INFORME DE LA COMISIÓN CONSULTIVA DE LA TRANSPARENCIA Y LA PROTECCIÓN DE DATOS AL BORRADOR DE LA ORDEN POR LA QUE SE MODIFICA LA DE DE 12 DE JULIO DE 2019, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN EL ÁMBITO DE LA CONSEJERÍA Y DE SUS ENTIDADES ADSCRITAS

Se ha recibido, con fecha 23 de septiembre de 2021, procedente de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades, solicitud de informe del PROYECTO DE ORDEN POR LA QUE SE MODIFICA LA DE 12 DE JULIO DE 2019, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES EN EL ÁMBITO DE LA CONSEJERÍA Y DE SUS ENTIDADES ADSCRITAS**,** de acuerdo con lo previsto en el artículo 15.1 d) del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía.

Se acompaña la siguiente documentación:

* Proyecto de Orden.

* Acuerdo de Inicio, así como Memorias Justificativa y de principios de buena regulación.

Por esta Comisión Consultiva se ha examinado el texto remitido cuyo objeto lo constituye (artículo 1.1.): *La Modificación de la Orden del Consejero de Economía, Conocimiento, Empresas y Universidad de 12 de julio de 2019, por la que se establece la política de seguridad de las tecnologías de la información y comunicaciones en el ámbito de la Consejería y de sus entidades adscritas.*

Con carácter previo, se advierte de que este informe se ocupa exclusivamente de aquellas cuestiones que, tras el análisis del texto de la norma proyectada, afectan, a juicio de la Comisión, a materias relacionadas directamente (o por conexión o consecuencia) con la transparencia pública y la protección de datos. Por tanto, dado que sería excederse en nuestro cometido, no se realizan consideraciones sobre otros aspectos generales o mejoras de técnica normativa, que serán informados por los órganos correspondientes.

Sentado lo anterior, examinado el texto del Proyecto de Orden se realizan las siguientes observaciones a su articulado.

En materia de transparencia pública.

Única. se recuerda la necesidad de cumplir con las obligaciones de publicidad activa que pudiera tener como órgano colegiado, según la normativa que les resulte de aplicación.

En materia de protección de datos personales

- OBSERVACIÓN 1 (General)

Aparece 7 veces a lo largo del texto la expresión "*datos de carácter personal".*

La expresión actualmente utilizada en la normativa vigente sobre la materia habla de 'datos personales' en vez de 'datos de carácter personal', que sí era la utilizada en la anterior normativa. Así, el propio Reglamento General de Protección de Datos (RGPD), lo que define en su artículo 4.1) son los "*datos personales*".

Se sugiere, por lo tanto, la sustitución en el texto de la expresión mencionada (datos de carácter personal) por la que es más acorde con la normativa vigente en la materia (datos personales).

- OBSERVACIÓN 2 (Mdf. Artículo 2, pg. 3)

En el apartado a) se indica:

"En la Consejería de Transformación Económica, Industria, Conocimiento y Universidades:
1.º Comité de Seguridad Interior y Seguridad TIC.
2.º Las personas responsables de la información.
3.º Las personas responsables del servicio.
4.º La Unidad de Seguridad TIC.
5.º La Unidad de Seguridad Interior.
6.º La persona responsable de seguridad TIC.
7.º Las personas responsables del sistema.
Además, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal, deberán existir las siguientes figuras que ostentan funciones directamente relacionadas con la seguridad TIC:
1. La persona delegada de protección de datos.
2. La persona responsable del tratamiento de datos de carácter personal.
3. La persona encargada del tratamiento de datos de carácter personal."

En este caso, la aplicación de lo que puede entenderse como un buen uso del lenguaje de género podría suponer un alejamiento del verdadero alcance que se recoge en el Reglamento general de protección de Datos y en la LOPDGDD en relación con el Delegado de Protección de Datos, donde el vocablo “Delegado” se entiende como referido a la “figura de Delegado” y no a una persona física concreta, dado que, podría tratarse de una o varias personas físicas que desarrollen su labor formando parte de la organización del responsable o encargado, sin que se concrete ese grupo de trabajo como una persona jurídica, o bien a través de un contrato de servicios, pudiendo tratarse también de una persona jurídica.

Es por ello, por lo que se sugiere la expresión utilizada en la normativa: “*Delegado de protección de datos*", dado que en el párrafo citado del proyecto se está haciendo referencia a las figuras que contempla la normativa de protección de datos, y con independencia de que el artículo 43 de la Orden objeto de modificación indica expresamente que la mencionada figura del delegado de protección de datos será asumida por una persona funcionaria.

En relación con las figuras de los responsables y los encargados del tratamiento, efectivamente, podría hablarse de personas puesto que podrían ser personas físicas o jurídicas, pero el RGPD no solo habla de esos términos, sino además, de “*autoridad pública, servicio u otro organismo*”, por lo que la expresión utilizada podría reflejar lo que establece la propia normativa. Además, el término ‘personas’ podrían inducir a error al ser también utilizado en la primera parte del apartado refiriéndose a “*responsables de la información”, “responsables del servicio”, “responsables de seguridad TIC” y “responsables del sistema”*, cuando en este caso, parece referirse solo a personas físicas.

Es por esto por lo que se sugiere que la parte final del apartado se redacte de la siguiente forma:

> *“Además, de conformidad con lo establecido en la normativa sobre protección de datos personales, deberán existir, ostentando funciones directamente relacionadas con la seguridad TIC:*
> *1. La figura del delegado de protección de datos.*
> *2. La figura del responsable del tratamiento.*
> *3. La figura del encargado del tratamiento.”*

En los puntos 2 y 3 se ha obviado indicar “de datos personales”, porque va implícito en la introducción.

O, directamente:

"Además, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal, deberán existir las siguientes figuras que ostentan funciones directamente relacionadas con la seguridad TIC:
1. El delegado de protección de datos.
2. El responsable del tratamiento.
3. El encargado del tratamiento."

En todos los casos, se hace notar que la existencia de la figura del encargado del tratamiento no es de existencia obligatoria de acuerdo con la normativa, si bien en el caso de la entidad que nos ocupa, dicha existencia está prácticamente asegurada.

Así, en general a lo largo del texto, cuando se realice una referencia a la figura genérica del delegado de protección de datos, no se considera adecuado, por lo expresado anteriormente, anteponerle las palabras 'la persona', cuestión que no ocurre cuando se haga referencia a un delegado de protección de datos concreto que, por las circunstancias que fueren, si conste que deba ser desempeñado por una persona física.

- OBSERVACIÓN 3 (Mdf. Artículo 7)

En el apartado 2 se establece lo siguiente:

"2. Las unidades organizativas, entendiéndose por tal órganos y unidades administrativas, deben cumplir los requisitos mínimos de seguridad exigidos en el Esquema Nacional de Seguridad (en adelante, ENS) y por la legislación de protección de datos de carácter personal. En concreto, en lo que respecta al ENS, los requisitos mínimos son los siguientes:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
[...]"

Se hace una referencia a unos *"...requisitos mínimos de seguridad exigidos en el Esquema Nacional de Seguridad (en adelante, ENS) y por la legislación de protección de datos..."* .

Se detallan posteriormente requisitos referidos al ENS, pero no se dice nada respecto de protección de datos, con lo que quedaría incompleto el desarrollo del enunciado.

Se sugiere la eliminación de la referencia a la legislación de protección de datos en el párrafo expuesto, o bien que se concreten cuáles serían esos 'requisitos mínimos'.

Cuestión distinta es que pudiera hacerse una adecuada referencia a la Disposición adicional primera de la LOPDGDD relativa a las "Medidas de seguridad en el ámbito del sector público", que a su vez remite al cumplimiento de lo establecido en el ENS.

- OBSERVACIÓN 4.1 (Mdf. Artículo primero 12.2)

Se plantea la modificación del artículo 12.2 de la mencionada Orden. Al respecto, tras la diferenciación de tres bloques de responsabilidad, se indica lo siguiente:

"En este sentido, los distintos bloques de responsabilidad mencionados quedarán distribuidos convenientemente, conforme a lo estipulado en el artículo siguiente, sobre los distintos agentes integrantes de la siguiente estructura organizativa en dos niveles:"

Analizado el artículo siguiente contenido en la Orden objeto de modificación, se constata que éste, tras la nueva redacción propuesta, versa sobre la creación del Comité de Seguridad Interior y Seguridad TIC de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades.

Teniendo en cuenta el contenido del artículo 13 en su nueva redacción, no se identifica en el mismo la distribución de responsabilidad aludida en el inciso transcrito.

Por consiguiente, se sugiere la modificación del precepto en ese punto.

- OBSERVACIÓN 4.2 (Mdf. Artículo primero 12.2)

Con respecto a la estructura organizativa dispuesta se identifica que en el nivel 1), relativo a la Consejería de Transformación Económica, Industria, Conocimiento y Universidades, se inserta una mención al Delegado de Protección de Datos en los siguientes términos:

Además, de conformidad con lo establecido en la normativa sobre protección de datos de carácter personal, deberán existir las siguientes figuras que ostentan funciones directamente relacionadas
con la seguridad TIC:

- 1. La persona delegada de protección de datos.
- 2. La persona responsable del tratamiento de datos de carácter personal.
- 3. La persona encargada del tratamiento de datos de carácter personal.

A este respecto, y toda vez que la mención se inserta en un precepto que versa sobre la distribución de bloques de responsabilidad, se estima que situar al DPD al nivel del Responsable y el Encargado del tratamiento podría inducir a error en relación a los cometidos funcionales y a la responsabilidad del DPD en el seno de la organización, por lo que se aconseja aclarar este particular.

- OBSERVACIÓN 4.3 (Modf. Artículo primero 12.2)

El precepto identifica un segundo nivel de responsabilidad en cada una de las entidades vinculadas o dependientes, disponiéndose una estructura organizativa algo distinta a la contemplada para la Consejería.

En relación a esta estructura organizativa, se detecta que de nuevo se cita al DPD y que ahora se hace al mismo nivel que el Comité de seguridad interior y seguridad TIC, la persona responsable de la seguridad TIC o las personas responsables del sistema.

A este respecto, de nuevo se aconseja evitar la confusión que el precepto podría provocar en relación al régimen funcional y de responsabilidad del DPD.

- OBSERVACIÓN 5 (Mdf. Artículo 14)

En el apartado 1.d) se establece lo siguiente en relación con el Comité de Seguridad Interior TIC de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades:

> *"La secretaría será ejercida por la persona titular de la Jefatura del Servicio de Informática, con voz y voto."*

La presente observación va dirigida simplemente a señalar si se ha tenido en cuenta que la mencionada Jefatura, a diferencia de cuando se aprobó la Orden ahora modificada, ya no pertenece a la Consejería, y por lo tanto, se está manteniendo la secretaría del "Comité de Seguridad Interior y Seguridad TIC", con voz y voto, y participando de todas las funciones de dicho Comité, en una persona externa a la Consejería, sin que ese apartado sea objeto de modificación.

- OBSERVACIÓN 5.1 (Mdf. Artículo 14.2)

El apartado primero del artículo 12 de la Orden alude a la composición del Comité de Seguridad Interior y Seguridad TIC de la Consejería, no previendo que el DPD, en su condición de tal, forme parte de dicho Comité.

No obstante, el apartado segundo reza de la siguiente manera:

"La persona delegada de protección de datos y las personas responsables de seguridad interior y seguridad TIC, en el caso de que no formen parte del Comité como vocales o ejerciendo la secretaría, asistirán en calidad de personas asesoras a las reuniones del Comité de Seguridad Interior y Seguridad TIC, salvo que puntualmente se disponga lo contrario de forma expresa por parte de la presidencia".

Al respecto, se detecta una aparente discrepancia entre dicha disposición y la composición prevista del Comité en el apartado primero, ya que cuando dicha composición no alude al DPD entre los integrantes de las vocalías y quien debe ostentar la función de secretario/a del órgano, el apartado segundo sí parece reconocer tal posibilidad.

En consecuencia, se sugiere la disposición de una redacción que evite esta aparente incongruencia.

- OBSERVACIÓN 5.2 (Mdf. Artículo 14.2)

Al margen de lo anterior, y para el supuesto en que el precepto transcrito partiera de la premisa de que la función de DPD pudiera ser ejercida por las personas que tienen asignada la condición de vocales ((i) la persona titular de cada uno de los órganos directivos centrales de la Consejería de Transformación Económica, Industria, Conocimiento y Universidades que tengan responsabilidad sobre algún sistema de información y (ii) La persona titular de la Coordinación General de la Secretaría General Técnica), o por quien tiene encomendada la secretaría del órgano (la persona titular de la Jefatura del Servicio de Informática), debe señalarse que en tales casos podría incurrirse en supuestos de conflicto de intereses que resultan vetados por el RGPD.

En concreto, el art. 38.6 del RGPD prevé que "El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses".

- OBSERVACIÓN 6 (Mdf. Artículo 39)

Se sugiere la modificación del artículo 39 de la Orden toda vez que el apartado primero del precepto indica que "En dicho ámbito cada responsable del tratamiento de datos de carácter personal aplicará las medidas técnicas y organizativas apropiadas a fin de garantizar y ser capaz de demostrar que los tratamientos de datos de carácter personal son conformes con dicha normativa, de acuerdo con el principio de responsabilidad proactiva, de conformidad con el artículo 24 del RGPD" y el apartado tercero indica que *"las personas responsables del tratamiento y encargadas del tratamiento en el ámbito de aplicación de esta orden,*

aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo".

Se estima que las menciones, al no resultar idénticas, podrían provocar confusión en relación a quién es el sujeto obligado a aplicar las medidas técnicas y organizativas exigidas por el RGPD.

- OBSERVACIÓN 7 (Mdf. Artículo 41)

En este apartado se propone la redacción:

> *"1. La persona responsable del tratamiento llevará un registro de las actividades de tratamiento de datos de carácter personal efectuadas bajo su responsabilidad, de acuerdo con lo establecido en el artículo 31 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y el resto de normativa de datos de carácter personal aplicable. Este registro deberá publicarse y mantenerse actualizado en el inventario de actividades de tratamiento de datos de la Junta de Andalucía."*

En relación con "la persona responsable del tratamiento" ya se han realizado observaciones.

Por otra parte, es necesario señalar que la normativa de protección de datos personales no exige la publicación del registro como indica el párrafo anterior (*"[e]ste registro deberá publicarse..."*), sino que, el artículo 31 LOPDGDD habla de la publicación del inventario de las actividades de tratamiento incluyendo la información indicada en el artículo 30 RGPD y su base legal.

Hay que tener en cuenta que el registro de actividades de tratamiento puede contener determinada información (más allá del a establecida en el artículo 31.1 RGPD) que no deba ser difundida externamente, si bien, siempre estaría a disposición de la autoridad de control (artículo 30.4 RGPD).

Se sugiere una redacción más adecuada del párrafo señalado que no dé lugar a posibles interpretaciones incorrectas.

- OBSERVACIÓN 8 (Artículo 43.1)

El artículo 43.1 de la Orden prevé que "*La figura de la persona delegada de protección de datos, en los términos establecidos en el RGPD, será asumida por una persona funcionaria del grupo A1 perteneciente a la Consejería de Economía, Conocimiento, Empresas y Universidad, que deberá tener un perfil jurídico especializado, y reconocida competencia en materia de protección de datos, de*

conformidad con lo establecido en los artículos 37 y 38 del RGPD y los artículos 34 y 35 de la Ley Orgánica 3/2018, de 5 de diciembre ”.

Al respecto, procede significar que ni el RGPD ni la LOPDGDD ni la normativa reguladora de la función pública de la Junta de Andalucía requiere que las funciones del DPD sean ejercidas por una persona funcionaria de carrera.

Sin perjuicio de lo expresado en el párrafo anterior, el Departamento promotor de esta regulación puede en su ámbito regulatorio optar por esta solución.

- OBSERVACIÓN 9 (Mdf. Artículo 46)

En este apartado se propone la redacción:

> *“1. De conformidad con el artículo 33 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, cuando se vayan a tratar datos de carácter personal por cuenta de un responsable, este elegirá únicamente los encargados del tratamiento que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, y garantice la protección de los derechos de las personas interesadas. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico constará por escrito, inclusive en formato electrónico.”*

En este caso se ha suprimido la referencia al artículo 28 RGPD, pero manteniendo e incluso añadiendo contenidos que replican lo expresado en dicho artículo, pero ahora, remitiéndose al artículo 33 LOPDGDD que en realidad no menciona lo que indica el párrafo señalado.

Se sugiere revisar adecuadamente la redacción, referenciando adecuadamente la normativa y sin realizar una innecesaria adaptación de lo que ya se expresa en la misma, lo que podría dar lugar a equívocos en su aplicación.

El secretario de la Comisión
Consta la firna
Amador Martínez Herrera

VºBº El presidente de la Comisión
Consta la firma
Jesús Jiménez López