N/REF: 0004/2021

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 de Apoderamientos de la Administración General del Estado, previsto en el artículo 6 de la Ley 39/2015 y regulado en el artículo 33 del proyecto de real decreto de desarrollo, determinando los órganos responsables del citado Registro y el sistema de funcionamiento del mismo, el procedimiento de incorporación de los apoderamientos en el Registro, así como la revocación y renuncia y vigencia de los poderes.

Por otra parte, se aprueban los modelos de poderes inscribibles en el registro en el ámbito de la Administración General del Estado y de sus organismos públicos y entidades de derecho público, adheridos al mismo.

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, asume la gobernanza y gestión funcional del Registro electrónico de apoderamientos, 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 que soporte el Registro.
>
> 2. En cada Ministerio y organismo público adherido al REA-AGE se designará un Delegado del REA-AGE con rango Subdirector General o similar. Dicha designación corresponderá al titular de la Subsecretaría o, en su caso, por el titular del organismo público correspondiente.

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", por lo que estaría actuando como encargada del tratamiento.**

En cuanto al Delegado del Registro que debe designarse en cada Ministerio y organismo público adherido, las únicas funciones que,

específicamente, le atribuye el proyecto de Orden son las recogidas en el artículo 6.c).2º, en relación con el bastante de poderes:

> En los apoderamientos otorgados mediante comparecencia personal y por internet, contemplados en el artículo 3, apartado 1, letra b), para actuar ante un organismo público vinculado o dependiente de la Administración General del Estado, adherido al REA-AGE y los contemplados en el artículo 3, apartado 1 letra c), para actuar ante un ministerio u organismo adherido al REA-AGE, se actuará en la forma señalada en el apartado 1º, siendo el Delegado del REA-AGE del ministerio u organismo al que esté adscrito el órgano competente de los trámites objeto del apoderamiento, el responsable de solicitar el bastanteo de los poderes a su servicio jurídico, en los términos que al efecto establezca la Abogacía General del Estado-Dirección del Servicio Jurídico del Estado, de la subsanación de defectos en su caso y de comprobar la incorporación del bastanteo en el REA-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, los tratamientos de datos personales que realicen lo será por cuenta del responsable, actuando 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 3 regula los tipos de apoderamientos y el contenido del REA-AGE, señalado en su aparatado 5 los datos necesarios para la inscripción en los siguientes términos:

> 5. Para inscribir un apoderamiento en el REA-AGE, se harán constar, al menos, los siguientes datos:
> a) Nombre y apellidos (para el caso de persona física), denominación o razón social (para el caso de persona jurídica) y NIF/NIE del poderdante.
> b) Nombre y apellidos (para el caso de persona física), denominación o razón social (para el caso de persona jurídica) y NIF/NIE del apoderado.

c) Tipología del poder.
d) Copia electrónica de documento público o privado con firma notarialmente legitimada, cuando proceda.
e) Estatutos de persona jurídica cuando actúa como apoderado, cuando proceda
f) El bastanteo de los poderes, cuando proceda
g) Periodo de vigencia del poder.
h) Fecha de otorgamiento.
i) Número de referencia del alta y fecha de alta en el REA-AGE.

Dicho precepto desarrolla lo previsto en el artículo 6.3 de la Ley 39/2015:

Los asientos que se realicen en los registros electrónicos generales y particulares de apoderamientos deberán contener, al menos, la siguiente información:

a) Nombre y apellidos o la denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del poderdante.
b) Nombre y apellidos o la denominación o razón social, documento nacional de identidad, número de identificación fiscal o documento equivalente del apoderado.
c) Fecha de inscripción.
d) Período de tiempo por el cual se otorga el poder.
e) Tipo de poder según las facultades que otorgue.

Por consiguiente, la Orden está concretando el contenido mínimo previsto en la Ley 39/2015, estableciendo una regulación más detallada pero con el mismo carácter abierto, ya que establece que dichos datos son los que se harán constar “al menos”, por lo que está admitiendo que se puedan incluir más datos en los formularios que pueda aprobar la Secretaría de Estado de Política Territorial y Función Pública, conforme a la disposición adicional tercera de la misma.

En este punto, hay que tener en cuenta, desde la perspectiva de la protección de datos personales, la vigencia del principio de minimización recogido en el artículo 5.1.c) del RPGD, de modo que los datos personales serán “adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados”. **Por ello, siendo la Orden informada la norma jurídica de inferior rango que regula los datos que deben figurar en el Registro, la enumeración contenida en la misma debería ser cerrada, especificando los datos que deben figurar en el mismo atendiendo al citado principio, sin dejar una puerta abierta a una mayor de desagregación de la información que podría incurrir, si se hiciera referencia a datos personales, a la infracción de ese mencionado**

principio de minimización si el dato no fuera indispensable para la finalidad del tratamiento.

IV

El artículo 10 regula las consultas de los órganos y organismos públicos:

> El REA-AGE ofrecerá a los organismos interesados las siguientes vías de acceso a la información:
>
> a) Descarga, bajo petición, de un fichero, que contendrá todos los apoderamientos vigentes y válidos para los trámites y actuaciones por medios electrónicos de los que el órgano administrativo peticionario sea competente. El fichero contendrá todos los datos de los apoderamientos que se enumeran en el artículo 3 de esta Orden.
>
> b) Acceso en línea mediante servicios web, a los efectos de comprobar, automáticamente y en tiempo real desde las aplicaciones, que un apoderamiento está vigente. Las peticiones al REA-AGE, relativas a los apoderamientos vigentes y válidos para los procedimientos y trámites por medios electrónicos de las que el órgano administrativo peticionario sea competente, se enviarán por un canal seguro de comunicaciones y deberán firmarse con firma electrónica avanzada cualificada o sello electrónico cualificado del citado órgano o administración de adscripción. La aplicación de soporte al Registro mantendrá trazabilidad de todas las peticiones recibidas.

Dicho precepto mantiene las dos posibilidades de acceso previstas en el artículo 11 de la Orden HAP/1637/2012, de 5 de julio, por la que se regula el Registro Electrónico de Apoderamientos. No obstante, esta Agencia considera que, de acuerdo con los principios recogidos en el artículo 5 del RGPD, el mantenimiento de ambas posibilidades resulta excesivo e incrementa los riesgos derivados del tratamiento de datos personales.

En primer lugar, la descarga del fichero procede solo en los casos en los que así se solicite, por lo que en otro caso debería acudirse al acceso en línea previsto en la letra b). Además, no se establece la periodicidad con la que debe realizarse dicha descarga, los que plantea el problema de dar cumplimiento al principio de exactitud de los datos previsto en la letra d) del artículo 5.1. del RGPD, de acuerdo con el cual los datos personales serán “exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan”. Por ello, pese a la descarga del archivo, y salvo que la misma se realizara de una manera prácticamente

constante a fin de acreditar la vigencia de los poderes o las posibles rectificaciones realizadas en los datos de carácter personal, seguiría siendo necesario acudir al acceso en línea, para el cual, además, se han previsto unas garantías adicionales que no se establecen en el supuesto de descarga del fichero.

Por otro lado, la descarga del fichero va a permitir a los órganos y organismos de la Administración General del Estado y de otras administraciones que se adhieran al mismo acceder a todos los datos personales obrantes en el fichero, en la medida en que se refieran a trámites y actuaciones por medios electrónicos de los que el órgano administrativo peticionario sea competente, independientemente de que se correspondan con la tramitación de un procedimiento concreto, lo que sería excesivo y contrario al principio de minimización de datos, así como a la doctrina establecida por el Tribunal Constitucional contraria a los accesos masivos e indiscriminados a datos personales, recogida, entre otras, en su sentencia del Tribunal Constitucional17/2013, de 31 de enero.

Por todo ello, la descarga del fichero supondría un acceso masivo a datos personales que, además, no excluye la necesidad de acudir al acceso en línea para verificar la vigencia del poder siendo, por tanto, contraria al principio de minimización de datos y al principio de proporcionalidad, en la medida en que exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad, recogido, entre otras, en la sentencia del Tribunal Constitucional 14/2003, de 28 de enero.

Por consiguiente, esta Agencia que el procedimiento de acceso a los datos personales obrantes en el Registro que mejor se adecúa a la normativa sobre protección de datos personales es el contemplado en la letra b, el acceso en línea, para el cual el precepto establece unas garantías adicionales, sin perjuicio del resto de garantías que deban adoptarse conforme a lo que se señalará en el apartado siguiente. No obstante, también en este supuesto se deberán adoptar las medidas técnicas y organizativas que garanticen el cumplimiento del citado principio de minimización, de modo que se acceda a los datos estrictamente necesarios para verificar la existencia, vigencia y alcance del poder en relación con la concreta actuación administrativa que se pretende realizar y para poder comunicarse con el representante.

Todo ello sin perjuicio de que deban arbitrarse otras medidas que permitan, respetando igualmente el citado principio de minimización, acceder a los datos en los casos de fallo del sistema y siempre que, por razones de urgencia, no pueda esperarse al restablecimiento del mismo, debiendo preverse las garantías oportunas.

V

El artículo 11 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 poderdante o del apoderado, 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 poderdante o el apoderado 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).

En el presente caso, debe partirse de que uno de los objetivos de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, es la generalización del uso de medios electrónicos en las relaciones entre las Administraciones públicas y los ciudadanos para la realización de cualquier trámite de un procedimiento administrativo, si bien faculta a las personas físicas a elegir en todo momento si se comunican con las Administraciones públicas para el ejercicio de sus derechos y obligaciones a través de medios electrónicos o no, salvo que estén obligados a relacionarse a través de medios electrónicos por establecerlo de forma expresa la Ley, impulsando, de este modo, la denominada Administración electrónica.

Partiendo de esa premisa y a los efectos del presente informe, 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”, el tratamiento de los datos personales de los interesados en el procedimiento y de sus representantes deriva de lo previsto en el artículo 5 de la Ley 39/2015, que recoge la posibilidad de intervenir en el procedimiento mediante representante, señalando en su apartado 1 que “Los interesados con capacidad de obrar podrán actuar por medio de representante, entendiéndose con éste las actuaciones administrativas, salvo manifestación expresa en contra del interesado” y en su apartado 2 que “Las personas físicas con capacidad de obrar y las personas jurídicas, siempre que ello esté previsto en sus Estatutos, podrán actuar en representación de otras ante las Administraciones Públicas”. En cuanto a la acreditación del poder, el artículo 4 señala que “La representación podrá acreditarse mediante cualquier medio válido en Derecho que deje constancia fidedigna de su existencia. A estos efectos, se entenderá acreditada la representación realizada mediante apoderamiento apud acta efectuado por comparecencia personal o comparecencia electrónica en la correspondiente sede electrónica, o a través de la acreditación de su

inscripción en el registro electrónico de apoderamientos de la Administración Pública competente". Por consiguiente, el precepto se inspira en el principio antiformalista que ya recogía la Ley 30/1992, admitiendo la acreditación del poder por cualquier medio admisible en Derecho, siendo la inscripción en el Registro de apoderamientos uno más de los medios previstos para su acreditación, pero que no excluye que el poder, incluidos los otorgados apud acta, pueda acreditarse por otros medios, como la comparecencia personal a la que se refiere el propio precepto, careciendo dicha inscripción de efectos constitutivos, y siendo necesaria, tal y como se recoge en el proyecto de Orden, la previa solicitud para su inscripción, que según la regulación proyectada podrá presentar tanto el poderdante como el apoderado, así como la aceptación de este último para que el poder surta efectos en el primer caso.

De este modo, teniendo en cuenta que la eficacia de la inscripción depende de la voluntad del poderdante y del apoderado, podría plantearse si la base jurídica del tratamiento de sus datos sería el consentimiento, tal y como se analizó en el Informe 51/2020, referente al Proyecto de Orden por la que se regula el registro electrónico de apoderamientos de la Seguridad Social:

> Una circunstancia sobre la que merece extenderse un poco es cuál sería la base jurídica que aplicaría al tratamiento de datos personales derivado del registro de apoderamientos. A diferencia del momento en que se promulgó la orden de 2013, que el consentimiento ya no es la única, y ni siquiera la principal, base jurídica del tratamiento puesto que el RGPD contiene un elenco de bases jurídicas en su artículo 6.1, todas ellas de la misma importancia, y que sean aplicables según las circunstancias de cada caso concreto. Es cierto que el RGPD considera con carácter General que cuando existe un desequilibrio de poder la base jurídica del tratamiento no podrá ser la del consentimiento o puesto que éste no se entenderá otorgado libremente. Así, el considerando 43, indica claramente que no es probable que las autoridades públicas puedan basarse en el consentimiento para realizar el tratamiento de vida dicha disparidad o desequilibrio con el interesado. Sin embargo, y tal y como ha expuesto el Grupo de Trabajo del art. 29 de la Directiva 95/46/CE, posteriormente refrendado por el Comité Europeo de Protección de Datos, en las Directrices sobre el consentimiento en el sentido del Reglamento (UE) 2016/679 adoptadas el 28 de noviembre de 2017 revisadas por última vez y adoptadas el 10 de abril de 2018 (WP 259), el uso del consentimiento como base jurídica para el tratamiento de datos por parte de las autoridades públicas no queda totalmente excluido en virtud del marco jurídico del RGPD, y en dichas directrices se exponen determinados ejemplos.
>
> Cabe considerar que en este caso concreto el consentimiento del interesado si podría ser base jurídica suficiente para el tratamiento de los datos propios del Poderdante, por cuanto no resulta de la regulación de la orden que se siga ningún perjuicio para el administrado en el caso de

que decida no actuar en el procedimiento administrativo de seguridad social mediante un apoderado, pues en ese caso bien puede actuar directamente en su condición de interesados sin necesidad de apoderar a un tercero.

En cuanto al tratamiento por la administración de los datos de los apoderados, no sería posible el consentimiento del Poderdantes como base jurídica, dado que el apartado a) del art. 6.1 RGPD tan sólo hace referencia a esta base jurídica para permitir el tratamiento de "sus" datos personales, esto es de quien presta el consentimiento. Tampoco sería válida la base jurídica del interés legítimo de la letra f), por cuanto el último párrafo del art. 6.1 RGPD ver a esa posibilidad al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones. Por lo tanto, cabe concluir que la base jurídica para el tratamiento de los datos de los apoderados podría ser la establecida en la letra e) del art. 6.1: el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento.

No obstante, teniendo en cuenta el procedimiento articulado en la Orden, en la que la solicitud de inscripción la pueden realizar tanto el poderdante como el apoderado, diferenciándose, en cuanto a sus requisitos y tramitación en función de que uno u otro puedan ser personas físicas no obligadas a relacionarse electrónicamente con la Administración, y siendo la finalidad del Registro la articular un mecanismo que facilite al interesado la actuación por medio de representante, una vez solicitada la inscripción, el tratamiento de los datos personales incluidos en el Registro electrónico de apoderamientos lo es a los efectos de acreditar la misma, de modo que las actuaciones administrativas se entiendan con el representante, salvo manifestación en contra del interesado, y ello es necesario para el adecuado desarrollo del procedimiento administrativo, en el que deberá quedar debidamente acreditada dicha representación, **por lo que encontraría su fundamento 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".**

A juicio de esta Agencia, para que el tratamiento pudiera ampararse en el cumplimiento de una obligación legal aplicable al responsable, hubiera sido necesario que en la Ley 39/2015 se hubiese establecido dicha inscripción como obligatoria para que pudiera acreditarse la representación, sin admitir otros medios de acreditación, lo que hubiera ido en contra del principio antiformalista que inspira dicha normativa.

Por consiguiente, aun siendo potestativo para el interesado la actuación por medio de representante y el otorgamiento del poder correspondiente, así como para el apoderado su aceptación, pudiendo en cualquier momento

revocar el poder o renunciar a la representación, en tanto en cuanto no se produzcan dichas circunstancias, el tratamiento de los datos personales necesarios para proceder a la inscripción de los mismos en el Registro se encontraría amparado por lo dispuesto en la letra e) del artículo 6.1.del RGPD, habiéndose 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”, sin perjuicio del deber de informar a los afectados en los términos previstos en los artículos 13 y 14 del RGPD, pudiendo realizarse dicha información “por capas”, conforme al artículo 11 de la LOPDGDD.

En todo caso, siendo la finalidad del Registro la de acreditar la representación y su vigencia, una vez que el poderdante haya revocado el poder, el apoderado haya renunciado, o haya transcurrido el plazo máximo de vigencia del apoderamiento sin que se haya prorrogado, no podría continuarse con el tratamiento de los datos, al haber desaparecido la finalidad del mismo, debiendo procederse a su supresión sin dilación, conforme al artículo 17.1.a) del RGPD.

En este caso, teniendo en cuenta la vinculación del tratamiento a la voluntad de los afectados, en los términos que se han señalado, y al objeto de garantizar debidamente el principio de limitación de la finalidad recogido en el artículo 5.1.b) del RGPD, la norma debería recoger, expresamente, al amparo del artículo 6.3. del RGPD, que **los datos personales recogidos en el Registro no podrán tratarse para una finalidad diferente a la acreditación de la existencia y vigencia de un apoderamiento inscrito, debiendo suprimirse, sin dilación, en los supuestos de revocación, renuncia o finalización del plazo de vigencia del apoderamiento.**

Por otro lado, debe hacerse especial referencia a las medidas de seguridad que deben adoptarse para salvaguardar el derecho a la protección de datos, al no existir ya, a diferencia de lo que ocurría en el momento de aprobación de la Ley 39/2015, un elenco cerrado de las mismas establecido por la legislación de protección de datos.

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.

VI

En relación con el artículo 12 sobre la interoperabilidad del Registro, debe reiterarse lo señalado en el apartado anterior respecto a la seguridad de los datos personales, **por lo que debe modificarse el mismo para incluir la necesaria garantía de la protección de los datos personales**.

VII

Por último, figuran como Anexos a la Orden los correspondientes formularios normalizados. Dichos formularios, así como aquellos otros que pueda aprobar la Secretaría de Estado de Política Territorial y Función Pública en virtud de la Disposición adicional tercera deben ajustarse a la normativa sobre protección de datos personales y, singularmente, al principio de minimización ya citado. A estos efectos, se considera que el número de

teléfono de las personas físicas no es un dato necesario para la finalidad del registro, del mismo modo que tampoco lo es el dato del correo electrónico cuando el poderdante es una persona física que no esté obligada a relacionarse con la administración por medios electrónicos. **Por tanto, debería de modificarse los Anexos para indicar que la aportación del número de teléfono y el correo electrónico, en los supuestos indicados, es optativa y que su falta de cumplimentación no impedirá su inscripción.**

También **debe revisarse la cláusula informativa** para la adecuación a las observaciones realizadas en el presente informe, especialmente la relativa a la base jurídica, para indicar que es el artículo 6.1.e) 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) y que la finalidad del tratamiento no es únicamente la gestión de solicitudes de inscripción de poderes sino, especialmente, la acreditación de la representación en los términos previstos en los artículos 9 y 10.