

N/REF: 0012/2022

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 se 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 del texto sometido a informe constituye su objeto la aprobación de la Política de Seguridad de la Información —PSI— en el ámbito de la Administración Digital del Ministerio Consumo, así como el establecimiento del marco organizativo 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”.

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”.

En lo que atañe a la protección de datos de carácter personal, el *preámbulo de la norma* se refiere tanto al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, como a 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 regulatorio* de la seguridad de la información.

En cuanto a las directrices en materia de gestión de riesgos, el borrador analizado —por vía de remisión— se conforma básicamente con las previsiones recogidas en el Esquema Nacional de Seguridad —ENS—, regulado por el citado Real Decreto 3/2010, de 8 de enero. Así, el artículo 4 del proyecto establece, que “Los principios básicos y requisitos de la seguridad de la información desarrollados bajo el marco de esta Política de Seguridad son los recogidos en el ENS, regulado por el Real Decreto 3/2010, de 8 de enero, en particular, los previstos en sus capítulos II y III, y su normativa de desarrollo”, *sin incorporar en su texto una referencia concreta* a los referidos principios y requisitos. En consecuencia, no se desarrollan de manera explícita dichos principios, resultando claramente insuficiente la fórmula utilizada —por vía de remisión— en orden a las exigencias de seguridad jurídica y a la efectiva aplicación de los citados principios.

En este sentido, se informa de que —en aras del propósito de la norma de dotar de mayor seguridad jurídica a la organización y funcionamiento de la Política de Seguridad de la Información, y en atención a la necesaria transparencia a la que se refiere su Preámbulo—, debería incorporarse explícitamente, preferentemente en su artículo 4, una mención expresa a los principios rectores de dicha seguridad, y, siguiendo lo establecido en el artículo 6 del Esquema Nacional de Seguridad, una referencia específica a la gestión de riesgos.

De tal modo, partiendo de una visión conjunta de la gestión de riesgos, la Orden que se informa debería diferenciar por un lado la gestión de riesgos de la seguridad y, por otro lado, la gestión de riesgos de la privacidad, estableciéndose la necesaria coordinación entre ambas atendiendo al resultado del análisis de riesgos y, en su caso, de las evaluaciones de impacto relativas a la protección de datos. En este sentido, deberá tenerse 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.

Asimismo, se informa sobre la necesidad de *aludir expresamente* en el citado artículo 4 —como principio susceptible de especial mención en materia de seguridad—, al relativo a la protección de los datos de carácter personal, por cuanto, si bien el texto que se informa, en su Artículo 15, se refiere a la *Protección de datos de carácter personal*, no lo hace vinculando las acciones necesarias en orden a la garantía y protección de la información al correspondiente “análisis de riesgos”, tal y como se infiere, entre otros, de los artículos, 24, 25, 32 y 35 del Reglamento General de Protección de Datos.

La anterior exigencia no es óbice para el mantenimiento de las previsiones contenidas en el artículo 15 del texto que se informa, si bien *resulta aconsejable que su apartado 1*, incorpore una referencia expresa al citado “análisis de riesgos”, al que no se alude con la exigible literalidad. En consecuencia, se propone la modificación del citado párrafo 1 del artículo 15, que podría señalar lo siguiente:

“Protección de datos de carácter personal.

1. La seguridad de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, constituye uno de los principios que deben regir su tratamiento, aplicándose para ello las medidas técnicas u organizativas apropiadas que garanticen un nivel de seguridad adecuado **en función del correspondiente análisis de riesgos, 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 la Ley Orgánica 3/2018, de 5 de diciembre. Dicho análisis de riesgos se realizará** teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.”

Asimismo, en relación con las previsiones contenidas en el artículo 15 del texto sometido a informe, se echa en falta la referencia específica a los *principios de protección de datos*, cuyo respeto, garantía y cumplimiento deberán guiar la actuación del Departamento en relación con su actividad con incidencia en la información personal de las personas afectadas. De tal suerte, se informa la necesidad de incorporar al borrador analizado un párrafo adicional en el que se contenga una mención específica a los referidos principios, de obligada observancia, en virtud de lo dispuesto por el artículo 5 del Reglamento general de protección de datos, cuando señala:

“Principios relativos al tratamiento

1. Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»); b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»); c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»); d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»); e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»); f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).

De acuerdo con lo anterior, el referido apartado, cuya adición se propone, debería referir —al menos— que:

“En el ámbito del Ministerio de Consumo, 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.**

Finalmente, según se observa, en el apartado 3 del artículo 15 del borrador, se advierte sobre la naturaleza y especialidad de determinados tratamientos de datos personales que, en su caso, deberán dar lugar a la realización de la “preceptiva *evaluación de impacto* relativa a la protección de datos”. Así, dicho apartado de la Orden menciona la posibilidad de realizar una “evaluación de impacto” cuando sea probable que un determinado tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.

De este modo, se recoge, 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, por lo que, *en este punto, no se propone* modificación alguna.

III

Dentro de la regulación de la estructura organizativa de la seguridad del departamento se determina que la misma estará compuesta por 1) La persona titular de la Subsecretaría de Consumo, 2) El Grupo de Trabajo de Seguridad de la Información del Departamento, 3) La persona designada como Responsable de Seguridad, 4) La persona designada como Responsable de los Sistemas, 5) Las personas designadas como Responsables de la Información y Responsables de los Servicios, 6) Las personas designadas como Delegado de Protección de Datos y Delegados de Protección de Datos de los organismos públicos adscritos al departamento, y 7) Las personas designadas como Administradores de Seguridad.

El análisis de las funciones atribuidas a cada elemento de la estructura organizativa conduce a aseverar que, en todo caso, independientemente de la situación que ocupe cada uno de los intervinientes en el tratamiento de los datos de carácter personal, todos deberán velar por que el mismo se ajuste a la normativa de protección de datos personales, tal y como señala el Considerando 78 del RGPD:

“La protección de los derechos y libertades de las personas físicas con respecto al tratamiento de datos personales exige la adopción de medidas técnicas y organizativas apropiadas con el fin de garantizar el cumplimiento de los requisitos del presente Reglamento. A fin de poder demostrar la conformidad con el presente Reglamento, el responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto. Dichas medidas podrían consistir, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo

a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad. Al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales para cumplir su función, ha de alentarse a los productores de los productos, servicios y aplicaciones a que tengan en cuenta el derecho a la protección de datos cuando desarrollan y diseñen estos productos, servicios y aplicaciones, y que se aseguren, con la debida atención al estado de la técnica, de que los responsables y los encargados del tratamiento están en condiciones de cumplir sus obligaciones en materia de protección de datos. Los principios de la protección de datos desde el diseño y por defecto también deben tenerse en cuenta en el contexto de los contratos públicos.”

En concreto, conviene detenerse en la regulación de la figura del Delegado de Protección de Datos en el ámbito de la Política de Seguridad de la Información del Ministerio, que se contiene en el artículo 13 del texto que se analiza.

A dichos efectos, no debe olvidarse que un papel fundamental dentro del nuevo modelo de responsabilidad activa establecido en el Reglamento general de Protección de Datos lo desempeña —precisamente— 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).

Pues bien, según se observa, en cuanto a la garantía de la independencia y la evitación de un posible conflicto de intereses de dicho Delegado, el párrafo 3 del artículo 13 prevé que “*Con carácter general*” no pueda coincidir en la misma persona la designación de Delegado con la del Responsable de Seguridad.

En este sentido, conviene matizar que, en el ámbito de la organización de la Política de Seguridad de la Información de un departamento ministerial, no tiene cabida la posible coincidencia en una misma persona de ambas designaciones y desempeño de funciones, por cuanto dicha posibilidad se encuentra justificada únicamente en aquellas organizaciones que, por su tamaño y/o recursos, no pudieran observar la debida separación de ambos nombramientos.

Así, tal y como se indicó en nuestro 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:

“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.

En resumen, la debida separación de funciones entre las personas designadas para uno u otro cargo (DPD y Responsables de Seguridad) debe quedar garantizada —*en todo caso*— en el ámbito organizativo del Ministerio, respetándose la separación de funciones señalada, sin que quepa la posibilidad de que ambos nombramientos recaigan en la misma persona. En consecuencia, debe procederse a la **supresión de la mención a “Con carácter general”** del artículo 13.3 del texto que se informa.

IV

No debe olvidarse que la inclusión del delegado de protección de datos dentro de la estructura organizativa vinculada con la seguridad de la información resulta esencial dentro del esquema establecido en el Reglamento general de protección de datos. 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 punto, conviene recordar que 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”.

En lo que al texto que se informa atañe, el artículo 8 del borrador se refiere a las funciones y composición del Grupo de Trabajo de Seguridad de la Información del Departamento, con labores de gestión, coordinación y supervisión en materia de seguridad de la información. Entre sus miembros componentes figuran diversos vocales, entre los que se encuentran las personas designadas como Delegado de Protección de Datos y como Delegados de Protección de Datos de los organismos públicos adscritos al departamento.

En este sentido, la función de asesoramiento del Delegado de Protección de Datos, así como la naturaleza de su figura —caracterizada por la autonomía e independencia de su actuación—, apuntan a la necesidad de que su participación en el citado “Grupo de Trabajo de Seguridad” tenga lugar únicamente en atención a la naturaleza de sus funciones de apoyo y asistencia.

En consecuencia, la garantía del eficaz desempeño de sus funciones exige que su participación en dicho Grupo se produzca únicamente *con voz, pero sin voto*, por cuanto el propio Delegado deberá velar por el control y cumplimiento por parte del responsable del tratamiento de las obligaciones establecidas por la normativa de protección de datos.

V

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. Así, en el punto II de este Informe, se refiere la necesidad de introducir las menciones necesarias en relación con la gestión de riesgos de manera expresa, y no por medio de una la simple remisión a su normativa general.

Y, por otra parte, se extrae que 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 esta y asesorar en su

diseño e implantación, en virtud de las funciones que el Reglamento General de Protección de Datos le otorga expresamente.

En definitiva, deberá procederse a las modificaciones apuntadas en el presente Informe para su debida adecuación a la normativa de protección de datos.