

Antes de entrar a analizar el texto sometido a informe es preciso señalar que, habida cuenta de la fundamentación legal del informe que inmediatamente va a evacuarse y su carácter preceptivo, a tenor de lo dispuesto en las normas que acaban de señalar, debería indicarse en la Exposición de Motivos de la norma que la misma ha sido sometida al previo informe de la Agencia Española de Protección de Datos.

I

Tal y como dispone el artículo 1.1 del texto sometido a informe constituye su objeto la aprobación de la Administración Electrónica del Ministerio de Derechos Sociales y Agenda 2030, así como el establecimiento del marco organizativo y tecnológico de la misma.

En este sentido, el artículo 11 del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica “exige que todos los órganos superiores de las Administraciones públicas dispongan formalmente de su política de seguridad, que se aprobará por el titular del órgano superior correspondiente. Esta política de seguridad se establecerá con base en los principios básicos recogidos en el capítulo II de la propia norma (seguridad integral, gestión de riesgos, prevención, reacción y recuperación, líneas de defensa, reevaluación periódica, y función diferenciada) y desarrollará una serie de requisitos mínimos consignados en el ya mencionado artículo 11.1”.

De este modo, el Proyecto desarrolla los principios de la seguridad de la información, así como los objetivos que garantizan su cumplimiento. Igualmente se desarrolla la estructura organizativa del Departamento en relación con la seguridad de la información, bajo la dirección de la Comisión Ministerial de Administración Digital, las directrices en materia de gestión de riesgos y los instrumentos normativos de la política de seguridad, conformados por tres niveles normativos estructurados jerárquicamente.

En lo que atañe a la protección de datos de carácter personal, el preámbulo de la norma hace referencia a la entrada en vigor del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento

de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, normas que igualmente cita en el Artículo 3 relativo al Marco legal y regulatorio de la seguridad de la información.

De ahí que el artículo 4.1 d) establece, dentro de los principios rectores de la seguridad de la información, y siguiendo lo establecido en el artículo 6 del Esquema nacional de Seguridad, el de gestión de riesgos, indicando que “de acuerdo a lo establecido en los artículos 24, 25 y 32 del Reglamento (UE) 2016/679, en el artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre, así como en el artículo 6 del Real Decreto 3/2010, de 8 de enero, el análisis y gestión de riesgos será parte esencial del proceso de seguridad. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, el impacto y la probabilidad de los riesgos a los que estén expuestos y la eficacia y el coste de las medidas de seguridad. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales”.

Asimismo, se configura como primero de los principios particulares enumerados en el artículo 2 el de protección de datos personales, indicando que “se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. Tal y como se establece en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en Ley Orgánica 3/2018, de 5 de diciembre, dichas medidas deberán ser apropiadas en función del análisis de riesgos, así como de una evaluación de impacto relativa a la protección de datos cuando sea probable que un tratamiento, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas”.

Dentro de la regulación de la estructura organizativa del departamento se determina que la misma estará compuesta, además de por la Comisión Ministerial de Administración Digital, por el Responsable de Seguridad, los Responsables de la Información, Responsables del Servicio, Responsables del Sistema, así como por los Delegados de Protección de Datos.

En cuanto al Delegado de Protección de Datos, se regula en el artículo 13:

“1. El Delegado de Protección de Datos ejerce las funciones detalladas en la sección 4 del capítulo IV del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en el capítulo III del título V de la Ley Orgánica 3/2018, de 5 de diciembre. Tendrá en todo caso acceso al

registro de las actividades de tratamiento de datos personales al que se refiere el artículo 30 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

La actuación de los Delegados de Protección de Datos se regirá por el principio de independencia, por lo que no recibirán ninguna instrucción en lo que respecta al desempeño de sus funciones. Podrán estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación.

2. La designación de los Delegados de Protección de Datos del Ministerio de Derechos Sociales y Agenda 2030 y de los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, se efectuará de conformidad con el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre. En consecuencia, serán designados atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que tienen encomendadas. Se comunicarán los nombramientos al Responsable de Seguridad.

El artículo 15, relativo a la gestión de los riesgos, comienza señalando que:

“1. La gestión de riesgos debe realizarse de manera continua sobre el sistema de información, conforme a los principios de gestión de la seguridad y protección de datos, basada en los riesgos, artículo 6 del Real Decreto 3/2010, de 8 de enero, y artículo 24 del Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y artículo 28 de la Ley Orgánica 3/2018, de 5 de diciembre y reevaluación periódica, artículo 9 del Real Decreto 3/2010, de 8 de enero, siendo el Responsable del Servicio el encargado de solicitar el preceptivo análisis de riesgos y de que se proponga el tratamiento adecuado, calculando los riesgos residuales. [...]”

Y concluye diciendo:

“5. Las indicadas fases del proceso de gestión de riesgos se realizarán según lo dispuesto en los anexos I y II del Real Decreto 3/2010, de 8 de enero, y siguiendo las normas, instrucciones, guías CCN-STIC y recomendaciones para la aplicación del mismo elaboradas por el Centro Criptológico Nacional, así como todo lo referente al análisis de riesgo y de impacto en la protección de datos especificado en el citado Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016”.

El artículo 13, lleva por rúbrica protección de datos de carácter personal, estableciendo que:

“1. En el ámbito del Ministerio de Derechos Sociales y Agenda 2030, la garantía de la protección de datos de carácter personal de las actividades de

tratamiento es un objetivo compartido por todas las unidades del Departamento que se rige por los siguientes principios:

- a. Licitud, lealtad y transparencia.
- b. Limitación de la finalidad.
- c. Minimización de datos.
- d. Exactitud.
- e. Limitación del plazo de conservación.
- f. Integridad y confidencialidad.
- g. Responsabilidad proactiva.

2. Se aplicarán a los datos personales que sean objeto de tratamiento por parte del Ministerio de Derechos Sociales y Agenda 2030 las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de, conforme se detalla en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y en la Ley Orgánica 3/2018, de 5 de diciembre.

Además, se aplicarán las medidas correspondientes al anexo II del Real Decreto 3/2010, de 8 de enero.

En el caso de que el análisis de riesgos determine medidas agravadas respecto a la normativa recogida en el anexo II del Real Decreto 3/2010, de 8 de enero, dichas medidas derivadas del análisis de riesgos serán las que se implementarán en la protección de datos personales.

3. En relación con los sistemas de información que, para soportar la prestación de servicios de administración electrónica, manejen datos de carácter personal, prevalecerán las mayores exigencias contenidas en la normativa de protección de datos en vigor que afecte al sistema de información concreto.”

II

El texto sometido a informe debe ser objeto de análisis atendiendo a lo dispuesto en el Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, RGPD) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En efecto, como indica la Exposición de motivos de la Ley 3/2018 “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”. De este modo, el cambio de aproximación de la normativa de protección de datos implica

necesariamente una modificación en el enfoque que habrá de darse a las políticas de seguridad de la información, en que se evoluciona de un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos que deberá incardinarse en el texto ahora sometido a informe.

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 la información, 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).

III

De lo que acaba de indicarse se desprenden dos conclusiones que afectan sustancialmente al Proyecto objeto de informe: por una parte, la evolución del modelo desde la lista de cumplimiento a la responsabilidad activa impone que el análisis de riesgos en materia de protección de datos y, en su caso la evaluación de impacto en la misma, pase a formar parte integrante de la política de seguridad de la información, de modo que no se produzca 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 papel del Delegado de Protección de Datos, obligatorio en el supuesto que ahora se está analizando, resulta esencial en todo el diseño y desarrollo de la política de seguridad de la información, debiendo tener pleno conocimiento de la misma y asesorar en su diseño e implantación, en virtud de las funciones que el reglamento general de Protección de Datos le otorga expresamente.

No obstante, tal y como se indicó en el Informe 170/2018, de 12 de noviembre de 2018, relativo a la compatibilidad funcional del delegado de protección de datos del RGPD y el responsable de seguridad del Esquema Nacional de Seguridad, se hace preciso deslindar dichos ámbitos:

“Con carácter previo a analizar la concreta cuestión que planteada en la consulta este Gabinete Jurídico estima conveniente hacer una referencia previa a la diferenciación, sustantiva y competencial, que existe entre el ámbito de la seguridad de información y el de la protección de datos de carácter personal.

Por lo que se refiere a la seguridad de la información, la misma comprende el conjunto de técnicas y medidas orientadas a garantizar la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para cualquier organización, independientemente del formato que tengan. En el ámbito de las Administraciones Públicas españolas y en relación con los sistemas que manejan información en formato electrónico (comúnmente denominados “Tecnologías de la Información y las Comunicaciones (TIC)”), el artículo 42.2 de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, actualmente sustituido por el artículo 156.2 de la Ley 40/2015, de régimen jurídico del sector público, creó el Esquema Nacional de Seguridad, que tiene por objeto establecer la política de seguridad en la utilización de medios electrónicos en el ámbito de la citada Ley, y está constituido por los principios básicos y requisitos mínimos que garanticen adecuadamente la seguridad de la información tratada.

Dicho precepto encuentra su desarrollo reglamentario en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, cuyo Preámbulo señala que “la finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones públicas, el ejercicio de derechos y el cumplimiento de deberes a través

de estos medios” añadiendo que “en este contexto se entiende por seguridad de las redes y de la información, la capacidad de las redes o de los sistemas de información de resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles”.

En este ámbito, son múltiples los órganos que ostentan competencias, pudiendo destacarse, conforme a lo recogido en el reciente Real Decreto-ley 12/2018, de 7 de septiembre, de seguridad de las redes y sistemas de información, al Centro Criptológico Nacional (CCN) responsable del citado ENS, el Instituto Nacional de Ciberseguridad (INCIBE) y el Ministerio de Defensa.

Por el contrario, la protección de datos de carácter personal de las personas físicas se configura como un auténtico derecho fundamental que encuentra su fundamento en el artículo 18.4 de la Constitución Española, conforme al cual “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”. Así lo ha reconocido nuestro Tribunal Constitucional, destacando en la Sentencia 94/1998, de 4 de mayo que el citado artículo 18.4 “no sólo entraña un específico instrumento de protección de los derechos del ciudadano frente al uso torticero de la tecnología informática, sino que consagra un derecho fundamental autónomo a controlar el flujo de informaciones que conciernen a cada persona -a la «privacidad» según el neologismo que reza en la Exposición de Motivos de la LORTAD- pertenezcan o no al ámbito más estricto de la intimidad, para así preservar el pleno ejercicio de sus derechos”.

Así se recoge en el Preámbulo del Proyecto de Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales, que por su claridad se transcribe a continuación:

“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». Se hacía así eco de los trabajos desarrollados desde finales de la década de 1960 en el Consejo de Europa y de las pocas disposiciones legales adoptadas en países de nuestro entorno.

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; 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 aquél 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 uso.

A nivel legislativo, la concreción y desarrollo del derecho fundamental de protección de las personas físicas en relación con el tratamiento de datos personales tuvo lugar en sus orígenes mediante la aprobación de la Ley Orgánica 5/1992, de 29 de octubre, reguladora del tratamiento automatizado de datos personales, conocida como LORTAD. La Ley Orgánica 5/1992 fue reemplazada por la Ley Orgánica 15/1999, de 5 de diciembre, de protección de datos personales, a fin de trasponer a nuestro derecho a 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. Esta ley orgánica supuso un segundo hito en la evolución de la regulación del derecho fundamental a la protección de datos en España y se complementó con una cada vez más abundante jurisprudencia procedente de los órganos de la jurisdicción contencioso-administrativa.

Por otra parte, también se recoge en el artículo 8 de la Carta de los Derechos Fundamentales de la Unión Europea y en el artículo 16.1 del Tratado de Funcionamiento de la Unión Europea. Anteriormente, a nivel europeo, se había adoptado la Directiva 95/46/CE citada, cuyo objeto era procurar que la garantía del derecho a la protección de datos personales no supusiese un obstáculo a la libre circulación de los datos en el seno de la Unión, estableciendo así un espacio común de garantía del derecho que, al propio tiempo, asegurase que en caso de transferencia internacional de los datos, su tratamiento en el país de destino estuviese protegido por salvaguardas adecuadas a las previstas en la propia directiva”.

Y en este mismo sentido se pronuncia 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 sus datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general

de protección de datos, RGPD), que tiene por objeto “proteger los derechos y libertades fundamentales de las personas físicas y, en particular, su derecho a la protección de los datos personales” (artículo 1.2.), destacando en su Considerando 1 que “la protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental” y en su Considerando 10 que “para garantizar un nivel uniforme y elevado de protección de las personas físicas y eliminar los obstáculos a la circulación de datos personales dentro de la Unión, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos deber ser equivalente en todos los Estados miembros. Debe garantizarse en toda la Unión que la aplicación de las normas de protección de los derechos y libertades fundamentales de las personas físicas en relación con el tratamiento de datos de carácter personal sea coherente y homogéneo”.

Consecuentemente, el derecho a la protección de datos de carácter personal de las personas físicas es un derecho fundamental y, por tanto, situado en el máximo nivel de protección jurídica, que actualmente se encuentra regulado directamente por la normativa comunitaria, estableciendo el citado RGPD un conjunto de principios, derechos, obligaciones y una estructura organizativa tendentes a garantizar dicho derecho fundamental. Dentro de los mismos, la seguridad de la información aparece como una obligación más de los responsables y encargados del tratamiento quienes deberán aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluirán, entre otros factores “la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento” y “la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico” (artículo 32.2. b) y c) del RGPD).

Por lo tanto, no cabe duda de que la garantía de la seguridad de los datos personales adquiere una especial trascendencia en cuanto a su protección, pero sin que ésta se limite exclusivamente al ámbito de la seguridad de dicha información, en cuanto que la protección de datos personales tiene un ámbito mucho más extenso que abarca, como decíamos, a un conjunto de principios, derechos y obligaciones mucho más amplio.

Y todo ello bajo la garantía administrativa de las “autoridades de control”, funciones que en España asume, sin perjuicio de las competencias que corresponde a las autoridades de las Comunidades Autónomas en su ámbito competencial, la Agencia Española de

Protección de Datos, que actúan con total independencia en el desempeño de sus funciones y en el ejercicio de sus poderes (Artículo 52 RGPD) y son las únicas competentes para “asesorar sobre las medidas legislativas y administrativas relativas a la protección de los derechos y libertades de las personas físicas con respecto al tratamiento” (artículo 57.1.c) RGPD)”.

El Proyecto sometido a informe toma en cuenta estas consideraciones, por cuanto incluye al delegado de protección de datos dentro de la estructura organizativa de la gestión de la seguridad de la información y atribuyendo al mismo las funciones que establece el propio Reglamento, de modo que sea oído en todo caso en el diseño e implantación de dicha política de seguridad.

Asimismo, partiendo de una visión conjunta de la gestión de riesgos en el artículo 4.1.d), se diferencia por un lado la gestión de riesgos de la seguridad, a la que se refiere el artículo 15, y la gestión de riesgos de la privacidad a la que se refiere el artículo 16, estableciendo la necesaria coordinación entre ambas atendiendo al resultado del análisis de riesgos y, en su caso, de la evaluaciones de impacto relativas a la protección de datos. Por tanto, se ha tenido en cuenta el nuevo régimen de protección de datos, basado en la necesidad de realización del análisis de riesgos establecido en el artículo 24 del Reglamento y, en su caso, de la evaluación de impacto en la protección de datos a la que se refiere su artículo 35 para la determinación de las medidas que garanticen adecuadamente la seguridad de la información desde el enfoque de la protección de datos de carácter personal. Además, se recoge expresamente, tal y como ha venido informando esta Agencia, que las medidas a implantar como consecuencia del análisis de riesgos previsto en el artículo 24.1 del RGPD, en caso de resultar agravadas respecto de las previstas en el Esquema Nacional de Seguridad deberán prevalecer sobre éstas últimas, a fin de dar adecuado cumplimiento a lo exigido por el Reglamento General de Protección de Datos.

IV

Debe hacerse especial referencia, como ya se anticipó, a la figura del Delegado de Protección de Datos.

La inclusión del delegado de protección de datos dentro de la estructura organizativa vinculada con la seguridad de la información resulta, como se ha expuesto en el apartado anterior, esencial dentro del esquema establecido en el Reglamento general de protección de datos. Y en ese sentido cabe valorar muy positivamente la referencia que el Proyecto hace de la citada figura.

Ahora bien, es necesario que dicha inclusión se lleve a cabo teniendo particularmente en cuenta cuál es la misión y las funciones del delegado de protección de datos dentro del sistema de responsabilidad activa establecido por el mencionado Reglamento general.

En este sentido, resulta esencial diferenciar al delegado de protección de datos de la figura del propio responsable del tratamiento, bien con carácter general, bien en el sentido de la estructura organizativa que tendrá a su cargo el cumplimiento de las obligaciones impuestas por la normativa de protección de datos.

En este sentido, el Reglamento es claro a la hora de imponer al responsable la obligación de cumplimiento de las medidas que el mismo prevé. Será así el responsable quien deberá mantener un registro de operaciones de tratamiento, evaluar el riesgo concurrente en un determinado tratamiento de datos o desarrollar en su caso a evaluación de impacto exigida por el reglamento. Del mismo modo, será el que habrá de determinar las medidas técnicas y organizativas que hayan de adoptarse para garantizar la seguridad del tratamiento. Lógicamente, estas medidas se desarrollarán por quienes las tuvieran atribuidas dentro de la estructura del responsable, siendo especialmente relevantes a estos efectos los distintos sujetos enumerados en los apartados 2 a 5 del artículo 5 del Proyecto y, particularmente, el responsable de seguridad.

Frente a lo que acaba de indicarse, la función del delegado de protección de datos será la de prestar al responsable la asistencia y asesoramiento necesarios en el proceso de adopción de las medidas y supervisar que las mismas se han adoptado y se llevan a la práctica. Es decir, el delegado de protección de datos asesora al responsable y controla el cumplimiento de las obligaciones establecidas por la normativa de protección de datos de carácter personal.

En este sentido, el documento de directrices sobre los delegados de protección de datos, adoptado por el Grupo de Trabajo creado por el artículo 29 de la Directiva 95/46/CE el 13 de diciembre de 2016 y revisado el 5 de abril de 2017 (documento WP243), aclara que “El RGPD establece claramente que es el responsable y no el DPD quien está obligado a aplicar «medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento» (artículo 24, apartado 1). El cumplimiento de las normas en materia de protección de datos es responsabilidad corporativa del responsable del tratamiento, no del DPD”.

Por otro lado, en el citado Informe 170/2018 en relación con la diferenciación entre el DPD y el responsable de seguridad del ENS, se señalaba lo siguiente:

IV

Las posiciones del RSEG y del DPD son requisitos exigidos en normas diferenciadas con objetivos y ámbitos de aplicación distintos y, el principio de independencia del DPD, debería entenderse de manera amplia incluso con relación a las figuras que menciona el artículo 10 del ENS. En el mismo orden de ideas, cabría tener en cuenta que el propio principio de segregación de funciones del ENS tuviera en cuenta la separación de los roles indicados (RINF, RSEG, RSER) con relación a las funciones del DPD.

Debe de entenderse que la función de seguridad de la información es una herramienta que permite abordar el cumplimiento de lo previsto en el artículo 32 del RGPD, pero no puede entenderse como una herramienta que garantice el pleno e íntegro cumplimiento del RGPD. En consecuencia, las funciones del RSEG tienen un alcance limitado en el RGPD frente al alcance de las competencias del DPD.

Carece de sentido que se especifique la diferenciación de los tres roles relacionados con la seguridad de la información en las Administraciones Públicas, y se quiera asignar ahora un rol adicional, el de DPD, al responsable de seguridad de la información. Resulta claro que un DPD, alimentará de requisitos, aconsejará y supervisará a los tres responsables: información, servicio y seguridad. Si el responsable de seguridad asume las tareas de DPD, se le asigna de forma directa tareas de los otros dos responsables, lo que contradice el propio ENS y, sin duda, generaría posibles conflictos de intereses que podrían afectar a los derechos y libertades de las personas o incluso a la propia seguridad de la información.

En definitiva, esa diferenciación de tareas que garantiza la efectividad del trabajo del responsable de seguridad tiene sentido extenderla a que no se le asignen tareas no específicas de su función. Del mismo modo que la necesaria independencia del DPD y la necesidad de evitar los conflictos de intereses impide asignarle responsabilidades directas en un ámbito que va a tener que supervisar y en el que estará sujeto a instrucciones de otros órganos.

Así lo han entendido en organizaciones con importantes responsabilidades en materia de seguridad de la información. En este sentido, en el Ministerio de Defensa, en el que la información “constituye un recurso estratégico del Departamento sobre el que se debe buscar la superioridad para facilitar el cumplimiento y alcanzar el éxito de los cometidos encomendados al Ministerio de Defensa y de las misiones de las Fuerzas Armadas” (artículo 2 de la Orden DEF/1196/2017, de 27 de

noviembre, por la que se establece la Estrategia de la Información del Ministerio de Defensa), está dotado de una estructura que depende del Secretario de Estado de Defensa en cuanto órgano responsable de la dirección, impulso y gestión de las políticas de las tecnologías, sistemas y seguridad de la información (artículo 4 del Real Decreto 998/2017, de 24 de noviembre, por el que se desarrolla la estructura orgánica básica del Ministerio de Defensa) y que se desarrolla en diferentes órdenes ministeriales, además de la ya citada Orden DEF/1196/2017: la Orden Ministerial 76/2006, de 19 de mayo, por la que se aprueba la política de seguridad de la información del Ministerio de Defensa, la Orden DEF/2639/2015, de 3 de diciembre, por la que se establece la Política de los Sistemas y Tecnologías de la Información y las Comunicaciones del Ministerio de Defensa y la Orden ministerial 5/2017, de 9 de febrero por la que se aprueba la Política de Gestión de Documentos electrónicos del Ministerio de Defensa.

Sin embargo, el delegado de protección de datos ha sido designado al margen de dicha estructura, dependiendo directamente del Subsecretario de Defensa, con lo que se garantiza su independencia y se evita cualquier tipo de conflicto de intereses en el ejercicio de sus funciones.

V

En conclusión, es criterio de este Gabinete Jurídico que, con carácter general, debe existir la necesaria separación entre el delegado de protección de datos regulado en el RGPD y el responsable de seguridad del ENS, sin que sus funciones puedan recaer en la misma persona u órgano colegiado.

Solo excepcionalmente, en aquellas organizaciones que, por su tamaño y recursos, no pudieran observar dicha separación, sería admisible la designación como delegado de protección de datos de la persona que ejerciera las funciones de responsable de seguridad del ENS, siempre que en la misma concurren los requisitos de formación y capacitación previstos en el RGPD. Además, resultaría imprescindible adoptar todas las medidas organizativas, debidamente reflejadas en su Política de seguridad de la información, que garantice la necesaria independencia y la ausencia de conflicto de intereses, por lo que no podría recibir instrucciones respecto al desempeño de sus funciones como delegado de protección de datos, deberá responder directamente al más alto nivel jerárquico y no podrá participar en las decisiones relativas a los fines y medios del tratamiento. En todo caso, esta circunstancia, que como decíamos, tiene carácter excepcional, deberá evaluarse caso por caso, y deberá dejarse documentada dicha

designación haciendo constar los motivos por lo que el organismo correspondiente no ha podido observar dicha separación de funciones así como las medidas que garantizan la necesaria independencia del delegado de protección de datos.

El texto remitido respeta la separación de funciones anteriormente señalada, diferenciando debidamente entre la figura del responsable de seguridad y la de delegado de protección de datos, remitiéndose a la regulación de esta figura contenida tanto en el Reglamento (UE) 2016/679 como en la Ley Orgánica 3/2018.

De acuerdo con el apartado 3 del artículo 16, se prevé la existencia de diferentes delegados de protección de datos:

2. La designación de los Delegados de Protección de Datos del Ministerio de Derechos Sociales y Agenda 2030 y de los organismos dependientes o adscritos al mismo a los que, conforme al artículo 1, les sea de aplicación la presente PSI, se efectuará de conformidad con el artículo 37 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y el artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre. En consecuencia, serán designados atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones que tienen encomendadas. Se comunicarán los nombramientos al Responsable de Seguridad.

Asimismo, el apartado 1 de dicho precepto prevé que “Podrán estar asistidos por grupos de trabajo integrados por representantes de las unidades administrativas de su ámbito de actuación”.

Dicha posibilidad es conforme al RGPD y la LOPDGDD, debiéndose recordar lo manifestado por esta Agencia en el Informe 100/2019 respecto a la necesidad de dotar al DPD de los medios necesarios que permitan el adecuado ejercicio de sus funciones:

IV

Atendiendo a lo señalado en el presente informe, y ya al margen de lo solicitado en la presente consulta, esta Agencia debe incidir, una vez más, en la importancia que la figura del DPD tiene en el nuevo modelo instaurado por el RGPD y que pivota sobre la base de la responsabilidad proactiva del responsable. De acuerdo con el mismo, en los casos en que resulte obligatorio o así se haya estimado adecuado con carácter voluntario, ha de ser el responsable el que valore la procedencia de designar uno o varios DPD, así como si el mismo ha de pertenecer o no a su propia estructura, garantizando en todo momento su independencia y disponibilidad. Asimismo, deberá garantizar que el

DPD cumple con los requisitos de capacitación adecuados y que se le dota de los medios personales y materiales necesarios para la realización eficaz de las funciones que tiene encomendadas, que participa de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales y que rinde cuentas al más alto nivel jerárquico, documentando adecuadamente el responsable, conforme al ya citado principio de responsabilidad proactiva, todas las decisiones que adopte a este respecto, para poder demostrarlo a requerimiento de las autoridades de control. De este modo, quedará garantizado que el nombramiento del DPD no se ha realizado con carácter meramente formal y que el mismo cumple eficazmente con las funciones que le asigna el RGPD, siendo el primer interesado en dicha eficacia el propio responsable, que es quien responderá, y no el DPD, en caso de inobservancia del RGPD.

V

Por consiguiente, el proyecto de Orden se ajusta a lo dispuesto en el RGPD y la LOPDGDD, si bien se realizan las siguientes observaciones:

En primer lugar, en el preámbulo debería suprimirse la referencia a la Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo, ya que la misma no resulta de aplicación a los tratamientos que se realizan por el Ministerio de Derechos Sociales y Agenda 2030.

Por otro lado, siendo el responsable del tratamiento y, en su caso, el encargado, los obligados a dar cumplimiento a las previsiones de los artículos 24, 25 y 32 del RGPD, dentro del principio de responsabilidad diferenciada recogido en el artículo 4.1.b) debería indicarse que “En los supuestos de tratamientos de datos personales se identificará además a la persona, organismo o unidad responsable de tratamiento y, en su caso, al encargado de tratamiento, de acuerdo con lo dispuesto en el artículo 4, apartados 7 y 8 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016”.

Y en el principio de seguridad desde el diseño y por defecto (artículo 4.1.g), teniendo en cuenta que la protección de datos personales es más amplia que la mera seguridad de los datos, debería añadirse una referencia expresa a la protección de datos personales.