Consejo de Transparencia y Protección de Datos de Andalucía

PROPUESTA DE INFORME DE LA COMISIÓN CONSULTIVA DE LA TRANSPARENCIA Y LA PROTECCIÓN DE DATOS AL PROYECTO DE ORDEN POR LA QUE SE MODIFICA LA ORDEN DE LA CONSEJERÍA DE HACIENDA, INDUSTRIA Y ENERGÍA DE 21 DE OCTUBRE DE 2019, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONSEJERÍA

Se ha recibido de la Consejería de Hacienda y Financiación Europea, el documento "PROYECTO DE ORDEN POR LA QUE SE MODIFICA LA ORDEN DE LA CONSEJERÍA DE HACIENDA, INDUSTRIA Y ENERGÍA DE 21 DE OCTUBRE DE 2019, POR LA QUE SE ESTABLECE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA CONSEJERÍA" para emisión de Informe preceptivo por esta Comisión Consultiva de Transparencia y Protección de datos de Andalucía, de acuerdo con lo previsto en el Artículo 15.1.d) de los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre, y en el artículo 57.1.c) 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 por el que se deroga la Directiva 95/46/CE.

Con la petición de informe se acompaña la siguiente documentación:

- Borrador del proyecto de Orden.
- Memoria justificativa sobre la necesidad y oportunidad de fecha 23 de febrero de 2022.
- Memoria económica de fecha 23 de febrero de 2022.
- Memoria justificativa sobre la adecuación a los principios de buena regulación de fecha 23 de febrero de 2022.
- Resto de documentación preceptiva.

Con carácter previo, se advierte de que este informe se refiere 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 personales. 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 en cada caso competentes.

Examinado el documento recibido, procede realizar las siguientes observaciones a su articulado:

1 En materia de transparencia.

En materia de transparencia, la normativa a la que ha de ajustarse el proyecto sometido a consulta es la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía (LTPA), la Ley 19/ 2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno (LTBG) y los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre, sin perjuicio de cualquier otra norma aplicable que pueda ser citada por su relación con cuestiones concretas en el presente documento.

1.1 Consideraciones generales

A la vista del contenido del Proyecto, no se realizan consideraciones desde el Área de Transparencia. Únicamente se recuerda la necesidad de publicar la información incluida en las obligaciones de publicidad activa contenidas en el Título II de la LTPA en los términos y condiciones establecidas.

2. En materia de protección de datos personales.

En materia de protección de datos personales, la normativa a la que ha de ajustarse el proyecto sometido a consulta es 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, en adelante RGPD); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los

derechos digitales (en adelante LOPDGDD); la Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía; los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre; sin perjuicio de cualquier otra norma aplicable que pueda ser citada por su relación con cuestiones concretas en el presente documento.

2.1 Artículo 6 (Modificación del artículo 5 de la Orden de la Consejería de Hacienda, Industria y Energía, de 21 de octubre de 2019, por la que se establece la política de seguridad de la información de la Consejería)

En el apartado 2 del artículo 5 objeto de modificación, quedaría redactado, según el proyecto de Orden, como sigue:

"*Además, en el ámbito de la Consejería, y de acuerdo con lo establecido en la normativa sobre protección de datos personales, deberán existir los siguientes perfiles:*

a) El Delegado de Protección de Datos.

b) Responsables del Tratamiento.

c) Encargados del Tratamiento.".

En este caso, la expresión '*deberán existir los siguientes perfiles*' quizás no sea muy correcta, ya que esas figuras tienen una existencia propia e independiente de la existencia o no de Política de Seguridad en la Consejería.

Por otra parte, 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.

En cualquier caso, de querer incluir estas importantes figuras en la norma que regule la política de seguridad, se considera más adecuado, en vez de utilizar la expresión "... *deberán existir los siguientes perfiles:*", utilizar la frase, "*...deberán contemplarse/tenerse en cuenta las siguientes figuras:*", o similar, entendiendo además que es más correcta emplear la palabra 'figura' que la palabra 'perfil'.

2.2 Artículo 7 (**Modificación del artículo 6 de la Orden de la Consejería de Hacienda, Industria y Energía, de 21 de octubre de 2019, por la que se establece la política de seguridad de la información de la Consejería)**

A)

En el apartado 1 del artículo 6 objeto de modificación, quedaría redactado, según el proyecto de Orden, como sigue:

"*1. La Consejería contará con un Comité de Seguridad Interior y Seguridad TIC como órgano de los regulados en el artículo 10 del Decreto 1/2011, de 11 de enero, para la dirección y seguimiento en materia de seguridad de la información y de los activos TIC, y tratamiento de datos personales de los que la Consejería sea titular o cuya gestión tenga encomendada. Asimismo, y de acuerdo con lo dispuesto en el artículo 9 del Decreto 171/2020, de 13 de octubre, le corresponderá la dirección y el seguimiento en materia de seguridad interior*".

Es de entender que la expresión "sea titular" pretende hacer referencia, dado que se está hablando del tratamiento de datos personales, a la responsabilidad sobre dichos tratamiento; es esta última, 'responsabilidad', la palabra que el RGPD reserva para aquellos que determinan los fines y medios del tratamiento [art. 4.7) RGPD] , por lo que se considera más adecuado utilizar dicha expresión. Así, el párrafo podría quedar redactado:

"*1. La Consejería contará con un Comité de Seguridad Interior y Seguridad TIC como órgano de los regulados en el artículo 10 del Decreto 1/2011, de 11 de enero, para la dirección y seguimiento en materia de seguridad de la información y de los activos TIC, y tratamiento de datos personales de los que la Consejería sea titular**, a través del correspondiente responsable del tratamiento,** o cuya gestión tenga encomendada. Asimismo, y de acuerdo con lo dispuesto en el artículo 9 del Decreto 171/2020, de 13 de octubre, le corresponderá la dirección y el seguimiento en materia de seguridad interior*".

B)

En relación con el párrafo anterior y en lo que al tratamiento de datos personales se refiere, la lectura del mismo, centrado en este aspecto sería:

"*1. La Consejería contará con un Comité de Seguridad Interior y Seguridad TIC [...]* ***para la dirección y seguimiento*** *en materia de seguridad de la información y de los activos TIC, y* ***tratamiento de datos personales*** *de los que la Consejería sea titular* ***[...]***".

La redacción no deja muy clara la relación del Comité con los datos personales: ¿su tratamiento?, ¿su dirección y seguimiento? ¿puede que le falta un 'del', y la redacción correcta sea '...y **del** tratamiento de datos personales...'.

Con la redacción actual se estima que no queda clara la relación o competencia del Comité en relación con el tratamiento de datos personales.

C)

Por otra parte, al indicarse en el apartado 2 del artículo 6 objeto de modificación, la composición del Comité de Seguridad Interior y Seguridad TIC de la Consejería, en su letra d), como miembro de dicho Comité se establece:

"d) Secretaría: la persona responsable de los sistemas TIC de la Agencia Digital de Andalucía que se ocupe de los sistemas de la Consejería."

La definición de las características de la persona mencionada es excesivamente genérica, toda vez que no se determina un puesto de trabajo concreto ni siquiera un nivel mínimo del que deba disponer.

El resto de miembros del Comité están claramente determinados: la persona titular de la Viceconsejería, la persona titular de la Secretaría General Técnica, o las personas titulares de cada uno de los órganos directivos centrales; es más, cuando se habla, en el apartado 3 de cómo actuar en el caso de vacante, ausencia o enfermedad, se indica que la Secretaría deberá ser sustituida por personal que ocupe puestos de trabajo de nivel 28 o superior, lo que parece que hace más necesario categorizar de alguna manera en relación a las características del puesto a quien ocupe la titularidad de la Secretaría.

D)

En relación al apartado 8 del artículo 6 proyectado, se observa que éste dispone lo siguiente:

> "*El Comité se reunirá de forma ordinaria al menos una vez al año. También podrá celebrar reuniones extraordinarias, adicionales a las ordinarias, si se produjeran incidentes de seguridad graves o se produjeran conflictos que pudieran afectar gravemente a los servicios prestados por la Consejería. La evaluación de la gravedad para convocar una reunión extraordinaria la realizará la persona titular de la Vicepresidencia del Comité, que lo someterá a la Presidencia del mismo. Todas las reuniones se realizarán previa convocatoria y de las mismas se levantará acta*".

Con respecto a dicha disposición, se sugiere que la reunión del Comité en supuestos de incidentes de seguridad grave o que puedan afectar gravemente a los servicios prestados por la Consejería, no sea estrictamente potestativa sino obligatoria; en particular cuando se esté ante brechas de datos personales, en los supuestos previstos en los artículos 33 y 34 del RGPD.

E)

En el apartado 10 del artículo 6 objeto de modificación, se detallan las funciones del Comité de Seguridad Interior y Seguridad TIC.

En el apartado i) se indica que es competencia del comité "*supervisar el nivel de riesgo y supervisar la toma de decisiones en la respuesta a incidentes de seguridad que afecten a la información y/o a los activos TIC*".

Se considera adecuado añadir en este punto la determinación de cuándo un incidente se seguridad puede considerarse, de acuerdo con lo requerido por la normativa de protección de datos como una 'brecha de seguridad' que se deba notificar a la autoridad de control en el plazo establecido para ello. Podría añadirse una frase como esta: "*. Determinar cuándo un incidente de seguridad ha de ser considerado como una brecha de seguridad en materia de protección de datos a los efectos de su notificación a la autoridad de control en dicha materia en el plazo establecido por la mencionada normativa.*", o similar.

Por otra parte, en el apartado m) se menciona el impulso de análisis de riesgos y en el p) se hace referencia a la coordinación de medidas técnicas y organizativas que puedan llevarse a cabo tras los análisis de riesgos o, en su caso, de las evaluaciones de impacto en la protección de datos.

No obstante, el impulso a la realización de estas últimas no figura entre las competencias del Comité. Se sugiere por tanto, incluir una función que incluya la competencia relativa al análisis de si un tratamiento previsto necesita la realización de una previa evaluación de impacto sobre la protección de datos, y el impulso para la realización de la misma o, por contra, justificar la no necesidad de dicha evaluación.

F)

Con respecto al artículo 6, se constata que el apartado 11 de dicho precepto prevé que "En el ámbito de la Seguridad Interior, el Comité de Seguridad Interior y Seguridad TIC" tendrá asignada, entre otras, la función de "*Analizar y adoptar decisiones para la prevención o para la respuesta a incidentes susceptibles de generar una crisis de seguridad en la Consejería*".

Partiendo de esta disposición, debe tenerse presente que el RGPD define, de un modo amplio, las "brechas de datos personales" como "*todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos*" y, con respecto a ellas, los artículos 33 y 34 establecen obligaciones de notificación a la autoridad de control y de comunicación a las personas afectadas cuando concurran las circunstancias que prevén tales preceptos.

Al respecto, procede significar que no tienen consideración de brecha de datos personales sujetas a los artículos 33 y 34 del RGPD aquellos incidentes que:

- No afecten a datos personales, es decir, a datos que no sean de personas físicas identificadas o identificables.

- No afecten a tratamientos de datos personales llevados a cabo por un responsable o un encargado.

• Ocurran en tratamientos llevados a cabo por una persona física en el ámbito doméstico.

Por lo tanto, no todos los incidentes de seguridad son necesariamente brechas de datos personales y no solo los ciberincidentes pueden ser brechas de datos personales.

A su vez, no toda acción que suponga una vulneración de la normativa de protección de datos puede ser considerada una brecha de datos personales.

Siendo esto así se sugiere que la norma proyectada identifique de forma explícita a quién corresponde la detección de este tipo de incidentes, su clasificación como brecha de datos personales, su gestión en sentido amplio concretando también los procedimientos y los medios que hayan de disponerse; su notificación a la autoridad de control y su comunicación a las personas afectadas, en su caso. Todo ello, teniendo en cuenta además las funciones y responsabilidades de las figuras implicadas en tales labores de gestión, a saber, el responsable o corresponsables del tratamiento, el encargado de tratamiento y el delegado de protección de datos.

2.3 Artículo 17 (Modificación del artículo 23 de la Orden de la Consejería de Hacienda, Industria y Energía, de 21 de octubre de 2019, por la que se establece la política de seguridad de la información de la Consejería)

En relación a la redacción proyectada del artículo 23.1 y, en concreto, su inciso final relativo al establecimiento de "*procedimientos de actuación para la reacción ante incidentes de seguridad*", se reitera la observación anterior al apartado 11 del artículo 6, dándose por íntegramente reproducida en este punto al objeto de evitar innecesarias reiteraciones.

El secretario de la Comisión
Consta la firma
Amador Martínez Herrera

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