañe al presente informe, respecto de los ***servicios de certificación de sistemas*** de gestión de calidad, medio ambiente, automoción, sistemas de información, y/o cualquier otro sistema de gestión sujeto a certificación de productos y servicios mediante auditoría independiente, las

normas *reguladoras aplicables* han establecido con nitidez la existencia de dos posibilidades diferentes de supervisión. Así, *en primer lugar*, la referida a los servicios prestados en virtud de encargos realizados por empresas clientes, y que se realizan sobre otras empresas y/o entidades vinculadas jurídicamente con "la cliente" a través de diversas modalidades. En estos supuestos, la auditoría se desarrolla bajo los esquemas propios de dicha "cliente" y en atención a las instrucciones recibidas de esta.

Tal y como se indica en el escrito de consulta, en este tipo de supuestos resulta clara la concurrencia de un "acceso a datos por cuenta de terceros", que deriva de un "encargo de tratamiento", al que resulta aplicable lo dispuesto en los artículos 4, apartado 8, y 28.3 del RGPD, y 33 de la LOPDGDD.

Y, *en segundo lugar*, las denominadas "auditorías de tercera parte" -especialmente reguladas en la actualidad por la *Norma ISO 19011: 2018, Directrices para los Sistemas de Gestión de Auditoría-,* en las que los fines y medios del tratamiento no los determina "el cliente", sino que se articulan bajo los propios esquemas y en atención a los requisitos establecidos por la entidad auditora que -actuando con absoluta independencia y siguiendo el correspondiente esquema estandarizado de certificación-, despliega su labor auditora sobre la estructura, organización y/o gestión de la propia "cliente".

La referida Norma ISO 19011:2018 – *Directrices para los Sistemas de Gestión de Auditoría -,* resulta de aplicación a todos los procesos de auditoría interna y externa de los distintos sistemas de gestión **basados en estándares de ISO.** Entre dichos sistemas, destacan los referidos a las Normas ISO 9001, ISO 14001, ISO 27001, ISO 45001.

Entre otros propósitos, la Norma ISO 19011:2018 acomete la actualización de los estándares aplicables para asegurar que las auditorías realizadas sobre los diferentes procesos se orienten de una manera efectiva a los cambios del mercado y a la evolución de la tecnología, imponiendo el mantenimiento de un enfoque coherente y armonizado para auditar sistemas de gestión de procesos. En resumen, esta Norma tiene por finalidad principal la descripción de un proceso eficaz de auditoría, señalando las pautas de

actuación y las funciones de los auditores en el marco de su trabajo *independiente*.

En la Norma ISO 19011:2018 se consolida la auditoría como un proceso *sistemático, **independiente** y documentado* cuyo objeto es la obtención de evidencias, que deberán ser evaluarlas ***de manera objetiva*** con el fin de determinar si la entidad auditada cumple con los criterios de referencia. Según se ha expuesto, estas auditorías pueden ir enfocadas a un sistema de gestión, producto o proceso.

Las auditorias de tercera parte son realizadas por organizaciones auditoras *independientes* y externas a la organización, que proporcionan la certificación de que el sistema cumple con la norma estándar de referencia. Las empresas que pueden realizar este tipo de auditoría deben *encontrarse acreditadas* por una Entidad Nacional de Certificación.

En España, la Entidad Nacional de Acreditación – **ENAC** – es la designada por el Gobierno, para operar como el único Organismo Nacional de Acreditación, en aplicación del ***Reglamento (CE) nº 765/2008*** que regula el funcionamiento de la acreditación en Europa.

ENAC es una asociación sin ánimo de lucro y declarada de utilidad pública. Su estructura y principios de funcionamiento garantizan que todas sus actuaciones se basan en los principios de imparcialidad, independencia y transparencia, contando en sus órganos de gobierno con todas las partes interesadas en el proceso, esto es, los acreditados, la industria usuaria de sus servicios y las administraciones públicas.

En conclusión, en relación con las auditorías de tercera parte, tanto en los procesos de gestión de calidad -ISO 9001-, como respecto a los de sistemas de gestión ambiental -ISO 14001- a las que se refiere expresamente el escrito de consulta, se extrae claramente que la consultante actuará como responsable del tratamiento, al exceder su actividad del concepto del concepto

y características propias del encargo de tratamiento de datos, no siguiendo en el desarrollo de sus funciones las instrucciones de su cliente, sino actuando ***de manera independiente*** en su ejercicio, y sin que la entidad auditada participe en el proceso de toma de decisiones.

De acuerdo con lo anterior, respondiendo a las cuestiones planteadas en la consulta con los números 1 y 2, la aplicación efectiva de lo previsto en el RGPD en relación con la actividad de las empresas auditoras, *cuando dichas entidades actúen* en auditorías "de tercera parte", siguiendo el propio criterio del auditor en la interpretación de la Norma ISO aplicable, y, en consecuencia, basándose en esquemas estándar de certificación, encontrándose debidamente registradas en ENAC, lo harán en **calidad de Responsables del tratamiento.**

III

La tercera cuestión planteada por la consultante se refiere a la base de legitimación para realizar los tratamientos de datos objeto del presente informe, referidos a auditoría de tercera parte. En este sentido, se plantea si para poder recabar los datos personales de los empleados y proveedores de sus clientes, deberá contar con el consentimiento expreso de los titulares de los datos personales, o si, por el contrario, existirá un interés legítimo para proceder a la recogida y tratamiento de información personal.

La normativa de protección de datos contempla diferentes supuestos que pueden dar lugar al tratamiento de datos de carácter personal. En concreto, de acuerdo con el **artículo 6** –"Licitud del tratamiento"-, del **RGPD**, entre otros, dicho tratamiento es lícito y legítimo cuando:

> "1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:
>
> a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;
>
> b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;
>
> c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;

d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;

e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;

f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.

Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones."

De acuerdo con lo anterior, procede enmarcar el tratamiento de los datos personales realizados por las entidades de servicios de *certificación de auditoría "de tercera parte"* dentro de las previsiones del referido precepto.

En este sentido, como ya se ha señalado, el artículo 6.1 del RGPD permite el tratamiento de los datos personales sin contar con el consentimiento del interesado en los diferentes supuestos a los que se refiere.

Pues bien, a diferencia del supuesto de la *auditoría de cuentas anuales*, en el que los tratamientos de datos realizados por los auditores y empresas de auditoría, se consideran tratamientos respecto de los cuales cabe predicar que la base jurídica para su licitud podría encontrarse en el apartado e) del art. 6.1 RGPD, por cuanto 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, en el supuesto objeto del *presente informe* ***no se extrae*** -salvo en los supuestos específicos en que la Ley establezca su obligatoriedad- la concurrencia de *dicha base jurídica* legitimadora -6.1 e RGPD-.

Por el contrario, en relación con la actividad de la entidad consultante concretada en la realización de su actividad *auditoria de tercera parte* en el marco de los servicios de certificación, y sometida a los estándares que resulten de aplicación para cada uno de los supuestos, el tratamiento de datos realizado se basa en la concurrencia del **interés legítimo** al que se refiere la **letra f)** del artículo 6.1 del RGPD.

En este sentido, los Considerandos del Reglamento General de Protección de Datos aportan ciertos elementos interpretativos en relación con la aplicación de la regla contenida en su artículo 6.1, letra f).

Así, el Considerando (47) recuerda que el interés legítimo de un responsable, de un cesionario o de un tercero, *"puede constituir una base jurídica para el tratamiento, siempre que no prevalezcan los intereses o los derechos y libertades del interesado, teniendo en cuenta las expectativas razonables de los interesados basadas en su relación con el responsable"*, añadiendo posteriormente que "*en cualquier caso, la existencia de un interés legítimo requeriría una evaluación meticulosa, inclusive si un interesado puede prever de forma razonable, en el momento y en el contexto de la recogida de datos personales, que pueda producirse el tratamiento con tal fin. En particular, los intereses y los derechos fundamentales del interesado podrían prevalecer sobre los intereses del responsable del tratamiento cuando se proceda al tratamiento de los datos personales en circunstancias en las que el interesado no espere razonablemente que se realice un tratamiento ulterior".*

Además, el propio RGPD enumera algunos supuestos que pueden ser tomados en consideración para determinar la aplicabilidad de dicha regla. Así, en primer lugar, se señala que el interés legítimo *"podría darse, por ejemplo, cuando existe una* ***relación pertinente y apropiada entre el interesado y el responsable, como en situaciones en las que el interesado es cliente o está al servicio del responsable****"*. Igualmente, en el propio considerando señala que *"el tratamiento de datos de carácter personal estrictamente necesario para la prevención del fraude constituye también un interés legítimo del responsable del tratamiento de que se trate"* y que *"el tratamiento de datos personales con fines de mercadotecnia directa puede considerarse realizado por interés legítimo".*

Por otra parte, el Grupo de Trabajo sobre Protección de Datos del Artículo 29 -de la Directiva 95/46/CE-, en su Dictamen 06/2014, de 9 de abril, sobre el concepto de interés legítimo del responsable del tratamiento de los datos en virtud del artículo 7 de la citada Directiva, alude a la aplicación de una *"prueba de sopesamiento"* en relación con la concurrencia del citado interés legítimo del responsable del tratamiento (o terceros), que deberá sopesarse en relación con los intereses o los derechos y libertades fundamentales de los afectados por los tratamientos. El resultado de esta prueba determinará en gran medida la concurrencia de dicho fundamento jurídico del tratamiento.

A dichos efectos, se señala que no se trata de una prueba de sopesamiento directa que consista simplemente en ponderar dos "pesos" fácilmente cuantificables y comparables. Por el contrario, como se explicará en

el propio documento con más detalle, la prueba de sopesamiento puede exigir una compleja evaluación que tenga en consideración una serie de factores. Con el fin de ayudar a estructurar y simplificar dicha evaluación, en el referido Dictamen 6/2014, de 9 de abril, se desglosa el proceso en varios pasos para facilitar que la prueba de sopesamiento se efectúe de manera eficaz.

En conclusión, el tratamiento de los datos de carácter personal realizado en el marco de los servicios de certificación *se encontraría* amparado por lo dispuesto en el artículo **6.1 f) RGPD,** quedando vinculado a la satisfacción de *intereses legítimos* perseguidos por el responsable del tratamiento *-la empresa auditora que actúa en calidad de responsable-* o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales.

En este escenario, la acreditación se constituye en una herramienta esencial para generar confianza sobre la correcta ejecución de determinados tipos de actividades, denominadas actividades de evaluación de la conformidad, y que incluyen -entre otras- el ensayo, la calibración, la inspección, la certificación y/o la verificación. La evaluación desarrollada genera valor añadido e incide positivamente en la eficacia, eficiencia y competitividad de las entidades auditadas.

En consecuencia, la evaluación de un producto, servicio, sistema, instalación y/o proceso, a los efectos de valorar su conformidad con los requisitos establecidos para la acreditación, se incardina en la base del tratamiento del artículo 6.1. f) -***interés legítimo***-.

La habilitación legal conferida debe cohesionarse con los principios de protección de datos recogidos en el artículo 5 del RGPD. A los efectos que aquí interesan, las letras b) c) y d) del mencionado artículo 5, en su apartado 1, se refieren a los **principios de limitación de la finalidad, minimización y exactitud**, y resultan plenamente predicables en relación con los servicios de certificación.

“5.1 Los datos personales serán:

(…)

b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («**limitación de la finalidad**»);

c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («**minimización** de datos»);

d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («**exactitud**»);"

Finalmente, es necesario recordar la obligación que incumbe a los responsables de los tratamientos en la adopción de las debidas medidas de seguridad sobre los tratamientos de datos de carácter personal que realicen.

Así, el artículo 24.1 del RGPD dispone que:

"Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".

En cuanto a las medidas de seguridad, el artículo 32 del RGPD, en su apartado primero dispone lo siguiente:

"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento".

Muy especialmente, en el supuesto objeto del presente Informe, por parte de los responsables de los tratamientos deberán adoptarse -siempre que sea posible- *"medidas de seudonimización y el cifrado de datos personales",* que garanticen la privacidad de los datos personales de los afectados, y que se ajusten a lo dispuesto en el citado artículo 32 del RGPD, y en los Considerandos (28) y (29) del propio Reglamento.