0004/2024

I

Tal y como dispone el artículo 1.1 del texto sometido a informe constituye su objeto la aprobación de la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Cultura, así como del marco organizativo y tecnológico de la misma.

El texto de la orden responde a la necesidad de adecuar la referida política a las exigencias derivadas de la entrada en vigor del nuevo Esquema Nacional de Seguridad, aprobado por Real Decreto 311/2022, de 3 de mayo, cuyo artículo 12.3 prevé que *"En la Administración General del Estado, cada ministerio contará con su política de seguridad, que aprobará la persona titular del Departamento"*, disponiéndose en el apartado 6 del propio artículo 12, que la política de seguridad se establecerá de acuerdo con los principios básicos señalados en el capítulo II y se desarrollará aplicando los requisitos mínimos que en dicho Esquema Nacional se contemplan.

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, conformando los diferentes niveles y responsabilidades de los diversos agentes implicados en su aplicación.

La nueva orden deroga la Orden CUD/1313/2019, de 27 de diciembre, por la que se aprueba la Política de Seguridad de la Información en el ámbito de la administración electrónica del Ministerio de Cultura y Deporte, que fue objeto de Informe 0086/2019, emitido por esta Agencia con carácter previo a su promulgación.

c. Jorge Juan 6
28001 Madrid

www.aepd.es

En lo que atañe a la protección de datos de carácter personal, el preámbulo de la norma dispone que *"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. La Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, tiene por objeto garantizar estos derechos de la ciudadanía y adaptar el ordenamiento jurídico español al 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)".* Dichas normas se citan igualmente en los artículos 3 y 4, relativos, respectivamente, al marco legal y regulatorio, y a los principios de la seguridad de la información.

De ahí que el artículo 4.1 d) establezca, dentro de los principios básicos de la seguridad de la información —siguiendo en este punto lo establecido en los artículos 5. b) y 7 del Esquema nacional de Seguridad (Real Decreto 311/2022, de 3 de mayo)—, el de gestión de riesgos, indicando que *"de acuerdo con lo establecido en la legislación vigente en materia de seguridad de la información y protección de datos personales, 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 establecerán 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."*

Por su parte, en el artículo 17 del proyecto se desarrolla la metodología de dicho proceso de gestión —con pleno sometimiento a la normativa de protección de datos—, así como la asignación de tareas entre los diferentes responsables del proceso.

Asimismo, en el artículo 4.2 de la orden se configura como principio y objetivo de seguridad el de *protección de datos de carácter personal*, indicando que:

> (…)
> *"q) "se adoptarán las medidas técnicas y organizativas destinadas a garantizar una adecuada protección de los datos. Tal y como se establece en la legislación vigente en materia de protección de datos personales, dichas medidas deberán ser apropiadas en función del análisis de riesgos mencionado en el apartado 4.1 d) del presente artículo, 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.*

c. Jorge Juan 6
28001 Madrid

r) se adoptarán las medidas técnicas, organizativas y procedimentales necesarias para garantizar el cumplimiento de la legislación vigente en materia de seguridad de la información, protección de datos personales, así como de la legislación especial que afecte al ámbito de actuación de la organización (…)"

Dentro de la regulación de la estructura organizativa del departamento —*ex artículo 5*— se determina que la misma estará compuesta, además de por la citada Comisión Ministerial de Administración Digital, por el responsable de seguridad, el responsable de la información, los responsables del servicio y los responsables del sistema, así como por el Delegado de Protección de Datos, el Grupo de trabajo de Delegados de Protección de Datos, y el Comité de Crisis.

En cuanto al Delegado de Protección de Datos y al Grupo de Trabajo de Delegados de Protección de Datos, su naturaleza y funciones, se regulan —respectivamente— en los artículos 11, 12 y 15 del proyecto de orden. Se prevé así, incluso, la existencia de un Grupo de Trabajo de Delegados de Protección de Datos —artículo 12— cuya misión consiste en asesorar y supervisar el cumplimiento de la normativa de protección de datos personales tratados por el Ministerio consultante.

En los artículos 11.3 y 15.5 se dispone que la *designación* del Delegado se efectuará de conformidad con lo dispuesto por la legislación vigente en materia de protección de datos, lo que debe interpretarse como una remisión a la regulación del artículo 37 del RGPD y del artículo 34 de la Ley Orgánica 3/2018, de 5 de diciembre.

En consecuencia, dichos delegados deberán ser 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 tiene encomendadas.

Por su parte, las funciones de los Delegados se enuncian en el artículo 11 del proyecto de orden. La enumeración de estas coincide con las detalladas en la Sección 4 del Capítulo IV del Reglamento General de Protección de Datos y en el Capítulo III del Título V de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

II

c. Jorge Juan 6
28001 Madrid
www.aepd.es

El artículo 13, lleva por rúbrica protección de datos de carácter personal, estableciendo que *"Se aplicarán a los datos personales que sean objeto de tratamiento por parte del Ministerio de Cultura, las medidas de seguridad apropiadas derivadas del análisis de riesgos, así como de las evaluaciones de impacto relativas a la protección de datos, conforme se detalla en la legislación vigente en materia de protección de datos de carácter personal. Además, se aplicarán las medidas correspondientes al Anexo II del Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. En caso de conflicto entre medidas de seguridad provenientes las legislaciones y normativas aplicables, prevalecerán, las mayores exigencias derivadas de la ley de mayor rango."*

Pues bien, respecto de la anterior previsión, tal y como se viene señalando en los informes emitidos por esta Agencia —por todos el **Informe** 170/2018, de 12 de noviembre de 2018—, debe recordarse que, sin perjuicio de la aplicación de las exigencias derivadas de cualquier norma de mayor rango, en el caso de que el análisis de riesgos determine la necesidad de medidas agravadas respecto a la normativa recogida en el Anexo II del Esquema Nacional de Seguridad, **siempre deberán implementarse las medidas derivadas del análisis de riesgos en materia de protección de datos personales.**

A saber:

> *"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.*

c. Jorge Juan 6
28001 Madrid

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)".

c. Jorge Juan 6
28001 Madrid

(…)

En síntesis, tal y como ha venido informando esta Agencia, 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 tanto, **se estima conveniente que en el artículo 13 de la orden se haga igualmente una referencia al análisis de riesgos derivado del artículo 24 del RGPD, así como a su necesaria observancia, sin que resulte suficiente la mención del artículo 17.8, cuando señala que:**

> *"Los análisis de riesgos, desde un enfoque de privacidad, se realizarán según lo establecido en la normativa vigente en materia de protección de datos personales, debiéndose seguir también las indicaciones de la Agencia Española de Protección de Datos y demás autoridades competentes al respecto."*

III

Por lo demás, según se advierte, el texto que se informa considera la evolución de las políticas de seguridad de la información desde un modelo de lista de cumplimiento a otro de análisis de riesgo y de impacto en la protección de datos (responsabilidad proactiva, art. 5.2 RGPD), quedando dicho enfoque claramente plasmado en el texto que se informa, con estricta observancia de los artículos 24 y 32.1 del RGPD, y en consonancia con las previsiones de su considerando 75.

La determinación de las diferentes funciones asignadas en los artículos 5 —referido a la estructura organizativa—, 11 y 12 de la orden, respeta el esencial conocimiento que el Delegado de Protección de Datos debe poseer de la política de seguridad de la información, participando en su asesoramiento e implantación en virtud de las funciones que el reglamento general de Protección de Datos le otorga expresamente.

A su vez, en relación con la *compatibilidad funcional del delegado de protección de datos del RGPD y el responsable de seguridad* del Esquema Nacional de Seguridad, tal y como se indicó en el **Informe 170/2018**, **la orden deslinda claramente los ámbitos de actuación de ambas figuras.**

c. Jorge Juan 6
28001 Madrid
www.aepd.es

Por otro lado, 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 tienen atribuidas dentro de la estructura del responsable, siendo especialmente relevantes a estos efectos los distintos sujetos enumerados en los artículos 6 a 10 del Proyecto y, particularmente, el responsable de seguridad.

La función del delegado de protección de datos es 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 articulado del texto que se informa atañe, las funciones atribuidas al delegado encajan claramente en su función de asesoramiento y consulta, así como en el ámbito de sus relaciones con *(i)* el resto de órganos del responsable, *(ii)* los sujetos afectados por los tratamientos, y *(iii)* las Administraciones públicas competentes, participando únicamente en calidad de "invitado" en las reuniones del denominado "Grupo técnico de seguridad de la información", encuadrado en el ámbito propio de actuación del Responsable de Seguridad —*ex artículo 7 del proyecto de orden*—.

La función de asesoramiento del Delegado de Protección de Datos, así como la naturaleza de su figura —caracterizada por la autonomía e

c. Jorge Juan 6
28001 Madrid
www.aepd.es

independencia de su actuación—, apuntan a la necesidad de que su participación en el citado “Grupo” tenga lugar únicamente en atención a la naturaleza de sus funciones de apoyo y asistencia. 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.

c. Jorge Juan 6
28001 Madrid