Fecha: 18 de septiembre de 2024

DICTAMEN 4/2024

Relativo a la gestión de las notificaciones y comunicaciones de brechas de datos personales en escenarios de múltiples responsables de tratamientos del sector público andaluz con un encargado común.

1. Objeto del dictamen.

El presente dictamen se emite en virtud del poder consultivo que el artículo 58.3 b) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016 (en adelante RGPD), le confiere a este Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo), en su condición de autoridad independiente de control en materia de protección de datos.

Su objeto lo constituye el análisis de la viabilidad, en el marco del RGPD, de que un encargado del tratamiento efectúe la notificación al Consejo de una violación de la seguridad de los datos personales (en adelante brecha de datos personales, salvo reproducción literal de preceptos legales) y, en su caso, la comunicación a los afectados, en nombre de una pluralidad de responsables de tratamientos del sector público andaluz afectados por la misma brecha.

Asimismo, el dictamen identifica las condiciones que, en el supuesto planteado, deberían exigirse por los responsables de los tratamientos al encargado, a la vez que se efectúan determinadas observaciones sobre el procedimiento y el encargo de tratamiento que debería regular esta forma de operar.

2. Sobre la consulta.

Se dirige al Consejo consulta realizada por una entidad instrumental perteneciente al sector público andaluz, en su condición de encargada del tratamiento de una pluralidad de responsables, dis-

poniendo para ello de infraestructuras o servicios digitales corporativos de uso común y transversales a todos los organismos, donde tratan datos personales.

Al respecto, en opinión de la entidad consultante, cuando se producen brechas que afectan a datos personales de infraestructuras corporativas o servicios digitales de uso común por todos los organismos que gestiona como encargada de tratamiento, en las que los hechos, consecuencias y medidas correctivas tomadas son las mismas, parece razonable y oportuno que la notificación a este Consejo sea realizada por dicha entidad, sin que ello suponga asumir la responsabilidad de la brecha, o de la obligación de su comunicación, sino la de ser el actor material de dicha notificación. Adicionalmente, considera que puede ser oportuno que en este tipo de brechas, la comunicación a los interesados afectados, en su caso, también se realice por la entidad encargada del tratamiento.

A tenor de lo expuesto, la entidad consultante realiza, en esencia, las siguientes consultas:

1. Si a juicio del Consejo resulta conveniente las actuaciones propuestas.

2. ¿Cómo delimitar o caracterizar correctamente aquellas brechas en las que sí resulta, no solo oportuna sino necesaria una notificación por parte del encargado del tratamiento en las circunstancias descritas?.

3. ¿Qué contenido, cuándo y cómo se considera que debe comunicarse a los organismos responsables de este tipo de brechas?.

4. ¿En qué circunstancias se considera apropiado que la comunicación y la justificación de la decisión a las personas afectadas se realice por parte del encargado del tratamiento en las circunstancias descritas?.

3. Marco normativo de la gestión de brechas de seguridad de los datos personales.

De conformidad con el artículo 4.12) del RGPD, se entiende por violación de la seguridad de los datos personales:

> *"toda violación de la seguridad que ocasione 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;".*

Al respecto, el artículo 33 del RGPD dispone:

> *"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.*

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.”.

Asimismo, el artículo 34.1 del RGPD establece:

"*1.Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.*"

Por su parte, el artículo 28.3.f) determina que el contrato o acto jurídico que vincule al encargado respecto del responsable, estipulará que el encargado:

“f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;”

La traslación del contenido de los preceptos indicados al supuesto referido en la consulta no debe conducir a descartar necesariamente la posibilidad de que un encargado del tratamiento efectúe la notificación de una brecha de datos personales a la autoridad de control y la comunicación a los afectados en su caso, en nombre del responsable del tratamiento, o incluso de una pluralidad de estos, si así queda adecuadamente recogido en el encargo de tratamiento suscrito mediante acto jurídico vinculante entre las respectivas partes y siempre tomando en consideración las restantes condiciones y garantías expuestas a lo largo del presente dictamen.

En todo caso, conviene tener presente que, la responsabilidad legal del cumplimiento de estas obligaciones recae en el responsable del tratamiento, como señala el Comité Europeo de Protección de Datos en el párrafo 48 de sus Directrices 9/2022, sobre notificación de violaciones de datos personales bajo el RGPD.

4. Sobre determinadas obligaciones de los responsables del tratamiento en la gestión de brechas.

La realización por parte del encargado del tratamiento de las previstas notificaciones y comunicaciones de las brechas de datos personales no podría vaciar de contenido las obligaciones que el RGPD atribuye a los responsables del tratamiento.

Al respecto, resulta relevante la lectura conjunta del considerando 85 y del artículo 33.3.b) del RGPD:

Considerando 85 RGPD:
"Si no se toman a tiempo medidas adecuadas, las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas, como pérdida de control sobre sus datos personales o restricción de sus derechos, discriminación, usurpación de identidad, pérdidas financieras, reversión no autorizada de la seudonimización, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, o cualquier otro perjuicio económico o social significativo para la persona física en cuestión.

Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales, el responsable debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas. "

Artículo 33.3 del RGPD (referido al contenido mínimo de la notificación):
"*d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*"

Las disposiciones transcritas inciden en dos aspectos fundamentales: por un lado, en la necesidad de realizar un análisis específico de los riesgos que para los derechos y libertades de las personas físicas pudiera entrañar cada brecha de datos personales, y de adoptar, en su caso, las medidas adecuadas; y, por otro, en la importancia de su oportuna notificación.

En el referido análisis deben considerarse los daños y perjuicios que las brechas de datos personales pueden provocar a las personas físicas. Tales daños y perjuicios pueden ser de diversa índole y materializarse de forma distinta en relación con la naturaleza, alcance, contexto y fines del tratamiento en cuestión. Todo ello con independencia de que sea un mismo evento, como por ejemplo un incidente de seguridad en una infraestructura tecnológica compartida, el que hubiera originado los diversos riesgos. Así, mientras que dicho incidente de seguridad podría conllevar en determinados tratamientos un riesgo de daño en la reputación personal de los afectados, en otro podría suponer un riesgo de restricción de derechos personales, y en un tercero, un riesgo para la integridad física personal.

Resulta, pues, evidente que no todos los tratamientos se verán siempre afectados de la misma forma por una brecha de datos personales. Es por ello, por lo que el RGPD exige al responsable del cada tratamiento afectado un análisis de los riesgos que la brecha supone para los derechos y las libertades de las personas físicas.

Este análisis, podría partir de un análisis de riesgos "general" derivado de la información que, sobre la naturaleza, gravedad y posibles consecuencias de la brecha, dispone el encargado,

sin duda más relevante, al estar este directamente involucrado en la operación y en el mantenimiento de la infraestructura o servicio digital afectado. Correspondería a cada responsable del tratamiento, utilizando la información facilitada por el encargado, culminar el análisis de como afecta la brecha de datos personales a los tratamientos que lleva a cabo, evaluando el riesgo que la misma entraña para los derechos y libertades de las personas físicas (improbabilidad de riesgo,probabilidad de riesgo, o probabilidad de alto riesgo) a los efectos de su adecuada gestión.

En íntima conexión con lo indicado y aún con mayor intensidad, deberá actuarse en relación con las medidas adoptadas o propuestas para poner remedio a la brecha de datos personales, incluyendo, si procede, las medidas para mitigar los posibles efectos negativos. Una brecha puede afectar tanto a las dimensiones de confidencialidad e integridad de los datos como a la de disponibilidad. Por tanto, existirán medidas de carácter técnico que serán de aplicación a la infraestructura afectada, lo cual no impide que sean también necesarias otras medidas concretas para determinados escenarios derivados de los riesgos en un tratamiento en particular. Dichas medidas, más específicas, requerirán de un conocimiento especializado del tratamiento, que a priori deberán ser determinadas y aplicadas por el responsable, como podría ser la declaración de la ampliación de plazos para un determinado procedimiento que se hubiese visto afectado.

5. Análisis de la notificación de la brecha de datos por el encargado del tratamiento.

La notificación de las brechas de datos personales por parte del encargado en nombre de múltiples responsables, aun siendo posible en el marco del RGPD, debe ser analizada cuidadosamente. El principal reto radica en aunar la deseable eficiencia operativa con la necesidad de adoptar las medidas adecuadas para garantizar la mayor protección para los derechos y las libertades de las personas físicas en caso de una brecha. Un enfoque generalizado podría resultar insuficiente para abordar los riesgos específicos que suponga la brecha para cada tratamiento. Sin embargo, pueden darse escenarios donde la notificación por parte del encargado al Consejo, a la vez que se informa a los responsables, pudiera constituir la acción adecuada.

Para ello, los responsables del tratamiento deberían exigir al encargado una serie de condiciones a satisfacer simultáneamente que garantizasen el cumplimiento del marco de diligencia que les es exigido en virtud del artículo 33 del RGPD. Sin perjuicio de que corresponde en exclusiva a los responsables establecer dichas condiciones, podría ser apropiado considerar las siguientes para que la notificación de la brecha al Consejo la llevase a cabo el encargado:

1. La brecha afecta a una infraestructura o servicio común que presta servicio a múltiples responsables.

2. El encargado posee información técnica detallada sobre la naturaleza y alcance de la brecha que los responsables no podrían obtener fácilmente por sí mismos.

3. El encargado está en disposición de realizar una evaluación inicial de los riesgos y de adoptar medidas de mitigación aplicables de manera general, sin perjuicio de los análisis específicos posteriores de cada responsable.

4. El encargo de tratamiento establece la obligación de que el encargado se encuentre en disposición de acreditar haber proporcionado información completa y detallada de la brecha a todos los responsables afectados a la vez que se realiza la notificación.

En la situación propuesta, cuando concurriesen las condiciones previamente indicadas y siempre que se garantizase el pleno cumplimiento de los requisitos del RGPD, especialmente en términos de plazos y responsabilidad y la adopción a tiempo de las medidas adecuadas, se podría implementar un sistema de notificación en dos fases. En la primera, se realizaría la notificación inicial por el encargado al Consejo, dentro del plazo de 72 horas establecido por el RGPD. Dicha notificación contendría todos los elementos exigidos en el artículo 33.3 del RGPD, incluyendo el nombre y los datos de contacto del DPD o de otro punto de contacto de todos los responsables afectados por la brecha, así como las posibles consecuencias de la misma y las medidas adoptadas o propuestas, expuestas lo más detalladamente posible. La información contenida en la notificación inicial y en las complementarias que llegasen a efectuarse por el encargado, se haría llegar simultáneamente a los puntos de contacto de todos los responsables afectados, los cuales podrían ser los DPD u otras personas, siempre y cuando se garantice que disponen de autoridad y competencia suficiente para impulsar las acciones necesarias en el seno del responsable con vistas a poner remedio a la brecha y mitigar sus consecuencias. El canal de comunicación empleado para ello deberá asegurar las condiciones de integridad y confidencialidad de la información intercambiada entre encargado y responsables de tratamiento.

Tras la notificación inicial del encargado, cada responsable afectado debería realizar y documentar, con la ayuda del encargado, su propio análisis de riesgos específico para los tratamientos bajo su responsabilidad, utilizando la información proporcionada por el encargado. En este contexto, si los responsables reciben nueva información relativa a la brecha deberían revisar su valoración del riesgo efectuada, documentando las decisiones adoptadas, siendo recomendable que compartan los resultados de sus análisis, garantizándose en todo caso el pleno respeto a la protección de datos personales.

Si se identificasen riesgos específicos para el tratamiento no documentados por el encargado, el responsable debería determinar y aplicar sin dilación las medidas adicionales necesarias para mitigar esos riesgos, así como realizar una notificación complementaria a las efectuadas por el encargado al Consejo, detallando los riesgos específicos identificados y las medidas adoptadas o propuestas, que sería recomendable hacer llegar al encargado.

En todo caso, tanto los responsables que hayan realizado notificaciones complementarias como el propio encargado deberán asegurarse que proporcionan toda la información que sea requerida por este Consejo.

6. Análisis de la comunicación a los interesados afectados de la brecha por el encargado del tratamiento.

La comunicación de la brecha de datos personales a los interesados resulta obligatoria, salvo las excepciones previstas en el artículo 34.3 del RGPD, en caso de que sea probable que entrañe un alto riesgo para sus derechos y libertades y tiene como objetivos principales ayudar a los afectados a entender la naturaleza de la brecha y permitirles tomar las precauciones necesarias. La comunicación debe efectuarse lo antes posible puesto que cualquier dilación en la misma le resta efectividad, de forma que una comunicación a destiempo puede llegar a tener el mismo efecto que una comunicación no realizada. Esta circunstancia debe constituir un elemento esencial a la hora de diseñar cualquier procedimiento de gestión de brechas de datos personales.

La comunicación deberá contener, entre otra información, recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la brecha, así como los datos de contacto del DPD (o de otro punto de contacto).

A tenor de lo expuesto se infiere un escenario particularmente complejo para la gestión de las comunicaciones a los afectados por parte del encargado, con vistas a procurar la adecuada protección de los derechos y libertades de aquellos y a responder al principio de responsabilidad proactiva exigido a los responsables del tratamiento. Aunque un incidente de seguridad sea común y el encargado pueda realizar una evaluación inicial de los riesgos del mismo, la decisión final sobre si la brecha puede entrañar un alto riesgo para los derechos y libertades de los afectados que requiera comunicación a estos recae en cada responsable. Pueden darse situaciones donde tanto el canal de comunicación como las recomendaciones a proporcionar a los afectados para mitigar los potenciales efectos adversos varíen según el tratamiento de que se trate. Los responsables deben disponer de medios y capacidad para atender preguntas de los afectados sobre las causas de la brecha, los posibles efectos concretos de la misma y las medidas adoptadas o recomendadas, entre otras.

Todo ello demanda el establecimiento de una serie de condiciones que los responsables deberían exigir al encargado para equilibrar adecuadamente la deseable eficiencia en la gestión de las comunicaciones con las obligaciones establecidas en el artículo 34 del RGPD para los responsables del tratamiento. Sin perjuicio de que corresponde en exclusiva a los responsables establecer dichas condiciones, podría ser apropiado considerar las siguientes para que las comunicaciones a los interesados afectados las llevase a cabo el encargado:

1. La brecha afecta a una infraestructura o servicio común que presta servicio a múltiples responsables, y el impacto en los datos personales es similar para todos o la mayoría de los responsables afectados.

2. El encargado posee información técnica detallada sobre la naturaleza y alcance de la brecha que los responsables no podrían obtener fácilmente por sí mismos.

3. El encargado ha realizado una evaluación inicial de los riesgos que indica la probabilidad de un alto riesgo para los derechos y libertades de los afectados, y esta evaluación es aplicable de manera general a los tratamientos de todos o la mayoría de los responsables implicados.

4. El encargado está en condiciones de proporcionar recomendaciones prácticas y efectivas para que los afectados mitiguen los potenciales efectos adversos de la brecha, y estas recomendaciones son aplicables de manera uniforme a todos o la mayoría de los afectados, independientemente del tratamiento específico.

5. El encargo de tratamiento establece la obligación de que el encargado proporcione sin dilación indebida información completa y detallada sobre las comunicaciones realizadas a todos los responsables afectados.

6. El encargado cuenta con la capacidad y la formación suficiente en las especificidades de los tratamientos de los responsables necesarias para gestionar las posibles consultas de los afectados y se ha establecido un protocolo claro para trasladar rápidamente las cuestiones específicas a cada responsable.

7. Se garantiza que la comunicación centralizada no impide ni retrasa que cada responsable realice y documente su propio análisis de riesgos específico para los tratamientos de su responsabilidad y adopte las medidas adecuadas, incluyendo comunicaciones adicionales a los afectados por sus tratamientos, en su caso.

7. Procedimiento y encargo de tratamiento.

El protocolo o procedimiento que regule esta forma de gestionar notificaciones y comunicaciones de brechas de datos personales en la que intervengan múltiples responsables y un encargado común, requeriría de un marco de gobernanza detallado, adecuadamente formalizado en el encargo de tratamiento suscrito mediante un acto jurídico vinculante entre las partes. Dicho encargo debería contemplar al menos, los siguientes aspectos esenciales:

1. Definición de las situaciones que activarían el protocolo centralizado, identificando con precisión los incidentes que afectan a la infraestructura o servicio común y detalles concretos de las condiciones que deben cumplirse para iniciar el proceso centralizado.

2. Descripción detallada del flujo de trabajo, desde la detección de la brecha hasta la resolución final, especificando los plazos concretos para cada fase, los canales de comunicación entre encargado y responsables, los modelos estandarizados para el intercambio de información y los mecanismos de escalado.

3. Definición clara de las funciones y responsabilidades de cada parte, incluyendo las obligaciones específicas del encargado en la evaluación inicial y en la notificación, las responsabilidades de cada responsable en el análisis de riesgo específico y en la adopción de medidas adicionales y la designación de los puntos de contacto. Deberá asegurarse el respeto al principio de responsabilidad proactiva y la capacidad de demostrar su cumplimiento ante el Consejo.

4. Descripción detallada de la gestión de las comunicaciones a los afectados, incluyendo el proceso de decisión sobre la misma, los modelos y los canales de comunicación a utilizar y la gestión de las consultas de los afectados.

5. Implementación del sistema documental donde registrar cada brecha de datos personales, los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas.

6. Establecimiento de mecanismos de coordinación eficientes entre encargado y responsables de tratamiento.

8. Papel del delegado de protección de datos (DPD)

Resulta incuestionable la relevancia del papel que el DPD debe desempeñar durante todo el proceso de gestión de una brecha de datos personales dadas sus funciones de asesoramiento a responsables y encargados de tratamientos sobre sus obligaciones en materia de protección de datos, de supervisión del cumplimiento del RGPD para garantizar una respuesta efectiva y conforme a la normativa, y de actuación como punto de contacto de la autoridad de control para cuestiones relativas al tratamiento.

Por tanto, el DPD de cada responsable o encargado debería ser informado con celeridad de la existencia de una brecha, de forma que, desde el primer momento pueda asesorar y supervisar activamente ~~en~~ todas las fases de gestión y notificación de la misma y actuar como interlocutor ante el Consejo y ante los afectados por la brecha. Se estima conveniente que sus funciones en este contexto, ya sea actuando en calidad de DPD de un responsable o de un encargado del tratamiento, queden descritas adecuadamente en el protocolo o procedimiento citado en el apartado anterior.

9. Conclusiones.

La gestión centralizada de notificaciones y comunicaciones de brechas de datos personales en escenarios de múltiples responsables con un encargado común, presenta tanto oportunidades como dificultades significativas en el marco del RGPD. Si bien la misma puede ofrecer una mayor eficiencia operativa, solo podría llevarse a cabo garantizando el pleno cumplimiento de

las obligaciones legales de cada responsable del tratamiento, y en particular del principio de responsabilidad proactiva.

La viabilidad de dicha gestión se basaría en un ponderado equilibrio entre la centralización de ciertas funciones en el encargado y el mantenimiento de la responsabilidad individual de cada responsable. Para ello, resulta imprescindible establecer un marco de gobernanza robusto y detallado, formalizado mediante un acto jurídico vinculante, que delimite con precisión las funciones, responsabilidades y procedimientos de todas las partes implicadas.

Conviene subrayar que este modelo de gestión no exime a los responsables de sus obligaciones individuales en cuanto al análisis de riesgos específicos de sus tratamientos y la adopción de medidas de mitigación adecuadas. Así, la notificación y comunicación a los afectados, en su caso, de la brecha de datos personales que efectuara el encargado debe concebirse como un primer paso, complementado posteriormente por las acciones individualizadas de cada responsable que fueran necesarias.

Este modelo requiere una atención especial a aspectos como la rapidez en la actuación, la coordinación eficaz entre las partes, la documentación exhaustiva de todo el proceso y la capacidad de adaptación a las particularidades de cada tratamiento afectado.

Finalmente, el papel de los DPDs involucrados adquiere, si cabe, una relevancia aún mayor en este contexto, siendo recomendable su participación activa en todas las fases del proceso, contribuyendo a garantizar el cumplimiento normativo y la protección efectiva de los derechos y libertades de los interesados afectados.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA
Y PROTECCIÓN DE DATOS DE ANDALUCÍA

Jesús Jiménez López.