Máster Universitario en Auditoría de Cuentas

Universidad de Alcalá

Auditores
INSTITUTO DE CENSORES JURADOS DE CUENTAS DE ESPAÑA

Reglamento General de Protección de Datos y su implicación en la auditoría de cuentas

Curso académico: 2019 -2020

Trabajo Fin de Máster

Presentado por:

D. Miguel Ortiz Illescas

Dirigido por:

Dra. Mónica Arenas Ramiro

Alcalá de Henares, octubre de 2020

CONTENIDO

1. INTRODUCCIÓN

La protección de los datos personales de las personas físicas es un derecho fundamental tal y como se establece en Europa en la Carta de los Derechos Fundamentales de la Unión Europea (CDFUE)[1], y en España en la Constitución Española[2].

Pero a todos nos suele surgir la pregunta típica, ¿qué son los datos personales y qué datos no son personales? En general, la normativa europea, así como las nacionales hasta ahora, responde a esta pregunta considerando dato personal cualquier dato que identifica a una persona física identificable[3], es decir, el nombre, número de DNI, e-mail, número de teléfono, de móvil, dirección del domicilio, fecha de nacimiento o matrícula del coche entre otros. Así como imágenes, huellas o grabaciones de voz. También se admite como información personal aquellos datos que puedan identificar a una persona física mediante cualquier información referida a su físico, fisiología, su identidad económica o cultural.

La regulación de la protección de estos datos se aplica a las relaciones comerciales entre cualquier persona física o jurídica y al intercambio de información entre ambos para el desarrollo de dichas relaciones. Incluyendo además la aplicación de la regulación entre cualquier relación entre particulares. Además, el uso de las nuevas tecnologías, de Internet principalmente, aunque anteriormente a la aparición de este ya existía la regulación y normas sobre protección de datos, el intercambio masivo de información en la Red en tan poco tiempo ha potenciado y concienciado el uso de la regulación de la protección de los datos personales.

En la actualidad, es de aplicación 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 (Reglamento general de protección de datos, en adelante RGPD) y a nivel nacional, la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD).

¿Por qué realizar un trabajo sobre la regulación de la protección de datos y su implicación en la auditoría? En primer lugar, he elegido el tema relacionado con la protección de datos por la evolución principalmente de la tecnología y la informática, lo que ha facilitado la manera de almacenar datos de cualquier tipo poniendo en peligro los datos personales. El interés por estos datos y su protección me ha llevado en segundo lugar, a relacionarlo con la auditoría, profesión a la que me dedico.

Después de haber realizado la auditoría de cuentas anuales de diversos clientes, de diferentes sectores, he percibido las distintas formas de gestionar la información. También he podido corroborar, la cantidad de datos que las compañías almacenan y en algunos clientes en especial, la cantidad de datos personales. En general, todos las empresas a las que hemos auditado almacenan datos personales de todos sus empleados y clientes, pero en concreto, me ha llamado la atención, la cantidad de datos personales

[1] Art. 8 CDFUE.
[2] Art. 18 CE.
[3] Art. 4 RGPD.

que puede almacenar una clínica sanitaria ya que dispone además de los datos personales de todo el personal de la clínica, todos los datos personales de los clientes, los cuales son todos aquellos pacientes de los cuales pueden llegar a almacenar desde sus nombres, número de identificación, hasta cualquier enfermedad que haya padecido o padezca como hasta el tipo de sangre que poseen.

En todos los casos y clientes auditados, el auditor de cuentas necesita el consentimiento de estos para usar los datos personales facilitados para los procedimientos de auditoría a realizar.

A lo largo de este trabajo analizaremos dicho Reglamento general, así como el inicio y los antecedentes del mismo, en relación a la protección de los datos personales. Además, los diferentes aspectos relacionados con dicha regulación como son los titulares y obligados por el RGPD, los derechos y obligaciones derivadas del mismo y las infracciones y sanciones establecidas ante el incumplimiento del Reglamento.

Posteriormente al análisis del Reglamento, y tal y como indica el título del presente trabajo, "El Reglamento general de Protección de Datos y su incidencia en la auditoría de cuentas" analizaremos la implicación de la protección de datos y la regulación de esta materia en la auditoría de cuentas mediante el cumplimiento por los auditores del RGPD, el cumplimiento de derechos y obligaciones del RGPD en la auditoría, así como ejemplos y fases en la auditoría de cuentas en las cuales tiene incidencia dicho RGPD.

2. REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

2.1. Definición de la protección de datos

La protección de datos consiste en mantener el control de los datos personales facilitados por cada individuo a cualquier tercero el cual los haya almacenado o recopilado, teniendo en todo momento el individuo titular de estos datos el poder de decisión sobre estos ya sea para decidir sobre el traspaso de los mismos o para oponerse a la posesión de estos.

El Tribunal Constitucional señaló en su sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados. Siguiendo la sentencia y tal y como se establece en el preámbulo de la LOPDGDD, "*el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención*". Por otro lado, el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre, consideraba al derecho de protección de datos personales como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sin hacer distinción entre un particular o el Estado, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o uso.

El objetivo del RGPD, tal y como se explica en el artículo 1 de dicho Reglamento es *"La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europea ("la Carta") y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de carácter personal que le conciernan"*.

Dicho de otro modo, el artículo 1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales de Carácter Personal, la LOPDGDD, tiene por objeto "*Adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones. El derecho fundamental de las personas físicas a la protección de datos personales, amparado por el artículo 18.4 de la Constitución, se ejercerá con arreglo a lo establecido en el Reglamento (UE) 2016/679 y en esta ley orgánica*". También añade que pretende "*Garantizar los derechos digitales de la ciudadanía conforme al mandato establecido en el artículo 18.4 de la Constitución.*".

En definitiva, la protección de datos pretende salvaguardar datos de carácter personal, entendidos como tal, según se define en el artículo 4.1 del RGPD, *"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"*.

La diferencia entre datos personales y no personales se explica resumidamente como cualquier dato que identifica y que es capaz de identificar a cualquier persona física. Ciertos datos que no son de carácter personal, si son recopilados de forma conjunta, es decir, si aún sin ser de carácter personal se recogen a la vez en un momento concreto, entonces pueden constituir información que puede identificar a una persona y, por lo tanto, considerarse datos personales y, por consiguiente, información identificable.

Se considera datos personales, por lo tanto, cualquier información (numérica, fotográfica, acústica, alfabética, o de cualquier tipo) correspondientes a personas físicas identificadas o identificables, ya se refieran a su identidad como a su ocupación y existencia. Algunos de los ejemplos más comunes de datos personales son: nombre y apellidos de la persona física, domicilio o dirección de residencia, dirección de correo electrónico, número de documento nacional de identidad (DNI), los datos en poder de un hospital o médico, etcétera. Además, de aquellos datos relacionados con las nuevas tecnologías y los cambios en la digitalización de los medios, como son los datos de localización (referido a los datos correspondientes a la función de localización de los *smartphones*[4]), dirección

[4] Smartphone: Terminal móvil que ofrece servicios avanzados de comunicaciones (acceso a internet y correo electrónico), así como servicios de agenda y organizador personal con un mayor grado de conectividad que un terminal móvil convencional. (Diccionario del Español Jurídico, RAE).

de protocolo de internet (IP)[5], el identificador de una *cookie*[6] y el identificador de la publicidad del teléfono.

Los datos personales que hayan sido anonimizados, es decir, forma de eliminación de posibilidades para identificación de las personas, o cifrados también serán considerados datos personales, siempre que puedan utilizarse para volver a identificar a una persona y, por lo tanto, se encuentran en el ámbito de aplicación del RGPD, en caso de no poder utilizarse para identificar a una persona, no serán datos personales.

Tal y como se define en una guía emitida por la AEPD, "*la finalidad del proceso de anonimización es eliminar o reducir al mínimo los riesgos de reidentificación de los datos anonimizados manteniendo la veracidad de los resultados del tratamiento de los mismos, es decir, además de evitar la identificación de las personas, los datos anonimizados deben garantizar que cualquier operación o tratamiento que pueda ser realizado con posterioridad a la anonimización no conlleva una distorsión de los datos reales*"[7].

No obstante, no hay que olvidar que el RGPD, en su artículo 1.1 no sólo protege los datos de carácter personal sino también su tratamiento: "*El presente Reglamento establece las normas relativas a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y las normas relativas a la libre circulación de tales datos."* Entendiendo como "tratamiento", según el artículo 4.2 del RGPD, *"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*".

El objeto principal de la regulación de la protección de datos de carácter personal y el tratamiento es garantizar y proteger los derechos de las personas físicas a los que correspondan, en especial proteger la libertad, intimidad y honorabilidad de estas personas.

Inicialmente se pensaba que los riesgos y el peligro de tratar datos sólo se producía por su tratamiento informático, pero con los años y el uso de datos se comprobó que esto no era así y que el problema también se puede producir por un tratamiento manual.
Por lo mencionado anteriormente, la Protección de Datos Personales se encuentra vinculado en el ámbito de estudio del Derecho Informático, ya que como hemos observado se trata del control sobre la información de dichos datos personales

[5] IP es la sigla de Internet Protocol o, en nuestro idioma, Protocolo de Internet. Se trata de un estándar que se emplea para el envío y recepción de información mediante una red que reúne paquetes conmutados. PÉREZ PORTO, J., & MERINO, M. Definición.DE. 2012.

[6] Una cookie es un archivo creado por un sitio web que contiene pequeñas cantidades de datos y que se envían entre un emisor y un receptor. En el caso de Internet el emisor sería el servidor donde está alojada la página web y el receptor es el navegador que usas para visitar cualquier página web. Su propósito principal es identificar al usuario almacenando su historial de actividad en un sitio web específico, de manera que se le pueda ofrecer el contenido más apropiado según sus hábitos. GONZÁLEZ, G. Qué son las cookies de tu navegador y para qué sirven. Blogthinkbig.com. 2014.

[7] Agencia Española de Protección de datos. "1. ANONIMIZACIÓN", en *Orientaciones y garantías en los procedimientos de anonimización de datos personales*, España, 2016, p. 2.

almacenados que permitan la utilización de los mismos, ya sean datos albergados en sistemas informáticos o en papel, se trata de datos en cualquier soporte que permita ser utilizados.

La protección de las personas físicas en relación con el tratamiento de cualquier dato de carácter personal se encuentra vinculado a otros derechos como el secreto de las comunicaciones realizadas por cualquier medio informático, así como por cualquier medio manual.

El Tribunal Superior de Justicia de Andalucía en su Sentencia núm. 1619/2003, de 9 de mayo refleja la relación entre estos derechos a los que denomina "derechos de tercera generación"[8]:

"*Ante todo, es interesante destacar que las novedades informáticas y telemáticas están obligando a una nueva clasificación de los derechos fundamentales, no bastando la distinción entre derechos individuales o libertades y derechos sociales o prestacionales, naciendo así derechos o libertades llamados de «tercera generación», constituidos por las garantías del individuo frente a la contaminación o deterioro que las libertades pueden sufrir por las nuevas tecnologías. Entre esos derechos se incluirían el secreto de las comunicaciones informáticas y telemáticas, la intimidad informática y el derecho a la autodeterminación informativa, formando un conjunto que me atrevería a denominar de «libertades informáticas».*

(…) En efecto, los dos primeros –el secreto de las comunicaciones y la intimidad informáticas – son examinados por algunos autores y por la doctrina del Tribunal Constitucional como meras manifestaciones singulares de los derechos reconocidos en los apartados correspondientes del art. 18 CE (RCL 1978, 2836)".

Es por ello por lo que, el derecho a la protección de datos está configurado en nuestro ordenamiento jurídico como un derecho fundamental, reconocido así en el artículo 18.4 de la Constitución Española y que ha sido llamado como "libertad informática", ya que como dice la Sentencia 254/1993, de 20 de julio de 1993, "*La «libertad informática», reconocida por el art. 18.4 de la Constitución, ya no es la libertad de negar información sobre los propios hechos privados o datos personales, sino la libertad de controlar el uso de esos mismos datos insertos en un programa informático*".

Tal y como se ha reflejado en el preámbulo de la LOPDGDD "*La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental protegido por el artículo 18.4 de la Constitución española. De esta manera, nuestra Constitución fue pionera en el reconocimiento del derecho fundamental a la protección de datos personales cuando dispuso que «la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos»*".

El Tribunal Constitucional señaló en su Sentencia 94/1998, de 4 de mayo, que nos encontramos ante un derecho fundamental a la protección de datos por el que se garantiza

[8] PÉREZ LUÑO, Antonio Enrique, *La tercera generación de los derechos humanos*, Thomson-Aranzadi, Navarra, 2006.

a la persona el control sobre sus datos, cualesquiera datos personales, y sobre su uso y destino, para evitar el tráfico ilícito de los mismos o lesivo para la dignidad y los derechos de los afectados; de esta forma, el derecho a la protección de datos se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención. Por su parte, en la Sentencia 292/2000, de 30 de noviembre, lo considera como un derecho autónomo e independiente que consiste en un poder de disposición y de control sobre los datos personales que faculta a la persona para decidir cuáles de esos datos proporcionar a un tercero, sea el Estado o un particular, o cuáles puede este tercero recabar, y que también permite al individuo saber quién posee esos datos personales y para qué, pudiendo oponerse a esa posesión o al uso de los mismos[9].

Hay que considerar que tanto el derecho a la protección de datos como el derecho a la intimidad son derechos diferentes, aunque pretendan proteger lo mismo, la dignidad de las personas. Es decir, aquella información que las personas consideran como íntima o no, en relación con la protección de datos, debe ser brindada la protección de dicha información, así como su control.

Expresado de otro modo, el derecho fundamental a la protección de datos establecido en el artículo 18.4 de la Constitución Española, está estrechamente relacionado con otro de los derechos fundamentales, el derecho a la intimidad personal y familiar de los ciudadanos, pero son derechos fundamentales diferentes y autónomos.

Tal y como refleja Pérez Royo "*lo que con este derecho se pretende es que la persona pueda controlar el acceso a y la divulgación de información sobre su vida privada. (…) El derecho a la intimidad resulta vulnerado por la imputación de un hecho susceptible de ser integrado en la esfera íntima y personal de un ciudadano, por muy veraz que sea. Es el consentimiento propio el elemento decisivo. Si hay consentimiento, no hay violación. Si no hay consentimiento, en principio la hay*"[10].

De hecho, según el criterio del anterior autor citado "*el derecho a la intimidad protege la intimidad en todos sus aspectos, no sólo la intimidad "informativa"*". Esto es, "*el derecho independientemente de que esa entrada no nos ocasione ningún daño y de que no le proporcione información a esos otros que pueda ser perjudicial para nosotros*"[11].

Es decir, el derecho a la intimidad está estrechamente vinculado con el derecho de protección de datos, siendo ambos derechos fundamentales, uno consecuencia del otro. Este derecho tiene el fin de regular esa "intimidad informativa", la cual se configura como la posibilidad de que el individuo pueda determinar cuándo, cómo y con qué alcance se va a transmitir información sobre el mismo a los demás.

[9] Sentencia del Tribunal Constitucional 292/2000, de 30 de noviembre de 2000 (BOE núm. 4, de 4 de enero de 2001).
[10] PÉREZ ROYO, Javier, *Curso de derecho constitucional*, Marcial Pons, Madrid, 2018, p. 294.
[11] PÉREZ ROYO, Javier, *Curso de derecho constitucional*, Marcial Pons, Madrid, 2018, p. 295.

A pesar de la vinculación entre el derecho a la intimidad y el derecho a la protección de datos de carácter personal, tenemos que tener presente que se trata de dos derechos fundamentales e independientes uno del otro[12].

Concluimos por lo tanto que la protección de datos de carácter personal es un derecho fundamental de las personas físicas. Es decir, un derecho que pretende brindar la protección de la información personal, la cual puede ser considerada íntima, y el tratamiento de los datos propiedad de estas personas físicas frente a las vulneraciones de tales derechos por parte de empresas o entidades que puedan recoger y almacenar los datos personales de estas.

2.2. Regulación de la protección de datos

2.2.1. Antecedentes al Reglamento General de Protección de Datos

Con anterioridad a la entrada del nuevo RGPD, la norma reguladora de la Protección de datos era 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. Junto con esta normativa europea, convivía en España la Ley Orgánica 15/1999, de 13 de diciembre (LOPD).

Desde que España es miembro de la Unión Europea, la normativa comunitaria debe ser aplicada a todos los Estados miembros. Por ello, la entrada en vigor del nuevo Reglamento de Protección de datos es de aplicación en el Estado español. No obstante, el nuevo Reglamento no deroga la normativa nacional, permitiendo así que convivan ambas normas en lo que no la contradiga. De esta forma, todo lo que no se encuentre regulado por la normativa europea (RGPD), habrá que estar a lo dispuesto en la actual LOPDGDD desde la entrada en vigor el 7 de diciembre de 2018, tras la derogación de la LOPD.

Como venimos diciendo, este nuevo giro normativo y necesario surge de las continuas relaciones comerciales, cada vez más globales, con un intercambio cada vez mayor, de datos personales. Tal y como recoge los considerandos del nuevo Reglamento:

"*(5) La integración económica y social resultante del funcionamiento del mercado interior ha llevado a un aumento sustancial de los flujos transfronterizos de datos personales. En toda la Unión se ha incrementado el intercambio de datos personales entre los operadores públicos y privados, incluidas las personas físicas, las asociaciones y las empresas. El Derecho de la Unión insta a las autoridades nacionales de los Estados miembros a que cooperen e intercambien datos personales a fin de poder cumplir sus funciones o desempeñar otras por cuenta de una autoridad de otro Estado miembro.*

(6) La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales ha aumentado de manera significativa. La tecnología permite que tanto las empresas privadas como las autoridades públicas utilicen datos personales en una escala sin precedentes a la hora de realizar sus actividades. Las personas físicas difunden un volumen cada vez mayor de información personal a escala mundial. La tecnología ha

[12] DEL PESO NAVARRO, Emilio, *Servicios de la sociedad de la información*, Diaz de Santos, Madrid, 2003, p. 59.

transformado tanto la economía como la vida social, y ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

(7) Estos avances requieren un marco más sólido y coherente para la protección de datos en la Unión Europea, respaldado por una ejecución estricta, dada la importancia de generar la confianza que permita a la economía digital desarrollarse en todo el mercado interior. Las personas físicas deben tener el control de sus propios datos personales. Hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas".

Explicado principalmente por el incremento de las transacciones comerciales entre países miembros de la Unión Europea, y ante el riesgo de intercambio de datos con países fuera de la Unión Europea, el RGPD ha llegado a convertirse en un ejemplo de norma de seguridad para la protección y tratamiento de datos, ya que dicho Reglamento prohíbe compartir datos de carácter personal a cualquier país que esté considerado como un país de un nivel de protección de datos por debajo de unos estándares de calidad establecidos por la Unión Europea[13]. El RGPD establece excepciones siempre que el país esté dispuesto a cumplir, y por supuesto, lo hacen, con los principios y estándares de calidad establecidos en dicho Reglamento. Tal y como establece la Unión Europea la protección ofrecida por el Reglamento acompaña a los datos de carácter personal cuando se transfieran fuera de la Unión Europea. Es decir, las empresas que transfieran datos al extranjero de la UE deben garantizar que se cumpla alguna de las siguientes condiciones: la protección de datos del país tercero es adecuada, se toma por parte de las empresas las oportunas salvaguardas o existen excepciones a las que se acoge la empresa como el consentimiento del interesado.

Destacamos cinco novedades principales que consideramos relevante de este nuevo Reglamento establecido:

- **Delegado de Protección de Datos**: Se incorpora en el nuevo Reglamento la figura del Delegado de Protección de Datos (DPO) obligatoria en las entidades públicas y recomendables en todas las sociedades, aunque en algunas de ellas, en función de la información que manejen también es obligatoria. En la anterior normativa esta figura no era obligatoria, aunque era obligatorio la designación de un responsable de seguridad (ver apartado 2.2.3.)[14].

- **Nuevos derechos**: La LOPD establecía para los interesados de los datos personales cuatro derechos, conocidos en España como derechos ARCO: Acceso, Rectificación, Cancelación y Oposición. Pero con el nuevo Reglamento se incluyen adicionalmente otros cuatro derechos:
    - Derecho a la transparencia y comunicación de la información[15].
    - Derecho de supresión («el derecho al olvido»)[16].

[13] Art. 44 RGPD.
[14] Art. 37.1 RGPD.
[15] Art. 12 RGPD.
[16] Art. 17 RGPD.

- Derecho a la limitación del tratamiento[17].
- Derecho a la portabilidad de los datos[18].

Analizamos estos derechos más en profundidad en el apartado 2.2.3.

- **Obtención del consentimiento**: El Reglamento establece que para considerar que el consentimiento es inequívoco, deberá existir un consentimiento expreso del interesado o una acción positiva manifestando así su conformidad (ver apartado 2.2.3.).

- **Análisis de riesgos y evaluación de impactos**: El nuevo Reglamento ha establecido que son las entidades públicas o privadas las que tienen la responsabilidad del diseño y la adopción de medidas organizativas y técnicas, por ello, consideramos que es imprescindible que estas, realicen un análisis de riesgos y, por consiguiente, la evaluación de impactos de estos. Además, esta evaluación de impactos se establece obligatoria para las entidades que realicen tratamiento de datos (ver apartado 2.2.3.).

- **Incremento de las sanciones**: Antes de la entrada en vigor en mayo de 2018 del nuevo Reglamento las sanciones oscilaban entre un mínimo de 900 euros hasta un máximo de 600.000 euros, según el artículo 45 de la antigua LOPD. Sin embargo, con el nuevo Reglamento, se establece sanciones de entre 10 millones de euros y 20 millones de euros para infracciones consideradas graves y muy graves, pero estas sanciones pueden ser superiores en algunos casos ya que puede alcanzar hasta el 4% de cifra de negocios total anual del ejercicio fiscal correspondiente (ver apartado 2.2.4.).

2.2.2. Titulares y obligados

En este apartado, debemos diferenciar aquéllos que son los titulares de los derechos de protección de datos y quiénes son los obligados a cumplir la normativa de protección de datos establecida.

Entre los primeros, los titulares, se encuentran todas aquellas personas físicas cuyos datos personales hayan sido proporcionados o recogidos para su tratamiento. Es decir, las personas físicas que pueden ser identificadas con los datos personales proporcionados (ver definición de "datos personales" en el apartado 2.1. del RGPD). Estos tienen una serie de derechos que podrán ejercer en cualquier momento durante el tiempo que dure el tratamiento de sus datos personales e incluso posteriormente a la finalización del tratamiento de estos datos. Por ejemplo, cualquier persona cuando compra o realiza una reserva por Internet e introduce sus datos personales para que sean recopilados por la empresa mercantil correspondiente. De igual modo cuando cualquier persona realiza una operación por Internet con cualquier entidad pública e introduce sus datos personales.

[17] Art. 18 RGPD.
[18] Art. 20 RGPD.

Los segundos, los obligados, son aquellas personas físicas o jurídicas que recaben datos personales para su tratamiento o inclusión en fichero, es decir, los responsables y encargados del tratamiento definidos en el artículo 4.7. y 4.8. del RGPD respectivamente.

La diferencia principal entre el responsable y el encargado es que el primero determina los fines y medios del tratamiento, y el segundo, es el que trata los datos personales por cuenta del responsable, sin tomar decisión ninguna sobre los datos. Estos, además, tienen una serie de obligaciones, por lo tanto, tienen que cumplir la normativa vigente. En caso de incumplimiento de éstas, estarán sujetos a sanciones administrativas que se explicarán a continuación (ver punto 2.2.4. Infracciones y sanciones). Pero hay que destacar, que todos estamos obligados a respetar el derecho de la protección de datos de carácter personal y a cumplir la Ley y el Reglamento, pero los referidos anteriormente son los conocidos como "responsables del tratamiento de datos".

Están obligados al cumplimiento del RGPD las entidades mercantiles, administraciones y organismos públicos, asociaciones, autónomos, ONG. Esto es, cualquier persona física o jurídica que trate datos personales.

El RGPD establece diferentes obligaciones para tres figuras: el responsable del tratamiento, el encargado del tratamiento y el Delegado de protección de datos.

El responsable del tratamiento será según se define en el artículo 4.7. del RGPD 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*".

El encargado del tratamiento será según se define en el artículo 4.8. del RGPD como "*la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento*" es decir, a modo de ejemplo, en el caso de la auditoría, el responsable del tratamiento sería la propia empresa auditora, sin embargo, el encargado del tratamiento podría ser una empresa externa, una empresa de informática que se encargue del tratamiento o almacenamiento en sí de los datos recabados por el auditor.

Adicionalmente, los trabajadores que pertenezcan a la organización definida como encargado o responsable del tratamiento serán denominados como usuarios de los datos y deberán cumplir con las políticas internas de protección de datos de la propia organización. Por ejemplo, los trabajadores de la empresa auditora son usuarios de los datos y deben cumplir con las políticas internas de protección de datos de la propia empresa de auditoría. También, un hospital o centro sanitario es responsable del tratamiento de los datos personales de los pacientes, así como de los informes y resultados correspondientes a la visita de estos, estos datos no podrán ser enviados ni al propio paciente, sin solicitud expresa con documento de identidad adjunto.

El Delegado de protección de datos es una figura de nueva creación que surge con el nuevo Reglamento y cuya regulación se encuentra entre los artículos 37 y 39 del mismo.

Se trata de una figura la cual pretende garantizar el cumplimiento normativo de protección de datos en las organizaciones, aunque la responsabilidad sobre el cumplimiento de la normativa incurre en el responsable o encargado. Esta figura siempre será necesaria en organismos públicos y en organismos privados sólo será necesaria en aquellos cuyos datos recogidos sean a gran escala o cumpla con el resto de condiciones establecidas en el artículo 37.1.[19] A grandes rasgos, el Delegado de protección de datos se encargará de las funciones principales recogidas en el artículo 39[20] entre las que se encuentra *"informar y asesorar al responsable o al encargado del tratamiento…"*; *"supervisar el cumplimiento de lo dispuesto en el presente Reglamento…"*, es decir, velar por el cumplimiento del Reglamento por parte del responsable y encargado del tratamiento de datos; asesorar sobre cualquier aspecto solicitado; *"cooperar con la autoridad de control"*; y actuar como referente y contacto de la Autoridad de control.

En definitiva, todos aquéllos que tengan acceso a datos personales o se dediquen a determinar los fines y medios del tratamiento, al propio tratamiento o al almacenamiento de estos serán titulares y/u obligados por el RGPD.

2.2.3. Derechos y obligaciones

Los derechos que tienen los interesados con el Reglamento se encuentran regulados en su capítulo III de la citada norma en los artículos del 15 al 22. Estos derechos son los de acceso, rectificación, olvido o supresión, limitación, derecho a la transparencia, portabilidad y oposición.

Es interesante este punto, no sólo por la importancia del mismo, sino porque los derechos han sido modificados con el Reglamento, o, mejor dicho, los derechos han sido ampliados con respecto a los que el interesado tenía reconocido en la anterior normativa.

---

[19] "*1.El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que: a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10."* Art. 37 RGPD.

[20] "*1.El delegado de protección de datos tendrá como mínimo las siguientes funciones: a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros; b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes; c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35; d) cooperar con la autoridad de control; e) actuar como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento, incluida la consulta previa a que se refiere el artículo 36, y realizar consultas, en su caso, sobre cualquier otro asunto. 2.El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento."* Art. 39 RGPD.

Los derechos que venían recogidos en la LOPD, en sus artículos del 13 al 19 (y que son los que recogía la Directiva anterior), sólo se incluían los de acceso, rectificación, oposición y cancelación (los ARCO como mencionamos anteriormente). Por lo que, con la nueva normativa, se han incluido derechos tan importantes como el derecho a la transparencia, el de olvido o supresión, limitación del tratamiento y portabilidad. Al igual que ya se recogen en la nueva LOPDGDD, el RGPD recoge estos nuevos derechos referentes a la transparencia, olvido o supresión y limitación y portabilidad en los artículos 12, 17 y 18, respectivamente.

El derecho a la transparencia y comunicación de la información definido en el artículo 12 del RGPD, se menciona como "*Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado*" y hace referencia a que los responsables de los tratamientos de los datos deben facilitar a los interesados toda la información cuando los datos se obtengan del interesado. En concreto, el mencionado artículo dice que "*El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13*[21] *y 14*[22]*, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios*".

En lo que se refiere al derecho al olvido o supresión, recogido concretamente en el artículo 17 del RGPD, "*El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan*", es decir, el interesado podrá solicitar la supresión de los datos personales que a él le conciernan cuando se den determinadas circunstancias entre las que se encuentran, por ejemplo, las siguientes:

[21] *1.Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento; d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado*. […]. Art. 13 RGPD.

[22] *1.Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información: a) la identidad y los datos de contacto del responsable y, en su caso, de su representante; b) los datos de contacto del delegado de protección de datos, en su caso; c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento; d) las categorías de datos personales de que se trate; e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso; f) en su caso, la intención del responsable de transferir datos personales a un destinatario en un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de ellas o al hecho de que se hayan prestado.* […]. Art. 14 RGPD.

- Cuando los datos personales ya no sean necesarios.
- Cuando el interesado retire el consentimiento (siempre que esa fuera la base del tratamiento).
- Cuando los datos personales hayan sido tratados ilícitamente.
- Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal.

Además, en dicho derecho, se menciona que, aunque los datos hayan sido publicados, en caso de estar obligado a suprimirlo, el responsable del tratamiento de datos deberá tomar los medios necesarios para eliminarlos. Exactamente el artículo 17.2 del RGPD lo menciona de la siguiente forma "*Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos*".

Por contrario el artículo 17.3, especifica que los apartados 1 y 2 del mencionado artículo no se aplicarán cuando el tratamiento sea necesario para determinados casos, entre ellos, ejercer el derecho a la libertad de expresión e información o por razones de interés público.

En lo que respecta al derecho de limitación del tratamiento, en virtud del artículo 18 del RGPD, "*El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes: a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos; b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso; c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones; d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado*".

Es decir, se podrá limitar el tratamiento de datos personales cuando se cumplan determinadas condiciones. Como, por ejemplo, en caso de ser inexactos los datos, en caso de ilicitud o cuando el interesado lo solicite para reclamar o ejercer su derecho de oposición. Sin embargo, también se matiza que cuando estos datos personales hayan sido limitados según lo mencionado anteriormente, solo podrán ser objeto de tratamiento con el consentimiento expreso del interesado. Y, además, previamente al levantamiento de la limitación de los datos el interesado deberá ser informado.

Por último, el nuevo derecho introducido, el de portabilidad, recogido en el artículo 20 del RGPD, establece que "*el interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando: a)*

el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y b) el tratamiento se efectúe por medios automatizados.". Este artículo viene a indicar que el interesado tendrá derecho a recibir los datos facilitados al encargado del tratamiento de datos, en un formato legible. Es decir, estructurado, en un formato común y de lectura mecánica siempre y cuando el tratamiento esté basado en el consentimiento y se haya efectuado por medios automatizados. Este artículo estima que tal derecho no se aplicará cuando sea necesario para el cumplimiento de la realización de una misión de interés público. Además, este derecho "*no afectará negativamente a los derechos y libertades de otros*".

Por otro lado, consideramos que las obligaciones más destacadas con la entrada en vigor del nuevo Reglamento son las siguientes: seguridad del tratamiento de los datos de carácter personal, evaluación del impacto relativo a la protección de datos, designación de un Delegado de protección de datos y la posibilidad de aprobar códigos de conducta.

Para poder tratar los datos y de manera previa a las medidas de seguridad y diferentes obligaciones detalladas anteriormente, tanto los responsables como los encargados deben cumplir los principios relativos al tratamiento y la licitud del tratamiento definidos en el artículo 5 y 6 del RGPD, respectivamente. Los principios destacan la necesidad de que los datos de carácter personal sean tratados de manera lícita, leal y transparente en relación con el interesado; se recojan con fines determinados, legítimos y explícitos y por consiguiente, sean tratados con estos fines; que sean limitados a estos fines y exactos, siendo actualizados cuando sea necesario; y además, que se traten de manera que la seguridad de dichos datos sea adecuada. Por otro lado, se especifica que el tratamiento solo será lícito si se cumple al menos una de las condiciones detalladas en el artículo 6 del RGPD entre las que destaca el consentimiento del interesado para uno o varios fines específicos, la necesidad del tratamiento de estos datos para la ejecución de un contrato en el cual el interesado está implicado o el tratamiento es necesario para la protección de intereses vitales del interesado u otra persona física.

Los responsables y encargados del tratamiento de datos de carácter personal tendrán que aplicar una serie de medidas adecuadas, tanto técnicas como organizativas, que garanticen un adecuado nivel de seguridad de los datos expuestos a los diferentes riesgos. El artículo 32 del RGPD detalla algunas propuestas para garantizar esta seguridad de los datos: "*la seudonimización y el cifrado de datos personales; la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento; la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico; un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento*".

Previamente a la implantación de las medidas de seguridad y para, posteriormente, tener una correcta evaluación del nivel de seguridad alcanzado con las medidas adoptadas, es recomendable realizar un análisis de los riesgos a los cuales están expuestos los datos personales. Este análisis de los riesgos es importante que sea realizado por los

responsables del tratamiento detectando el riesgo, la probabilidad y el impacto del mismo[23].

Por otro lado, la Agencia Española de Protección de Datos (en adelante AEPD) ha trabajado en la realización de un esquema de certificación de Delegado de protección de datos en el cual se detalla que el asesorar sobre el análisis de riesgo de los tratamientos realizados es una de las funciones genéricas del Delegado de protección de datos[24]. En este esquema, también se especifica la implantación de las medidas de seguridad adecuadas a los riesgos, así como la evaluación del riesgo para los derechos y libertades de los afectados. En resumen, lo que se establece es un análisis de los riesgos, una implantación de medidas de seguridad y una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

Es en la evaluación del impacto en la que nos detenemos a continuación. En el apartado 1 del artículo 35 del RGPD se establece que "*cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares*". Es decir, con el análisis de riesgos realizado y con los tratamientos a adoptar, el responsable deberá evaluar el impacto relativa a la protección de datos recabando el asesoramiento del Delegado de protección de datos designado.

En este aspecto, la AEPD también ha desarrollado una guía para las evaluaciones de impacto en la cual se define la evaluación de impacto de la protección de datos personales como "*una herramienta que permite evaluar de manera anticipada cuáles son los potenciales riesgos a los que están expuestos los datos personales en función de las actividades de tratamiento que se llevan a cabo con los mismos. El análisis de riesgos para un determinado tratamiento permite identificar los riesgos que se ciernen sobre los datos de los interesados y establecer una respuesta adoptando las salvaguardas necesarias para reducirlos hasta un nivel de riesgo aceptable*"[25]. En esta guía se ha establecido las bases y aspectos principales que los obligados a la realización de una evaluación de impacto deberán tener en cuenta. También se establece en el artículo 35 del RGPD los requisitos mínimos que deberá tener una evaluación de impacto. Siendo obligatorio incluir:

- "*Una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento*".
- "*Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad*".
- "*Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad*".
- "*Las medidas previstas para afrontar los riesgos*".

[23] Art. 35 RGPD.
[24] Agencia Española de Protección de Datos, *Esquema de certificación de delegados de protección de datos*, 13 de junio de 2018.
[25] Agencia Española de Protección de Datos. "1. Introducción", en *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*, España, 2018, p. 2.

Es en los siguientes casos establecidos en el apartado 3 del artículo 35 del RGPD en los que será requerida la evaluación del impacto: "*a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o c) observación sistemática a gran escala de una zona de acceso público*".

Otra obligación considerada en el RGPD es la designación de un Delegado de protección de datos. En el Reglamento se define esta nueva figura en una sección entera, donde se detalla la designación, la posición y las funciones. Pero esta figura no es obligatoria para todas las compañías, el artículo 37 del RGPD expone que es obligatorio la designación de un DPO en los siguientes casos: "*el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial; las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9*[26] *y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10*[27]".

En el sector privado, es importante identificar si la empresa tiene la obligación de designar a un DPO, establecida en el artículo 37 del RGPD, ya que, en caso de estarlo y no hacerlo, podría tener una sanción de hasta 10 millones de euros, tal y como establece el artículo 83.4 a) del RGPD. Por lo que resumidamente, están obligados los organismos, entidades, o empresas públicas (a excepción de los tribunales que actúen en ejercicio de su función judicial, los cuales, aunque no están obligados, de manera voluntaria pueden nombrar un DPO); las empresas que realicen una observación sistemática y habitual de personas a gran escala o por último, si la empresa maneja a gran escala categorías especiales de datos personales[28], conocidos como "datos sensibles".

Esta designación tal y como se establece en el Reglamento, debe ser realizada por el responsable y el encargado del tratamiento de los datos. El cual matiza que si este responsable o encargado es una autoridad u organismo público y el tamaño y estructura organizativa lo permite, se podrá designar un único DPO para varias de estas autoridades u organismos.

---

[26] *1.Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.* […]. Art. 9 RGPD.

[27] *El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.* Art. 10 RGPD.

[28] Art. 9 RGPD.

El tamaño de la empresa o la facturación de esta no influye en la exigencia de designar a un DPO, es el nivel o tipo de tratamiento de datos que tenga sobre sus clientes. Por ejemplo, una empresa *E-Commerce*[29], aunque tenga una pequeña dimensión, podría estar obligada ya que realiza un tratamiento exhaustivo y sobre gran cantidad de datos.

También se matiza en el punto 2 del artículo 37 que "*Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento*". Es decir, por ejemplo, el Grupo Inditex, podría nombrar un único DPO siempre y cuando cualquier establecimiento perteneciente a dicho grupo pueda estar en contacto fácilmente con éste.

El Reglamento menciona que el DPO debería ser designado "*atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho*" y por supuesto, a su experiencia en el ámbito de protección de datos.

De acuerdo con el apartado 6 del artículo 37 el DPO "*podrá formar parte de la plantilla del responsable o del encargado del tratamiento*", aunque, por otro lado, también podría ser externo y ser contratado para prestar sus servicios.

Por último, en aquellas entidades u organismos que existan códigos de conductas deberán ser modificados o ampliados para incluir apartados que contribuyan a la correcta aplicación del RGPD. En los casos que no existan, se promoverá la elaboración de estos con los correspondientes aspectos para la correcta aplicación del Reglamento. En ambos casos tal y como se especifica en el Reglamento, se tendrá en cuenta tanto las características de los diferentes sectores de tratamiento como las necesidades específicas de las empresas de menor dimensión. Un organismo "*que tenga el nivel adecuado de pericia en relación con el objeto del código*"[30] efectuará el control obligatorio del cumplimiento de las disposiciones del código de conducta por los responsables o encargados de tratamiento que se comprometan a aplicarlo mediante los mecanismos que contenga el propio código.

2.2.4. Infracciones y sanciones

Como hemos dicho anteriormente, aquellos responsables, y/o encargados, del tratamiento de datos personales tienen una serie de obligaciones reguladas por el RGPD y, en caso de incumplimiento, de las mismas, el RGPD prevé sanciones administrativas. Aunque también será sancionado cualquier sujeto que trate datos de carácter personal de forma ilícita, como un titular o sujeto privado que, por ejemplo, graba a otro sujeto sin su consentimiento.

Hay que tener en cuenta que estas sanciones no son únicamente para responsables y encargados del tratamiento de datos sino para cualquier persona que lesione o incumpla con el RGPD y la LOPDGDD.

[29] El e-commerce consiste en la distribución, venta, compra, marketing y suministro de información de productos o servicios a través de Internet. RODRÍGUEZ MERINO, Cristina. *¿Qué es E-commerce o comercio electrónico?* En Blog del Máster en Marketing Directo y Digital de la UPF Barcelona School of Management. 12 de agosto de 2015.
[30] Art. 41 RGPD.

El artículo 84, prevé la posibilidad que cada Estado miembro regule no sólo el tipo de sanciones sino también la forma de controlarlas. En el caso de España, hasta el momento, las sanciones son las mismas, multas administrativas, con la única diferencia dependiendo de si se trata de ficheros de titularidad pública o privada, la diferencia se centra básicamente en las obligaciones asumidas por el sector público o por el privado, siendo más estrictos para el sector público y para quienes se relacionan con el mismo. Si se trata de ficheros de titularidad pública, desde el pasado 6 de noviembre de 2019, entraron en vigor las modificaciones introducidas en la Ley de Contratos del Sector Público, por el Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones. Esta modificación, refuerza el cumplimiento de las disposiciones nacionales y comunitarias en materia de protección de datos en el ámbito de la contratación pública. De este modo, los contratistas en relación a la protección de datos asumen obligaciones específicas, cuando el contrato celebrado entre las partes implique el tratamiento de datos por cuenta del responsable; y también, cuando haya por parte de entidades u organismos del sector público cesión de datos al contratista. Estas obligaciones pasan a tener el carácter de esenciales y el incumplimiento de estas, podrá dar lugar a la nulidad del contrato, la resolución del contrato y, además, incluso si esta fuera calificada de culpable podría conllevar una prohibición de contratar con las entidades del sector público.

En la LOPDGDD, las infracciones se dividen en leves, graves y muy graves. Según el artículo 72 de la LOPDGDD, se consideran infracciones muy graves aquellas que supongan una vulneración sustancial de los artículos mencionados en el artículo 83.5 del RGPD, prescribiendo estos a los tres años. Además, se consideran también, entre otros, las siguientes: la vulneración de los principios relativos al tratamiento como que los datos personales serán tratados de manera lícita, leal y transparente, recogidos con fines determinados, explícitos y legítimos o que los datos serán adecuados y exactos; el incumplimiento de los requisitos exigidos para la validez del consentimiento recogidos en el artículo 7 del RGPD; la utilización de los datos para otra finalidad que no sea compatible con aquella para la cual fueron recogidos; la vulneración del deber de confidencialidad establecido en el artículo 5 de la LOPDGDD; o no facilitar el acceso a la autoridad de protección de datos competentes a los datos personales.

Respecto a las infracciones graves se considerarán y tendrán también el mismo periodo de prescripción las infracciones a las que se refiere el artículo 83.6 del RGPD.

Por otro lado, en el artículo 73 de la LOPDGDD se establece la consideración de las infracciones como graves. Según este artículo se consideran infracciones graves las infracciones que supongan una vulneración sustancial de los artículos mencionados en el artículo 83.4 del RGPD y en concreto, entre otras, las siguientes:

"*El tratamiento de datos personales de un menor de edad sin recabar su consentimiento…"*; *"No acreditar la realización de esfuerzos razonables para verificar la validez del consentimiento prestado por un menor de edad…"*; *"La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento…"*; *"incumplimiento de la obligación de designar un representante del responsable o encargado del tratamiento no*

establecido en el territorio de la Unión Europea…"; *"Que el encargado de tratamiento que no ofrezca las garantías suficientes para aplicar las medidas técnicas y organizativas apropiadas…"*; *"contratación por un encargado del tratamiento de otros encargados sin contar con la autorización previa del responsable…"*; *"No disponer del registro de actividades de tratamiento…"*; *"No cooperar con las autoridades de control en el desempeño de sus funciones…"*; *"No posibilitar la efectiva participación del delegado de protección de datos en todas las cuestiones relativas a la protección de datos personales…"*; o *"utilización de un sello o certificación en materia de protección de datos que no haya sido otorgado por una entidad de certificación…".*

Estas infracciones, consideradas como graves en el artículo 73 de la LOPDGDD prescribirán a los dos años.

Por último, según el artículo 74 de la LOPDGDD, se catalogan como leves y prescriben al año de producirse las infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del RGPD, y en concreto, las siguientes: incumplimiento del principio de transparencia de la información o la exigencia del pago de un canon para facilitar al afectado información como identidad y datos de contacto del responsable o del delegado de protección de datos; no atender a los derechos de acceso, rectificación, supresión… así como el incumplimiento de la obligación de notificación relativa a la rectificación o supresión; el incumplimiento de informar al afectado, si este lo solicitara, los destinatarios a los que se le haya facilitado los datos; la notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales; o la no publicación de los datos de contacto del delegado de protección de datos cuando su nombramiento sea exigible.

Las infracciones se sancionarán con multas administrativas de entre 10.000.000 de euros o si es una empresa con una multa de una cuantía del 2% de la cifra de negocios anual del ejercicio anterior como máximo si se trata de infracciones según lo establecido en el artículo 83.4 del RGPD. Como máximo podrán ascender a 20.000.000 de euros o el 4% de la cifra de negocios si se trata de una empresa, de acuerdo con disposiciones establecidas en el artículo 83.5 del RGPD.

La cuantía de las sanciones se graduará atendiendo a una serie de criterios recogidos en el artículo 76.2 de la LOPDGDD, adicionalmente a los establecidos en el artículo 83.2 del RGPD, entre los que se encuentra la continuidad de la infracción, el grado de intencionalidad, el beneficio obtenido como consecuencia de la infracción, la afectación a los derechos de los menores, el volumen de los tratamientos efectuados o incluso el disponer de un delegado de protección de datos cuando no fuera obligatorio.

Como resumen y tras haber leído sanciones por diferentes motivos interpuestas, se extraen los principales motivos por los cuales las Autoridades de control están interponiendo estas sanciones: el incumplimiento de los principio relativos al tratamiento establecidos en el artículo 5 del Reglamento; la no atención a los derechos de los interesados sobre protección de datos; la falta de transparencia; la violación y rotura de seguridad, y en especial, la no notificación de estas; y la falta de un contrato de encargo de tratamiento que regule la relación entre los responsables y encargados del tratamiento

de datos personales[31]. Sin embargo, las multas impuestas en 2019 han descendido en un 70% respecto a las impuestas en 2018, alcanzando este año más de seis millones de euros en multas en comparación con los trece millones del ejercicio anterior[32].

3. INCIDENCIA DEL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN LA AUDITORÍA DE CUENTAS

El RGPD es de aplicación para todos aquellos que trabajen con información que contenga datos de carácter personal como es el caso de los auditores y las firmas de servicios dedicadas a la auditoría.

Consideramos que, en relación con el tema de este trabajo, es decir, con la implicación en la auditoría, más allá de las obligaciones de los auditores, los derechos que se ejercerán más frecuentemente son los referidos en el artículo 15 del RGPD "*Derecho de acceso del interesado*" y el artículo 17 del RGPD "*Derecho de supresión («el derecho al olvido»)*".

Este Reglamento como ya hemos analizado anteriormente, incluye una serie de cambios y obligaciones de los procedimientos que actualmente tienen que seguir auditores y firmas de auditoría en el tratamiento de datos de carácter personal, tanto en la prestación de los servicios profesionales a clientes, como en la prestación de servicios internos en cada una de las firmas. En ambos casos deben ser comunicados, a clientes y usuarios. E internamente, deberá haber una comunicación a los trabajadores pertenecientes a dicha firma de auditoría.

Aunque nos centraremos principalmente en la afectación de la normativa de protección de datos de carácter personal en los servicios profesionales a clientes, internamente, las firmas de auditoría deben comunicar las obligaciones de cada uno de los trabajadores que deben asumir cuando se tratan datos de carácter personal en el día a día de cada profesional. No podemos olvidar que una firma de auditoría también es responsable del tratamiento de los datos personales que maneja. Una firma de auditoría debe realizar comunicaciones periódicas recordando información que los auditores deben tener siempre presente como saber qué es un dato personal, identificar cuándo se están usando datos personales en el trabajo, entender cómo tratar estos datos correctamente e informar de un incidente de seguridad en cuanto se tenga conocimiento de ello. Desde mi experiencia en PricewaterhouseCoopers Auditores (en adelante PwC), periódicamente mediante un mensaje que aparece automáticamente en la pantalla del ordenador de cada trabajador, nos informan y comunican sobre la protección de datos personales, este mensaje debemos de firmarlo para que desaparezca.
Además, cualquier firma de auditoría, desde la publicación del RGPD han hecho hincapié en la importancia de tener en cuenta los principios de: limitar los datos que recopilamos, es decir, recopilar solo los datos que se necesitan y no guardarlos más tiempo del necesario; proteger los datos, asegurándose cada trabajador de que el entorno en el que se

[31] MELIS, Iván. *Aplicando el RGPD: quién, cuánto, cómo, a quién y qué se sanciona*. Disponible en www.tendencias.kpmg.es, España, 2020.
[32] Agencia Española de Protección de Datos. "7. Multas", en *Memoria AEPD 2019*, España, 2019, p. 117.

tratan los datos sea seguro, y de guardarlos en sitios en que queden protegidos, restringiendo el acceso a estos; y respetar los datos que se están utilizando ya que los datos pertenecen a las personas de quienes los recopilamos. Es decir, con el cumplimiento de los principios del Reglamento, los cuales se encuentran regulados en su capítulo II de la citada norma en los artículos del 5 al 11, inclusive.

Por otra parte, en el caso de los servicios profesionales a clientes, se deben producir modificaciones de los contratos con clientes. El acceso a determinada información del cliente por parte de los auditores de cuentas que sea necesaria para la realización de la auditoría se tiene que considerar un ejemplo de acceso a los datos de personas físicas del cliente, ya sea su propio personal, sus accionistas, administradores, los clientes o los propios proveedores, es decir, el cliente de auditoría es a su vez titular de datos personales que deben ser protegidos. Como tal acceso el RGPD, del mismo modo que ocurría con la anterior LOPD y ocurre actualmente con la LOPDGDD, se incluye la necesidad de que este acceso a información esté totalmente recogido en un contrato o cualquier otro documento o acto jurídico[33].

Además, el ICJCE publicó en mayo de 2018 en su página web el informe "¿Qué implicaciones tiene la nueva normativa de protección de datos sobre expertos contables y auditores?"[34] que elaboró el Accountancy Europe (antes Federación Europea de Expertos Contables), entidad de la que forma parte el Instituto, y que pretende ayudar a los auditores a conocer cómo impacta en su trabajo esta nueva normativa. En este informe, se analiza entre otros aspectos, cuándo pueden tratarse datos personales legalmente, qué es importante tener en cuenta con respecto a los derechos sobre los datos de los interesados y cómo los responsables y encargados del tratamiento de datos deberían poder probar que están cumpliendo con sus obligaciones.

3.1. Cumplimiento por parte de los auditores del Reglamento General de Protección de Datos

El Reglamento, como ya hemos visto anteriormente, distingue en sus definiciones entre la figura del "responsable" del tratamiento de datos de carácter personal y de la del "encargado" de tal tratamiento por cuenta de un responsable, a estas definiciones se remite también la actual LOPDGDD. El RGPD incluye la necesidad de que en el contrato de servicios se incorporen una serie de estipulaciones dependiendo de que se trate de un "encargado" o de un "responsable" del tratamiento de datos, es decir, estipulaciones en la cual se detalle la figura que ocupa en relación a los datos cedidos por el cliente, así como los fines de uso de estos.

Siguiendo lo desarrollado en el apartado 2.2.2. *Titulares y obligados*, y en relación al cumplimiento por parte de los auditores del RGPD, es imprescindible aclarar la figura que desempeña en relación con el Reglamento cada uno de los implicados en una auditoría de cuentas.

[33] Art. 6 RGPD y arts. 6 y 12 LOPDGDD.
[34] Accountancy Europe. ¿Qué implicaciones tiene la nueva normativa de protección de datos sobre expertos contables y auditores?. Disponible en www.icjce.es, España, 2018.

La empresa auditora tendrá la consideración del responsable del tratamiento de datos de carácter personal. Por otro lado, el encargado del tratamiento sería una empresa externa, por ejemplo, una empresa informática que se dedique al tratamiento o almacenamiento de datos. Aunque no olvidemos y es necesario mencionar, que esta empresa informática a su vez es responsable del tratamiento de sus propios datos, datos de sus propios trabajadores o clientes, por lo tanto, actuaría en este sentido como encargado del tratamiento de los datos encomendados por la empresa auditora, y como responsable de sus datos propios.

Sin embargo, la figura del encargado del tratamiento no tiene por qué existir siempre, ya que si la empresa auditora, responsable del tratamiento de los datos de la entidad auditada, no externaliza servicios de tratamiento ni almacenamiento a ninguna otra empresa, no existiría la figura de encargado. Como ejemplo cuando un auditor o experto contable conserva y almacena datos personales de sus propios clientes en la nube interna, está actuando como responsable. Sin embargo, el proveedor de servicios de la nube utilizada es, en este supuesto, un encargado ya que trata los datos conservados por el auditor, responsable de los datos. Ahora bien, si el auditor externaliza el tratamiento de datos, sigue manteniendo las responsabilidades, lo que incluye seguir garantizando sobre los datos personales una seguridad adecuada.

Y, por último, mencionar que los trabajadores de la empresa auditora, es decir, los propios auditores o cualquier trabajador de dicha empresa auditora que tenga acceso a los datos de dicha empresa son usuarios de los datos y por lo tanto, deben cumplir con las políticas internas de protección de datos de la propia empresa de auditoría. Por ejemplo, la empresa PwC informa a sus trabajadores de la cláusula de protección de datos de carácter personal que tienen disponible en la intranet y que deben leer y firmar mensualmente.

A continuación, a pesar de lo anteriormente comentado, debemos analizar si un auditor de cuenta, respecto de los servicios que presta, es responsable o es encargado del tratamiento. En este sentido, ante la posibilidad de poder actuar tanto como responsables o como encargados, el ICJCE planteó una consulta a la Agencia Española de Protección de Datos en relación con las dudas existentes (tanto en España como a nivel de la Unión Europea) sobre cómo debía configurarse el auditor de cuentas o cualquier sociedad de auditoría en relación con la entidad auditada, de la cual puede obtener una gran cantidad de datos de carácter personal (DNI de accionistas y empleados, nombres, apellidos, teléfonos…) que tiene que conservar como sus papeles de trabajo[35]. En particular, se plantearon tres diferentes posibilidades al respecto: como responsable de tratamiento de los datos obtenidos de la entidad auditada, como encargado de la misma, o como responsable en unos casos y como encargado en otros, dependiendo de las circunstancias concretas que concurran en cada caso.

En dicha consulta, la consulta número 197282/2018 realizada a la AEPD se plantea la hipótesis de que el auditor de cuenta o empresa de auditoría sea encargado del tratamiento en relación con la entidad auditada, en lugar de responsable del tratamiento, al existir un contrato de servicios entre las partes. Pero la respuesta a dicha consulta de la AEPD (Registro de salida 199679/2018) establece que "*la delimitación entre una y otra figura*

[35] *Contestación de la AEPD a la consulta presentada por el ICJCE sobre el papel del auditor en materia de protección de datos: responsable o encargado* – ICJCE. España, 2018.

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".

Pero adicionalmente, se tiene en consideración, el artículo 12.1 del Real Decreto Legislativo 1/2011, de 1 de julio, por el que se aprueba el texto refundido de la Ley de Auditoría de Cuentas (en adelante la LAC) el cual añade que "*Los auditores de cuentas y las sociedades de auditoría deberán ser independientes…*" y por lo tanto, la revisión y verificación de los datos de la empresa auditada no puede ser restringida a los auditores de cuentas, por lo que con el párrafo descrito anteriormente, el auditor de cuentas realiza el tratamiento de datos en nombre propio, lo cual es determinante para considerar al auditor como responsable del tratamiento en lugar de encargado.

La AEPD concluye que "*la actividad de los auditores de cuentas o sociedades de auditoría en el ejercicio de sus funciones, lo harán en calidad de responsables del tratamiento*".

Por otro lado, aunque la actuación del auditor en la prestación de los servicios de auditoría se rige por la normativa reguladora vigente de la actividad de la auditoría en nuestro país, la cual contiene diferentes medidas como son el secreto profesional, limitaciones sobre el acceso a los diferentes papeles de trabajo, medidas sobre la confidencialidad, conservación y custodia de la documentación perteneciente al auditor de cuentas, las diferentes firmas de auditoría y auditores, también tienen que adaptar su forma de trabajar y documentación, al cumplimiento del RGPD.

Además, junto al deber de confidencialidad exigido por el RGPD, también debemos tener en cuenta las obligaciones respecto de los derechos de propiedad industrial o propiedad intelectual. Así, por ejemplo, existen en propuestas de servicios profesionales de auditoría párrafos referentes a la normativa reguladora de la actividad de la auditoría vigente como el siguiente respecto a los papeles de trabajo del auditor: "*Los papeles de trabajo preparados en relación con la auditoría son propiedad de los auditores, constituyen información confidencial y los mantendremos en nuestro poder de acuerdo con las exigencias de la Normativa reguladora de la actividad de Auditoría de Cuentas. Asimismo, y de acuerdo con el deber de secreto establecido en dicha normativa, nos comprometemos a mantener estricta confidencialidad sobre la información de la entidad obtenida en la realización del trabajo de auditoría, no pudiendo hacer uso de la misma para finalidades distintas de las de la propia auditoría de cuentas, salvo imperativo legal (como sería lo establecido en la Ley 22/2015 de 20 de julio, de Auditoría de Cuentas en su artículo 32 o en el artículo 21 de la Ley 10/2010, de 28 de abril, de prevención del blanqueo de capitales y de la financiación del terrorismo)*"[36].
En función de todo lo anterior, las diferentes firmas de auditoría han actualizado los contratos de servicios con los clientes para incluir modificaciones oportunas, en línea con las exigencias del RGPD, lo que supone la actualización de las diferentes cartas de

[36] PricewaterhouseCoopers Auditores, S.L. Propuesta de servicios profesionales de auditoría, España, 2019.

contratación establecidas con clientes para el cumplimiento de la nueva normativa. Es decir, se tratará de actualizaciones de diferentes cláusulas para adaptarlo al RGPD pero suponemos que no modificaciones ni inclusión de nuevas cláusulas ya que como indicamos anteriormente la obligación de cumplir con la normativa de protección de datos no proviene de la entrada en vigor del RGPD, sino que es anterior, así como las obligaciones o las figuras de responsables y encargados del tratamiento. Por lo tanto, para aquellas contrataciones que ya estaban en vigor previamente a la publicación del nuevo Reglamento, se deberían tener todos los contratos adaptados en consecuencia de las modificaciones, de hecho, en la práctica hay muchos clientes de las diferentes firmas de auditoría que ya han solicitado la actualización y modificación de la cláusula que hace referencia a la protección de datos en las cartas de contrataciones ya firmadas.

Sin embargo, respecto a este punto, hay que entender que debido al volumen tan elevado de contratos que pueden tener vigentes algunas firmas de auditoría como por ejemplo PricewaterhouseCoopers, Deloitte, KPMG o Ernst & Young, esta actualización y modificación es muy complicada. A pesar de esta complejidad, el cumplimiento del contenido del nuevo Reglamento es obligatorio y por lo tanto la modificación de contratos para adaptarse a este. Para facilitar y ayudar a las organizaciones a realizar una valoración del cumplimiento de las obligaciones, la AEPD con la colaboración de la Autoritat Catalana de Protecció de Dades (en adelante apdcat) y de la Agencia Vasca de Protección de Datos ha emitido una guía dirigida a los responsables del tratamiento en la cual se incluye una lista de verificación del cumplimiento de las obligaciones de estos ante el RGPD[37]. En este caso estas firmas de auditoría podrían dirigirse a esta lista para corroborar si están cumpliendo con las obligaciones del RGPD o no y por lo tanto, adaptar y modificar los contratos de servicios de auditoría ya formalizados anteriormente con los clientes. De igual modo, en esta guía también se ha incluido una lista de verificación simplificada para aquellas empresas que realicen tratamientos básicos sobre datos ya que como vimos anteriormente, el tipo de tratamiento es el elemento decisivo para el RGPD y no el tamaño de las organizaciones que realicen el tratamiento.

Aun así, la obligación de cumplir con la normativa de protección de datos es anterior a la entrada en vigor del RGPD en mayo de 2018, concretamente, desde el año 1992 cuando se aprobó la primera norma relativa a la protección de datos en España, la Ley Orgánica de regulación del tratamiento automatizado de los datos de carácter personal, conocida como LORTAD[38]. El RGPD ha introducido novedades, como he indicado anteriormente, pero las obligaciones principales siguen estando vigentes y la existencia de las figuras principales como responsable y encargado del tratamiento también existían con anterioridad, así como el contrato entre ambos.

Como hemos visto en el apartado 2.2.4. *Infracciones y sanciones* uno de los principales motivos por los cuales las autoridades están interponiendo sanciones es la falta de contrato entre el responsable y el encargado del tratamiento. Es decir, en caso de que una empresa auditora responsable del tratamiento de los datos de carácter personal del cliente auditado y con el cual tiene establecido un contrato de servicios de auditoría, esté derivando los

[37] Agencia Española de Protección de Datos. "9 Lista de Verificación", en *Guía del Reglamento General de Protección de Datos para Responsables de Tratamiento*, España, 2018, p. 31.
[38] Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de los datos de carácter personal (BOE núm. 262, de 31 de octubre de 1992).

datos e información recabada del cliente auditado, a una empresa externa para el tratamiento o almacenamiento de estos datos sin contrato entre las partes en el cual se establezcan las condiciones, cláusulas, fines del tratamiento y/o salvaguardas sobre la protección de datos de carácter personal, estaría incurriendo la empresa auditora en una infracción que podría acarrear una sanción.

En este caso, tanto la empresa auditora como la empresa externa informática encargada del tratamiento deben cumplir con los principios relativos al tratamiento y la licitud del tratamiento definidos en el artículo 5 y 6 del RGPD, respectivamente.

En línea con lo anterior, la empresa auditora y la empresa externa informática tendrán que garantizar un adecuado nivel de seguridad de los datos expuestos a los diferentes riesgos. Por ejemplo, la empresa PwC utiliza una plataforma para el traspaso de información con la entidad auditada, con acceso únicamente por parte de PwC y su cliente, la entidad auditada. Las personas encargadas de estos accesos tienen sus propios usuarios y contraseñas.

En conclusión y tomando la respuesta a la consulta planteada anteriormente, la AEPD señala que "*no procede considerar un cambio de criterio en aplicación del RGPD, entendiendo que la actividad de los auditores de cuentas o sociedades de auditoría en el ejercicio de sus funciones, lo harán en calidad de responsables del tratamiento*"[39]. Por lo tanto, y en línea con todo lo comentado en este apartado, la cláusula contractual sobre protección de datos de los contratos o cartas de encargo que se formalicen a partir de ahora deberá ajustarse a esa condición de responsable del tratamiento que corresponde al auditor de cuentas.

3.2. Cumplimiento de derechos y obligaciones del Reglamento General de Protección de Datos en el ámbito de la auditoría

En relación con los nuevos derechos y obligaciones derivados del RGPD expuestos anteriormente en el apartado 2.2.3., a continuación, procedemos a relacionar dichos derechos y obligaciones en el ámbito de la auditoría. Comenzando por los nuevos derechos incluidos en el Reglamento y que más trascendencia tienen en el ámbito de la auditoría.

En cumplimiento, por parte de una sociedad de auditoría, del derecho a la transparencia en los servicios de una auditoría de cuentas, esta sociedad deberá indicar cualquier información al cliente en relación con los datos facilitados por este último al auditor. El cliente podrá solicitar y el auditor deberá, por lo tanto, informar de los datos de contacto del DPO nombrado en la empresa de auditoría. Por ejemplo, en la propuesta de servicios de auditoría de PwC se incluye párrafos similares al indicado en su página web: "*le comunicamos que puede ejercitar los derecho de acceso, rectificación, supresión, limitación al tratamiento, oposición y portabilidad de tus datos personales, que podrás ejercitar mediante petición escrita dirigida a la Oficina de Protección de Datos de PwC (Paseo de la Castellana nº 259-B, 28046 Madrid) o a través de la siguiente dirección de*

[39] *Contestación de la AEPD a la consulta presentada por el ICJCE sobre el papel del auditor en materia de protección de datos: responsable o encargado* – ICJCE. España, 2018.

correo electrónico data.protection.office@es.pwc.com acompañando copia de su D.N.I. o documento que le identifique"[40]. Dirigiéndose a dicho correo electrónico el cliente tiene el derecho de obtener de dicha firma de auditoría los datos de contacto del DPO, y así poder ejercer sus derechos, a los que la sociedad de auditoría debe darle respuesta.

Relativo a este derecho, que así se recoge en nuestra LOPDGDD[41] y que también es una obligación o principio, se hace mención en la definición del derecho a la transparencia y comunicación en el RPGD[42] al artículo 13. Dicho artículo indica que el responsable del tratamiento en el momento que reciba datos personales del interesado deberá facilitarle si este lo solicita, "*la intención del responsable de transferir datos personales a un tercer país u organización internacional*".

Volviendo al ejemplo de PwC, en su página web también expone que "*Únicamente transferiremos los datos de carácter personal a los que tengamos acceso, a otras firmas PwC, o proveedores de servicios de IT en relación con cualquiera de los fines establecidos en la presente cláusula. Algunos de estos destinatarios pueden estar ubicados fuera del Espacio Económico Europeo. Llevaremos a cabo dichas transferencias solo cuando tengamos una base legal para hacerlo, o cuando el destinatario: (i) esté en un país u organización que brinde un nivel adecuado de protección; o (ii) haya firmado un acuerdo que garantice que cumplirá con los requerimientos establecidos en la UE para la transferencia de datos personales a procesadores fuera de la UE*". De este modo, se cumple con la prohibición del RGPD de compartir datos de carácter personal con cualquier país que tenga un nivel de protección de datos inferior al establecido por la Unión Europea.

Respecto al derecho al olvido o supresión[43] que podrían ejercer las personas físicas pertenecientes a la empresa auditada por un auditor de cuentas y por el cual podrían exigir, como su propio nombre indica, la supresión de los datos personales que hayan sido facilitados, el auditor de cuentas podrá suprimir aquellos datos que no deba conservar estrictamente de conformidad con lo establecido en la Ley de Auditoría de Cuentas 22/2015 de 20 de julio, para poder justificar la prestación de los servicios profesiones de este, para el caso de que la misma fuera cuestionada y el tiempo de prescripción legalmente establecido, es decir, 5 años, tal y como establece el artículo 30 de la citada ley, "*Los auditores de cuentas y las sociedades de auditoría de cuentas conservarán y custodiarán durante el plazo de cinco años, a contar desde la fecha del informe de auditoría, la documentación referente a cada auditoría de cuentas por ellos realizada, incluidos los papeles de trabajo del auditor que constituyan las pruebas y el soporte de las conclusiones que consten en el informe*".
Como nuevo tercer derecho mencionábamos el derecho de limitación del tratamiento[44], el cual en uno de los apartados del artículo 18 del RGPD se mencionaba la posibilidad de

[40] PwC. Política de protección de datos de PwC. Disponible en www.pwc.es, España, 2019.
[41] *1. Cuando los datos personales sean obtenidos del afectado el responsable del tratamiento podrá dar cumplimiento al deber de información establecido en el artículo 13 del Reglamento (UE) 2016/679 facilitando al afectado la información básica a la que se refiere el apartado siguiente e indicándole una dirección electrónica u otro medio que permita acceder de forma sencilla e inmediata a la restante información.* […]. Art. 11 LOPDGDD.
[42] Art. 12 RGPD.
[43] Art. 17 RGPD y art. 15 LOPDGDD.
[44] Art. 16 LOPDGDD.

limitar el tratamiento de datos personales por parte del responsable si dicho tratamiento es ilícito, es decir, por ejemplo, si el auditor de cuentas está tratando los datos personales cedidos por la empresa auditada para cualquier otro fin no detallado en el contrato entre ambas partes, los titulares de los datos de la empresa auditada tienen el derecho de limitar el tratamiento de los datos facilitados.

Y, por último, respecto al derecho de portabilidad recogido en el artículo 20 del RGPD (y en el artículo 17 de la LOPDGDD), por ejemplo, como hemos mencionado anteriormente, PwC detalla en su página web que sus clientes pueden ejercer el derecho de portabilidad mediante petición escrita. Esto significa que las personas físicas pueden solicitar sus datos personales facilitados a un responsable del tratamiento para transmitirlos a otro responsable del tratamiento sin oposición del primero.

Por otro lado, anteriormente hemos destacado cuatro obligaciones expuestas en el RGPD. La seguridad del tratamiento de los datos de carácter personal nos lleva principalmente al cumplimiento de los principios relativos al tratamiento y a los referidos anteriormente, artículo 5 y 6 del RGPD. Es por ello que el auditor de cuentas debe garantizar con las medidas de seguridad oportunas que no se realiza un tratamiento de los datos de carácter personal cedidos por el cliente de manera ilícita o no autorizada.

En relación con la licitud del tratamiento y lealtad a los datos personales facilitados por el titular al responsable del tratamiento, en este caso, el auditor de cuentas, también se compromete a la confidencialidad de dichos datos sobre la base de la obligación de secreto profesional regulada, entre otra, en la Ley de Auditoría de Cuentas[45].

Las obligaciones de designación de un DPO y de la evaluación del impacto relativo a la protección de datos van de la mano como hemos mencionado en el apartado 2.2.3. ya que esta evaluación después de realizar el análisis de riesgos del tratamiento de los datos es una de las funciones genéricas del DPO. Una sociedad de auditoría que tenga la obligación de designar un DPO deberá realizar un análisis de los riesgos. Tendrá que realizar un análisis objetivo de los riesgos para la privacidad y derechos de los interesados, los de los sujetos que trabajen para la empresa auditada o que hayan sido sus clientes, derivados de las actividades de tratamiento que realice. Este análisis de riesgos se podría estructurar en tres apartados:

1) Criterios para la evaluación inicial objetiva: descripción de los criterios generales para la evaluación objetiva inicial de la actividad de tratamiento.
2) Criterios de interpretación: descripción de los criterios para la interpretación de la evaluación de la actividad de tratamiento.
3) Descripción sistemática de las operaciones de tratamiento: detalle de forma resumida de todas las actividades incluidas en dicho análisis.

Posteriormente, en relación con cada actividad detallada en la descripción sistemática de las operaciones de tratamiento se debería introducir información general descriptiva de la actividad de tratamiento (responsable del tratamiento, nombre de la actividad del tratamiento, breve descripción de la actividad…); información sobre los datos utilizados

[45] Art. 31 LAC.

para el tratamiento en cuestión (datos de carácter identificativo, datos especialmente protegidos, características personales…); se deberá hacer referencia a los supuestos tasados en el RGPD para tener que realizar una evaluación de impacto objetiva (si se realiza el tratamiento a gran escala, si se produce una observación sistemática de una zona de acceso público para el tratamiento…)[46]; y por último, se podría introducir información sobre las situaciones potenciales de riesgo para los interesados recogida tanto en el RGPD como en la LOPDGDD (si se realizan operaciones de tratamiento de datos personales de colectivos vulnerables como menores, ancianos, si se realizan operaciones que impliquen transferencias fuera del Espacio Económico Europeo)[47]. De este análisis podemos obtener el riesgo inherente de cada actividad. La AEPD define el riesgo inherente como "*el riesgo intrínseco de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El cálculo del riesgo inherente se realiza mediante la siguiente fórmula: Riesgo = Probabilidad x Impacto*"[48].

De este modo, podríamos determinar el riesgo que tiene cada actividad realizada por el responsable del tratamiento de cara al interesado, debido a la probabilidad, es decir la posibilidad que existe de que la amenaza se materialice y el impacto, el cual es determinado según los posibles daños que se pueden causar si es materializada la amenaza.

3.3. Ejemplos de auditoría con incidencias sobre el Reglamento General de Protección de Datos

Teniendo en cuenta todo lo tratado en los apartados anteriores y respecto a la modificación planteada de la cláusula contractual sobre protección de datos en referencia a los responsables del tratamiento, exponemos la siguiente cláusula que hemos identificado en una propuesta de servicios de auditoría de la firma PwC[49]:

"*Responsables del Tratamiento:* (la firma de auditoría) *actúa como Responsable del tratamiento respecto de los datos cedidos y se compromete, en relación a dichos datos, a tratarlos exclusivamente para llevar a cabo la prestación de los servicios y los fines especificados en la presente Cláusula.*

Trataremos los datos para los siguientes fines: (i) proporcionar los servicios; (ii) llevar a cabo auditorías de calidad, riesgo y gestión del cliente, revisión y cumplimiento de los procedimientos internos de la firma.

(La firma de auditoría) *dará cumplimiento a las obligaciones que le son impuestas por la normativa de protección de datos vigente, y adoptará las medidas de seguridad oportunas habida cuenta del estado de la tecnología, los datos cedidos y los riesgos a que dichos datos pudieran estar expuestos y llevará a cabo las evaluaciones de impacto de protección de datos requeridas legalmente*".

[46] Art. 35 RGPD.
[47] Considerados 75 a 77 RGPD.
[48] Agencia Española de Protección de Datos. "3.3 Gestión de riesgos: Identificar, evaluar y tratar", en *Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD*, España, 2018, p. 26.
[49] PricewaterhouseCoopers Auditores, S.L. Propuesta de servicios profesionales de auditoría, España, 2019.

Esta cláusula incluida en las nuevas cartas de contratación es un claro ejemplo que los auditores de cuentas y sociedades de auditoría están adoptando las medidas de organización interna necesarias, y sin que lo dispuesto en la normativa de protección de datos, o en la de confidencialidad y secreto profesional, pueda aducirse como impedimento a la aplicación de lo exigido por la normativa reguladora de la actividad de auditoría de cuentas. Respecto a esto, volvemos al apartado anterior donde hemos detallado como PwC en su página web hace mención a cómo sus clientes pueden ejercer sus derechos en relación a los datos personales facilitados a esta y como se aprecia la involucración en materia de cumplimiento de protección de datos teniendo una oficina exclusiva para este ámbito.

Con la firma de las diferentes cláusulas relativas al RGPD incluidas en las cartas de contratación, la entidad auditada presta su consentimiento expreso para que los datos de carácter personal de los cuales es responsable, incluidos datos especialmente sensibles, sean tratados por el auditor durante la relación laboral de la forma y para los fines que se expresan. De igual modo y con la firma de esta cláusula, se cumple con el nuevo Reglamento el cual se establece que para considerar que el consentimiento del tratamiento es inequívoco deberá existir un consentimiento expreso y en concreto, ante un contrato que requiera de los datos para llevarse a cabo.

Como se puede apreciar, de este modo, los auditores de cuentas cumplen con los principios relativos al tratamiento establecidos en el artículo 5 del RGPD por el cual se debe establecer en contrato los fines del tratamiento de los datos de carácter personal que serán solicitados a la empresa auditada siendo estos limitados en relación a los estrictamente necesarios para cumplir con los procedimientos y normativa de auditoría.

Adicionalmente he comprobado como profesional durante los últimos cuatro años en la firma de auditoría de PwC, que esta utiliza los datos y los trata únicamente para realizar los servicios de auditoría cumpliendo con la normativa vigente y por supuesto, además, con las cláusulas adicionales que se especifiquen en el contrato con el cliente.

Por ejemplo, he formado parte de equipos que han realizado la auditoría a empresas de diferentes sectores, en las cuales, siempre y como hemos mencionado en los apartados anteriores y en la cláusula definida en el contrato, PwC desempeña la función de responsable del tratamiento y tanto yo como mis compañeros, la función de usuarios de los datos. Y siempre me he hecho la misma pregunta, ¿todas las empresas respetan la protección de datos personales? Desde mi experiencia puedo decir que en la mayoría sí, pero que hay excepciones. De hecho, según se recoge en la Memoria AEPD 2019, la Subdirección General de Inspección de Datos (en adelante SGID), la cual se centra en verificar el cumplimiento de la normativa en materia de protección de datos, ha realizado un 9% menos de investigaciones respecto al ejercicio 2018[50]. Aunque hay que destacar que en 2018 se produjo un incremento significativo de las investigaciones debido a la difusión del RGPD.

En algunos casos, existen empresas que aún sin tu pedirlos, te facilitan datos personales de sus propios clientes. En estos casos, aún sin estar dentro de nuestras obligaciones,

[50] Agencia Española de Protección de Datos. "2. Inspección de datos", en *Memoria AEPD 2019*, España, 2019, p. 107.

hemos recomendado que salvo que sea necesario, no faciliten datos personales. Pero, por otro lado, y en la mayoría de las empresas que he auditado, te facilitan los datos personales única y exclusivamente que solicitas porque sean necesarios para llevar a cabo procedimientos y comprobaciones en la realización de las pruebas de auditoría, debido a que están obligados por el contrato a facilitarnos la información solicitada, pero conforme a la normativa de protección de datos, los datos deben ser los mínimos necesarios para la finalidad establecida. Así, en una auditoría, habrá casos en que los datos personales de clientes no sean necesarios.

Como verás, aquí se cumple con lo que el RGPD denomina como "minimización de datos", es decir, limitar a lo necesario el tratamiento de datos personales, establecido también en el artículo 5 del RGPD.

En la auditoría de una clínica sanitaria en la cual se poseen multitud de datos personales de los pacientes, desde nombre y apellidos hasta la enfermedad o el número de identidad de dicha persona, necesitamos una serie de datos personales de diferentes pacientes para comprobar los ingresos registrados en el ejercicio auditado, mediante confirmaciones de estos. En el primer instante de solicitud de dichos datos, la Dirección de dicha compañía, nos negó la entrega de dicha información y nos solicitó que enfocáramos la prueba de otra forma en la cual no fueran necesario dichos datos personales, tras transmitirles la necesidad de estos para enviar cartas a dichos clientes, debido a que la NIA-ES 500 indica que "*la fiabilidad de la evidencia de auditoría se ve afectada por su origen y naturaleza, y depende de las circunstancias concretas en las que se obtiene*" y que la NIA-ES 505 establece que "*El objetivo del auditor cuando utiliza procedimientos de confirmación externa es diseñar y aplicar dichos procedimientos con el fin de obtener evidencia de auditoría relevante y fiable*", consultaron con el DPO asignado en dicha compañía si podían facilitarnos los datos. Tras las comprobaciones y consultas oportunas, accedieron a pasarnos dicha información, pero con la condición de que se pasaran en un disco duro externo encriptado con contraseña. En ese caso y dado que tenemos dispositivos ya encriptados para estos casos, nos facilitaron la información de este modo.

En otros casos, por ejemplo, a la hora de verificar la retribución percibida por la alta dirección de la Sociedad auditada, esta nos ha indicado que únicamente podía facilitar estos datos mediante la visualización de los documentos en los sistemas informáticos propios de la compañía y siempre visualizados por el gerente del proyecto al cual en algunos casos le han solicitado la firma de un documento de confidencialidad y protección de datos.

Dicho esto, puedo decir, con mi experiencia en el mundo profesional de la auditoría, que la gran mayoría de las empresas que he auditado, llevan un buen control y protección de los datos de carácter personal que poseen, ya sean de sus empleados, de sus clientes o incluso de los propietarios de la compañía.

Existen empresas con protocolos de actuación de protección de datos y por supuesto, empresas con su correspondiente DPO, el cual ha realizado la evaluación de riesgos e impactos sobre la protección de datos personales.

Pero como hemos comentado antes en el apartado 3.1. *Cumplimiento por parte de los auditores del Reglamento General de Protección de Datos* para intentar garantizar al máximo por parte de PwC la protección de los datos de aquellos datos que esta firma de auditoría es responsable del tratamiento, utiliza con sus clientes, entidades auditadas, una plataforma online en la cual únicamente tiene acceso el personal interno de PwC que pertenezca al equipo de dicha auditoría y el personal de la entidad auditada autorizado por esta para el intercambio de información la cual puede contener datos personales. El acceso a esta plataforma está restringido con un usuario y contraseña personal y la información subida a la misma puede ser eliminada en cualquier momento por el personal de PwC, eliminando así todos aquellos datos almacenados en dicha plataforma que tras la emisión del informe de auditoría, no sean necesarios conservar.

Puedo concluir en este apartado, teniendo en cuenta que no en todas las auditorías realizadas, existe incidencia del Reglamento, porque quizás no sea necesario el almacenamiento de datos personales de la entidad auditada por parte del auditor o de la sociedad de auditoría. Pero si existen casos, en los cuales hay una incidencia directa del RGPD debido al tratamiento de datos personales por parte de la sociedad de auditoría y, por lo tanto, ser ésta responsable del tratamiento de estos datos, ya que, por ejemplo, el simple hecho de visualización de datos de carácter personal, es considerado tratamiento de datos. Principalmente podemos destacar los casos de empresas relacionadas con el sector sanitario dado que la mayor parte de los clientes son personas físicas las cuales facilitan una gran cantidad de datos personales.

4. CONCLUSIONES

La manera de tratar los datos de cualquier tipo ha sido facilitada en gran medida por la evolución durante la historia reciente de la tecnología y la informática lo que ha puesto en peligro la protección de datos de carácter personal.

Las compañías y empresas cada vez almacenan más datos y en concreto, más datos de carácter personal: datos de empleados, de clientes hasta de proveedores y propietarios de la compañía. Y el auditor de cuentas necesita tener una base legítima por parte de las entidades auditadas para el uso de los datos personales necesarios para realizar los diferentes procedimientos de la auditoría.

En primer lugar, hemos analizado la protección de datos, y en el preámbulo de la LOPDGDD se define la protección de datos como "*el derecho que se configura como una facultad del ciudadano para oponerse a que determinados datos personales sean usados para fines distintos a aquel que justificó su obtención*". Es decir, el fin de esta ley pretende salvaguardar datos de carácter personal y entendiendo como dato personal, según la definición establecida en el RGPD, como cualquier dato que hace posible la identificación de cualquier persona física. De este modo, también se consideran datos personales aquellos que sean anonimizados siempre que estos sean utilizables para identificar a una persona física y dejen de ser anónimos.

Este Reglamento tiene como objeto principal la regulación de la protección de estos datos, datos de carácter personal, para garantizar y proteger los derechos de las personas físicas.

Además, como se recoge en la Constitución española, el derecho a la protección de datos de carácter personal es un derecho fundamental de las personas físicas.

En segundo lugar, hemos explicado que el Reglamento, entra en vigor el 25 de mayo de 2018 y que anteriormente, la norma reguladora de la protección de datos era la Directiva 95/46/CE, del Parlamento Europeo y del Consejo. Junto con esta, a nivel nacional convivía la LOPD, la cual fue derogada por la entrada en vigor de la actual LOPDGDD desde el 7 de diciembre de 2018.

Con este RGPD se han destacado cinco novedades: la figura del Delegado de Protección de Datos obligatoria en las entidades públicas y recomendable (o incluso obligatoria, según el caso) en todas las sociedades, y que pretende garantizar el cumplimiento normativo de protección de datos en organizaciones; nuevos derechos como el de supresión, transparencia y comunicación, limitación del tratamiento y portabilidad de los datos; obtención del consentimiento expresamente; análisis de riesgos y evaluación de impactos, siendo obligatorio para aquellas entidades que realicen tratamiento de datos; y por último, un incremento de las sanciones, pudiendo llegar a 20 millones de euros o incluso a un 4% de la cifra de negocio de la entidad sancionada.

Posteriormente y, en tercer lugar, se ha definido y expuesto las diferentes figuras intervinientes en el tratamiento de datos y por consiguiente en la protección de datos. Por un lado, los titulares por el RGPD, que son aquellas personas físicas cuyos datos personales hayan sido proporcionados o recogidos para su tratamiento, y por otro, los obligados, que son aquellas personas físicas y también jurídicas, que realicen tratamiento o almacenen datos personales.

En relación con este trabajo, es decir el RGPD y la auditoría de cuentas, hemos diferenciados a qué figura corresponde cada uno de los implicados en una auditoría de cuentas. La empresa auditora es considerada como el responsable del tratamiento y los trabajadores de ésta como usuarios de los datos. En caso de existir una empresa externa de informática que se encargara del tratamiento o almacenamiento de los datos recabados por el auditor, ocuparía la figura de encargado del tratamiento.

Del RGPD se derivan derechos y obligaciones, los cuales hemos analizado en cuarto lugar. Como he mencionado anteriormente, el Reglamento incorpora nuevos derechos, completando a los derechos ARCO. Y, además, una serie de obligaciones de las cuales destacamos la seguridad del tratamiento de los datos de carácter personal, evaluación del impacto relativo a la protección de datos, designación de un DPO y la formalización de códigos de conducta. Esto en el terreno de la auditoría implica que las sociedades de auditoría y auditores de cuentas tendrán que realizar un análisis de los riesgos a los cuales están expuestos los datos personales en las diferentes operaciones de tratamiento y concluir con una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, para tomar las medidas oportunas para garantizar un adecuado nivel de seguridad de los datos.

En quinto lugar y una vez analizadas las infracciones y sanciones podemos concluir que el RGPD prevé sanciones administrativas y la posibilidad de que cada Estado regule el tipo de sanción. En España, la LOPDGDD divide en tres las infracciones: muy graves

que prescriben a los tres años, graves que prescriben a los dos y leves que prescriben al año. En el ámbito de la auditoría, esto implica que las sociedades de auditoría como responsables del tratamiento de datos personales podrían ser sancionados por ejemplo por realizar tratamiento de datos con fines distintos a los establecidos en el contrato firmado con la entidad auditada, considerándose en este caso una infracción muy grave y pudiendo alcanzar la sanción la cuantía de hasta el 4% de la cifra de negocios de la sociedad de auditoría.

Por último, y en relación con la implicación del RGPD en la auditoría, hemos comprobado que afecta tanto a las firmas de auditoría en referencia a los datos internos de estas, como a la prestación de los servicios profesionales a clientes en tanto que sean responsables de los datos que tratan o manejan.

Internamente, las firmas de auditoría han prestado especial atención en la limitación de los datos recopilados, en la protección y el respeto de estos ya que pertenecen a un tercero y así, hemos visto cómo hacen para cumplir con todos los requerimientos y principios del RGPD. Esto debe ser comunicado a los trabajadores de la firma de auditoría, de igual modo que el RGPD, así como la LOPDGDD, expresan que el acceso a los datos personales debe estar recogido en un contrato. En este contrato se recoge que la empresa auditora es el responsable del tratamiento y no la encargada del tratamiento como se planteó a la AEPD, la cual corroboró que efectivamente la empresa auditora ocupa la figura de responsable del tratamiento en la actividad de auditoría de cuentas porque es quién decide los fines y los medios para llevar a cabo la actividad de auditoría.

La figura de encargado del tratamiento la ocuparía una empresa externa a la empresa de auditoría que fuera contratada para el tratamiento y/o almacenamiento de datos. En este caso al igual que con la entidad auditada, debe existir un contrato entre las partes. Esta falta de contrato es uno de los motivos principales de sanciones.

En relación con el ejercicio de los derechos, una entidad auditada tiene el derecho de poder solicitar los datos de contacto del DPO, en el caso de que estuviera designado en la sociedad de auditoría. Además, los sujetos titulares de los datos, de los que es responsable la entidad auditada, podrán exigir la supresión de los datos personales facilitados al auditor de cuentas, pero éste, únicamente podrá eliminar aquellos datos que no deba conservar durante cinco años tal y como se establece en la LAC. Y de poder limitar el tratamiento de datos del responsable si éste estuviese realizando un tratamiento distinto al establecido en el contrato entre las partes.

Y en relación con las obligaciones del auditor de cuentas o sociedad de auditoría, como responsable del tratamiento de datos, la obligación de realizar un análisis de riesgos de las actividades que realiza, pudiendo obtener así el riesgo de cada una en base a la probabilidad y el impacto, pudiendo así adoptar las medidas de seguridad necesarias al fin perseguido.

Desde mi experiencia laboral he podido apreciar la gran cantidad de datos personales que se utilizan en la auditoría de cuentas, a pesar que no en todas es necesario, ya sean solicitados o no. Por eso, es necesario el cumplimiento de la normativa tanto a nivel europeo como nacional, y es necesario, que en todo momento se mantenga la protección

de aquellos datos personales recabados y utilizados para los diferentes procedimientos de auditoría.

Por todo ello, podemos concluir que la aplicación del RGPD en una empresa de auditoría implica desde la formalización en un contrato de los fines del tratamiento de los datos de carácter personal de la entidad auditada, los cuales deben ser los necesarios, hasta el análisis de riesgos de las actividades realizadas por ésta y la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales, provocando que la empresa de auditoría adopte las medidas de seguridad necesarias para que los datos que maneja no se pierdan o alteren. De esta forma la empresa de auditoría cumplirá con la normativa.

5. BIBLIOGRAFÍA

Accountancy Europe. (2018). *¿Qué implicaciones tiene la nueva normativa de Protección de Datos sobre expertos contables y auditores?* Bruselas.

Agencia Española de Protección de Datos. (2018). Esquema de certificación de delegados de protección de datos de la Agencia Española de Protección de Datos (Esquema AEPD-DPD). España.

Agencia Española de Protección de Datos. (2018). Guía práctica para las evaluaciones de impacto en la protección de los datos sujetas al RGPD. España.

Agencia Española de Protección de Datos. (2018). Guía del Reglamento General de Protección de Datos para responsables de tratamiento. España.

Agencia Española de Protección de Datos. (2016). Orientaciones y garantías en los procedimientos de anonimización de datos personales. España.

Bacaria Martrus, J., & Simón Castellano, P. (2020). *Funciones del delegado de protección de datos en los distintos sectores de actividad.* Wolters Kluwer.

Benedito, I. (7 de Junio de 2018). *Expansión*. Obtenido de https://www.expansion.com/juridico/actualidad-tendencias/2018/06/06/5b18187522601dea078b4574.html Consultado el 29 de diciembre de 2019.

Del Peso Navarro, E. (2003). *Servicios de la sociedad de la información.* Madrid: Diaz de Santos.

Del Peso Navarro, E., & Miguel, R. G. (2002). *La Seguridad de los Datos de Carácter Personal.* Diaz de Santos.

Gonzalvo, I. (28 de Mayo de 2018). *DIARIOJURÍDICO.COM*. Obtenido de https://www.diariojuridico.com/principales-novedades-del-nuevo-reglamento-general-de-proteccion-de-datos/ Consultado el 12 de enero de 2020.

ICJCE. (22 de Noviembre de 2018). Contestación de la AEPD a la consulta presentada por el ICJCE sobre el papel del auditor en materia de protección de datos: responsable o encargado. España. Obtenido de https://www.icjce.es Consultado el 4 de agosto de 2020.

Iuristec. (s.f.). *Iuristec*. Obtenido de http://www.iuristec.es/?p=6727 Consultado el 23 de marzo de 2020.

Merino, C. R. (12 de Agosto de 2015). *Blog del Máster en Marketing Directo y Digital de la UPF Barcelona School of Management*. Obtenido de https://marketingdigital.bsm.upf.edu/e-commerce-comercio-electronico/ Consultado el 30 de mayo de 2020.

Pérez Luño, A.E. (2006). *La tercera generación de derechos humanos.* Thomson - Aranzadi.

Pérez Porto, J., & Merino, M. (2012). Definición.DE Obtenido de https://www.definicion.de Consultado el 13 de enero de 2020.

Pérez Royo, J. (2018). *Curso de derecho constitucional.* Marcial Pons.

PricewaterhouseCoopers Auditores, S.L. (2019). Propuesta de servicios de auditoría. Sevilla.

Signaturit. (9 de Enero de 2018). *Signaturit.* Obtenido de https://blog.signaturit.com/es/top-10-novedades-del-nuevo-reglamento-europeo-de-proteccion-de-datos Consultado el 29 de marzo de 2020.