N/REF: 0005/2021

Antes de entrar a analizar el texto sometido a informe, es preciso señalar que el mismo se emite sin que se haya aprobado el Real Decreto por el que se desarrollan la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las Administraciones Públicas y la Ley 40/2015, de 1 de octubre, de régimen jurídico del sector público, en materia de actuación y funcionamiento del sector público por medios electrónicos, encontrándose el correspondiente proyecto, tal y como se indica en la consulta, pendiente del preceptivo dictamen del Consejo de Estado. No obstante, teniendo en cuenta lo manifestado en la consulta y que, de acuerdo con la disposición final séptima de la Ley 39/2015, "las previsiones relativas al registro electrónico de apoderamientos, registro electrónico, registro de empleados públicos habilitados, punto de acceso general electrónico de la Administración y archivo único electrónico producirán efectos a partir del día 2 de abril de 2021", se procede a la emisión del mismo, sin perjuicio de que, si como consecuencia de las observaciones del alto órgano consultivo se introdujeran modificaciones en el proyecto que afecten sustancialmente al contenido de la presente Orden, debería solicitarse nuevo informe de esta Agencia.

El proyecto de orden objeto de informe tiene por objeto regular los requisitos y condiciones de funcionamiento del Registro Electrónico General de la Administración General del Estado, previsto en el artículo 16 de la Ley 39/2015 estableciéndose en el artículo 34 del proyecto de real decreto de desarrollo su creación, naturaleza y funcionamiento.

I

Esta Agencia ha tenido oportunidad de pronunciarse, en relación con la necesaria salvaguardia del derecho fundamental a la protección de datos personales en la Administración electrónica, en sus informes 26/2015 y 91/2018.

En el informe 26/2015, referente al Anteproyecto de Ley del Procedimiento Administrativo Común de las Administraciones Públicas ya

destacó la necesidad de incluir expresamente, dentro de los derechos de las personas en sus relaciones con la Administración, el de protección de sus datos de carácter personal, y en particular, en relación con los registros electrónicos, a la necesidad de implantar en los mismos las medidas de seguridad previstas en la normativa de protección de datos, a fin de garantizar que no se produzca la pérdida, acceso accidental o destrucción de los documentos o solicitudes presentadas por los ciudadanos que pudieran contener datos de carácter personal, señalando que

> Particularmente relevante será la referencia a la necesaria adopción de las medidas de seguridad establecidas no sólo en el Esquema Nacional de Seguridad sino también la normativa de protección de datos de carácter personal dentro de la normativa reguladora de los registros a los que se refiere el Anteproyecto y, en particular, en el Registro de apoderamientos y en los regulados por el artículo 30.

Posteriormente, el informe 91/2018 referente al proyecto de Real Decreto por el que se desarrollan las leyes 39/2015 y 40/2015 ambas de 1 de octubre de 2015, en materia de actuación y funcionamiento del sector público por medios electrónicos, incidía en la necesidad de garantizar, en dichas normas de desarrollo, el derecho a la protección de datos de carácter personal, tal y como se había recogido en la Ley 39/2015 tras las anteriores observaciones:

> La norma presentada a informe es, tal y como proclama su título, desarrollo de las leyes 39/2015 y 40/2015, de 1 de octubre (en adelante leyes 39/2015 y/o 40/2015) en materia de actuación y funcionamiento del sector público por medios electrónicos. Pues bien, una primera conclusión que cabe extraer, y que desde el punto de vista del informe de esta Agencia podría ser suficiente, es que dichas leyes contienen ya una referencia explícita a que las relaciones entre las Administraciones Públicas, o en las relaciones de estas con los interesados, habrá de cumplirse en todo momento con la normativa de protección de datos, circunstancia ésta, como no puede ser de otro modo, que se extiende igualmente a sus normas de desarrollo. Así, cabe mencionar que dichas obligaciones se recogen en los artículos 13.h), 16.1 (3º) y 17 de la ley 39/2015, y en los artículos 3.2, 4.2 y 155 de la ley 40/2015.
>
> El art. 13 h) de la ley 39/2015 establece como un derecho de las personas en sus relaciones con las administraciones públicas el de la protección de datos de carácter personal, y en particular a la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.

Ello se extiende a los registros, en cuanto que cauce esencial de las solicitudes de los administrados a las Administraciones: Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal. (art. 16.1 de la ley 39/2015), y también se extiende a los archivos, como soporte electrónico de los documentos de procedimientos finalizados: Los medios o soportes en que se almacenen documentos, deberán contar con medidas de seguridad, de acuerdo con lo previsto en el Esquema Nacional de Seguridad, que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. En particular, asegurarán la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos. (art. 17.3º de la ley 39/2015).

Desde el punto de vista del régimen jurídico de las Administraciones Públicas, la ley 40/2015 establece como un principio general de su actuación y de las relaciones entre las mismas el de garantizar […] la protección de los datos de carácter personal, (de los ciudadanos que se relacionan con ella) –art. 3.2 ley 40/2015. Y el art. 4.2 de dicha norma reconoce el valor del derecho fundamental a la protección de datos personales como un límite a la actuación administrativa, lo que corrobora el art. 155, ya que las transmisiones de datos entre las Administraciones Públicas han de estar sujetas a lo permitido por la normativa de protección de datos personales.

En definitiva, la actuación y el funcionamiento del sector público por medios electrónicos conlleva una serie de ventajas en materia de eficacia, eficiencia, simplicidad, racionalización de costes etc. pero no podemos dejar de mencionar que también existen más riesgos para el derecho fundamental de los particulares a la protección de sus datos personales, por lo que las leyes 39/2015 y 40/2015 han hecho hincapié en que dichos medios electrónicos han de ser usados siempre de conformidad con la normativa de protección de datos. Y dicha normativa habrá de ser cumplida por lo tanto escrupulosamente cuando de las normas de desarrollo de dichas leyes se trata, o de las actuaciones específicas derivadas de las mismas, pues en caso contrario dichas normas de desarrollo o actuaciones que incumpliesen los mandatos de la ley estarían incursos en causas de invalidez (art. 47 y 48 ley 39/2015).

II

En lo que a la materia de protección de datos personales se refiere, la normativa a la que debe ajustarse la Orden proyectada está constituida por el

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (RGPD en lo sucesivo) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD en lo sucesivo), que tiene incidencia en diversos aspectos regulados en la norma, que se analizarán siguiendo el orden seguido por su articulado.

En primer lugar, el artículo 2 regula los órganos competentes, señalando lo siguiente:

> 1. La Dirección General de Gobernanza Pública del Ministerio de Política Territorial y Función Pública es competente para la gobernanza y gestión funcional del REG-AGE, correspondiendo a la Secretaría General de Administración Digital del Ministerio de Asuntos Económicos y Transformación Digital el diseño, implantación y gestión técnica de la plataforma tecnológica del REG-AGE y del servicio electrónico para la presentación de solicitudes, escritos y comunicaciones accesible desde la sede electrónica del Punto de Acceso General de la Administración del Estado.
> 2. En cada Ministerio se designará un Delegado del REG-AGE, con rango de Subdirector General o similar, dicha designación corresponderá al titular de la Subsecretaría, pudiéndose nombrar más de un delegado cuando el volumen de actividad o número de Oficinas de Asistencia en Materia de Registro (OAMR) así lo aconseje. Dicha designación corresponderá al titular de la Subsecretaría o en su caso por el titular del organismo público correspondiente.
> Será responsable del seguimiento del correcto funcionamiento del REG-AGE sobre los documentos que tengan como emisor o destinatario el Ministerio y los organismos públicos y entidades de derecho público vinculadas o dependientes y la coordinación de las Oficinas de Asistencia en Materia de Registro, en su caso, en materia del REG-AGE.

Desde la perspectiva de la normativa de protección de datos, es relevante identificar la posición jurídica que, en relación con los tratamientos de datos personales, corresponde a cada uno de dichos órganos, en función de su efectiva participación en la determinación de los fines y los medios el tratamiento. A este respecto, el RGPD considera en el artículo 4 como «responsable del tratamiento» o «responsable»: “la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembro;” y como «encargado del tratamiento» o «encargado»: “la persona física o jurídica,

autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".

En cuanto a la designación por el Derecho de los Estados miembros a que se refiere el artículo 4.7) del RGPD *in fine* ("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 miembro"), las Directrices 07/2020 del Comité Europeo de Protección de Datos sobre los conceptos de responsable del tratamiento y encargado en el RGPD diferencia dos supuestos. Por un lado, los supuestos en los que el poder de decisión puede inferirse de una competencia legal explícita, por ejemplo, cuando el responsable del tratamiento o los criterios específicos para su nominación son designados por la legislación nacional o de la Unión. Cuando el responsable del tratamiento haya sido identificado específicamente por ley, esto será determinante para establecer quién actúa como responsable. Esto presupone que el legislador ha designado como responsable a la entidad que tiene una capacidad genuina para ejercer el control. Y que en algunos países, legislación nacional establece que las autoridades públicas son responsables del tratamiento de datos personales dentro del contexto de sus funciones (apartado 21). Y por otro, el supuesto más común en que, en lugar de nombrar directamente al responsable del tratamiento o establecer los criterios para su designación, la ley establece una tarea o impone un deber a alguien para captar y tratar ciertos datos. En esos casos, el fin del tratamiento a menudo está determinado por la ley y el responsable del tratamiento será normalmente el designado por ley para la realización de esta finalidad, como sería el caso cuando una entidad a la que se le confían determinadas tareas públicas (por ejemplo, seguridad social) que no puede cumplirse sin recopilar al menos algunos datos personales, establece una base de datos o registro para cumplir con esas tareas públicas. En ese caso, la ley, aunque indirectamente, establece quién es el responsable. De manera más general, la ley también puede imponer una obligación tanto a entidades públicas como privadas para retener o proporcionar ciertos datos. Estas entidades entonces normalmente se considerarían como responsables con respecto al tratamiento que es necesario para ejecutar esta obligación (apartado 22).

Considerando que, en el presente caso, los fines y los medios del tratamiento han sido establecidos por la Ley 39/2015 y su reglamento de desarrollo, la concreción de dichas figuras vendrá determinada por las competencias que correspondan a cada uno de los órganos intervinientes y que se concretan en el precepto informado. **A este respecto, a la Dirección General de Gobernanza Pública le corresponde la "gobernanza y gestión funcional" del Registro, por lo que a la misma le correspondería la condición de responsable del tratamiento. Mientras que la Secretaría General de Administración Digital asume el "diseño, implantación y gestión técnica de la plataforma tecnológica del REG-AGE y del servicio**

electrónico para la presentación de solicitudes, escritos y comunicaciones accesible desde la sede electrónica del Punto de Acceso General de la Administración del Estado", por lo que estaría actuando como encargada del tratamiento.

En cuanto al Delegado (o Delegados) del Registro que debe designarse en cada Ministerio y organismo público, el mismo "será responsable del seguimiento del correcto funcionamiento del REG-AGE sobre los documentos que tengan como emisor o destinatario el Ministerio y los organismos públicos y entidades de derecho público vinculadas o dependientes y la coordinación de las Oficinas de Asistencia en Materia de Registro, en su caso, en materia del REG-AGE".

En estos casos, teniendo en cuenta que el ejercicio de dichas funciones no derivan de las competencias propias que los decretos de estructura departamental asignan a los Subdirectores Generales o asimilados, sino de actuar **como Delegados del Registro, en el supuesto de las mismas requieran el tratamiento de datos personales, estarán actuando por cuenta del responsable, como encargados del tratamiento.**

En relación con los encargados del tratamiento, deberá darse cumplimiento a lo dispuesto en el artículo 28 del RGPD, de modo que exista el acto o contrato que regule el citado encargo, en los términos señalados en el apartado 3 del citado precepto. A estos efectos, la propia Orden proyectada podrá ser dicho acto siempre que recoja los extremos que señala el citado artículo 28.3 del RGPD, lo que podría hacerse en un anexo de la misma.

III

El artículo 10 se refiere específicamente a la protección de datos de carácter personal, en el que se refiere exclusivamente a la base jurídica del tratamiento respecto de los datos personales del interesado o su representante cuando sean personas físicas:

> De conformidad con lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, General de Protección de Datos, y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales, cuando el poderdante o el apoderado fueran personas físicas, el tratamiento automatizado de sus datos que resulte necesario para el adecuado funcionamiento del REA-AGE se fundamenta en el cumplimiento de una obligación legal aplicable al responsable del tratamiento.

A este respecto, hay que señalar, en primer lugar, que quedan excluidas de la aplicación de la normativa sobre datos personales las personas jurídicas, pero su ámbito protector se extiende a las personas físicas que las representan, cuyos datos personales deben ser tratados con sujeción a lo previsto en el RGPD y la LOPDGDD, en el caso de que el interesado o su representante sea una persona jurídica.

En segundo lugar, la Orden considera como base jurídica del tratamiento la contemplada en la letra c) del artículo 6.1 del RGPD: "el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento".

En relación con el tratamiento de datos por parte de las Administraciones Públicas, es criterio reiterado de esta Agencia que el fundamento del mismo debe encontrarse en las letras c) y e) del artículo 6.1 del RGPD. En este sentido, en el informe 175/2018 ya se señalaba lo siguiente:

> Como CONCLUSIÓN en este punto, cabe decir que, con carácter general, la base jurídica del tratamiento en las relaciones con la Administración, en aquellos supuestos en que existe una relación en la que no puede razonablemente predicarse que exista una situación de equilibrio entre el responsable del tratamiento (la Administración), y el interesado (el administrado) no sería el consentimiento (art. 6.1.a) RGPD), sino, según los casos, el cumplimiento de una obligación legal (art. 6.1.c) RGPD) o el cumplimiento de una misión de interés público o en el ejercicio de poderes públicos (art. 6.1.e) RGPD).

No obstante, en el Informe 74/2019, se destacaba la necesidad de deslindar ambos conceptos, ya que no hacerlo así implicaría confundir, en la práctica totalidad de los casos de actuación de la Administración, ambas bases jurídicas, concluyendo que

> Por ello, la base jurídica prevista en la letra c) del artículo 6.1. del RGPD será de aplicación en aquellos casos en los que una norma con rango de ley imponga a la Administración una obligación específica de dar, hacer o no hacer, que implique el tratamiento de datos de carácter personal, y diferente del deber jurídico genérico de la Administración de ejercer las potestades que el ordenamiento jurídico le atribuye para servir con objetividad al interés público (artículo 103 de la Constitución).

Y el criterio que viene manteniendo reiteradamente esta Agencia, en relación con los registros administrativos, es que el tratamiento de los datos personales correspondientes se encontraría se encontraría amparado por lo

dispuesto en la letra e) del artículo 6.1.del RGPD: “el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento”, siempre que se haya establecido por una norma con rango de ley, conforme a lo señalado por el artículo 8.2 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales: “El tratamiento de datos personales solo podrá considerarse fundado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable, en los términos previstos en el artículo 6.1 e) del Reglamento (UE) 2016/679, cuando derive de una competencia atribuida por una norma con rango de ley” (Informe 92/2020, en relación con el Registro de Variedades Protegidas y el Registro de Variedades Comerciales, el Informe 128/2018 sobre el registro unificado sobre certificados y centros de formación de gases fluorados o el informe 4/2021 relativo al registro electrónico de apoderamientos en el ámbito de la Administración General del Estado).

En el presente caso, siendo el procedimiento administrativo el “conjunto ordenado de trámites y actuaciones formalmente realizadas, según el cauce legalmente previsto, para dictar un acto administrativo o expresar la voluntad de la Administración”, y siendo necesario dejar constancia de todo documento que sea presentado o que se reciba en cualquier órgano administrativo mediante el correspondiente asiento en el Registro electrónico General (artículo 16.1 de la Ley 39/2015) con el objeto de dejar reflejada, entre otras circunstancias, la fecha y hora de su presentación (artículo 16.3 de la Ley 39/2015), lo que tiene especial importancia, entre otros supuestos, a efectos del cumplimiento de los plazos notificar la resolución expresa en los procedimientos iniciados a instancia del interesado (artículo 21.3 de la Ley 39/2015) o para la suspensión de la ejecución de los actos administrativos recurridos (artículo 117.3 de la Ley 39/2015) y, en general, para dejar acreditada la recepción de cualquier documento que forma parte del procedimiento. Por consiguiente, el tratamiento de los datos personales de los interesados en el procedimiento y de sus representantes **es necesario para dar cumplimiento a la obligación contemplada en el artículo 16.1., que exige específicamente que los asientos se hagan en el Registro electrónico general, así como para el adecuado desarrollo del procedimiento administrativo para que las Administraciones públicas puedan ejercer las potestades que tienen atribuidas, singularmente en su vertiente de garantía para el particular (Sentencia del Tribunal Supremo de 20 de septiembre de 1983) encontrando su legitimación, de este modo, en el artículo 6.1 letras c) y e) del RGPD, sin perjuicio del deber de informar a los afectados en los términos previstos en el artículo 13 del RGPD, pudiendo realizarse dicha información “por capas”, conforme al artículo 11 de la LOPDGDD.**

Por otro lado, debe hacerse especial referencia a las medidas de seguridad que deben adoptarse para salvaguardar el derecho a la protección de datos y a las que se refiere específicamente el artículo 16.1 de la Ley 39/2015:

> El Registro Electrónico General de cada Administración funcionará como un portal que facilitará el acceso a los registros electrónicos de cada Organismo. Tanto el Registro Electrónico General de cada Administración como los registros electrónicos de cada Organismo cumplirán con las garantías y medidas de seguridad previstas en la legislación en materia de protección de datos de carácter personal.

En este punto, hay que tener en cuenta que el RGPD ha supuesto un cambio de paradigma al abordar la regulación del derecho a la protección de datos personales, que pasa a fundamentarse en el principio de «accountability» o «responsabilidad proactiva» tal y como ha señalado reiteradamente la AEPD (Informe 17/2019, entre otros muchos) y se recoge en la Exposición de motivos de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD): “la mayor novedad que presenta el Reglamento (UE) 2016/679 es la evolución de un modelo basado, fundamentalmente, en el control del cumplimiento a otro que descansa en el principio de responsabilidad activa, lo que exige una previa valoración por el responsable o por el encargado del tratamiento del riesgo que pudiera generar el tratamiento de los datos de carácter personal para, a partir de dicha valoración, adoptar las medidas que procedan”. Dentro de este nuevo sistema, es el responsable del tratamiento el que, a través de los instrumentos regulados en el propio RGPD como el registro de actividades del tratamiento, el análisis de riesgos o la evaluación de impacto en la protección de datos personales, debe garantizar la protección de dicho derecho mediante el cumplimiento de todos los principios recogidos en el artículo 5.1 del RGPD, documentando adecuadamente todas las decisiones que adopte al objeto de poder demostrarlo.

Así, el artículo 24.1 del Reglamento General de Protección de Datos dispone que “Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario”.

Esta previsión se completa con lo señalado en el considerando 75 del Reglamento, según el cual “Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos,

materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados".

A su vez, en relación con la seguridad de los datos personales, el artículo 32.1 establece que "Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".

Un papel fundamental, en fin, dentro de este nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeñará el Delegado de Protección de Datos, que el Reglamento General regula en sus artículos 37 a 39. En particular, el artículo 37.1 a) impone obligatoriamente la designación de un Delegado en los supuestos en que "el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial".

A su vez, el artículo 38.1 establece claramente que "El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales" y el artículo 39.2 dispone que "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".

Finalmente, el artículo 39.1 enumera las funciones del delegado de Protección de Datos, entre las que se encuentran “”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” (apartado a), “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” (apartado b) y “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 (apartado c).

De lo que acaba de indicarse se desprenden dos conclusiones: por una parte, la evolución del modelo desde la lista de cumplimiento a la responsabilidad activa impone la necesidad de realizar un análisis de riesgos en materia de protección de datos y, en su caso una evaluación de impacto en la misma, sin que sea suficiente una mera remisión a las normas de protección de datos, habida cuenta que éstas ya no establecen un modelo tasado de cumplimiento.

Por otra, el Delegado de Protección de Datos, obligatorio en el supuesto que ahora se está analizando, deberá asesorar en dicho análisis y en la adopción de las medidas necesarias, en virtud de las funciones que el Reglamento General de Protección de Datos le otorga expresamente.

Por ello debería hacerse constar expresamente en el precepto que, previo análisis de los riesgos para los derechos y libertades de las personas físicas, se adoptarán las medidas técnicas y organizativas destinadas a garantizar y poder demostrar que el tratamiento es conforme con la normativa de protección de datos personales que serán revisadas y actualizadas cuando sea necesario.

Además, debería clarificarse en dicho precepto que las medidas a implantar como consecuencia del citado análisis de riesgos, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberían prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.