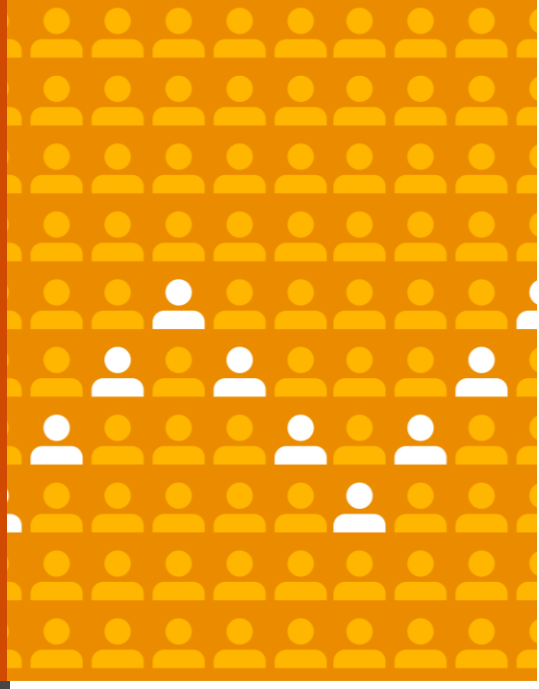
Newsletter de NewLaw de PwC Tax&Legal Services

Breves Regulación Digital: Sanciones entorno a la figura del Delegado de Protección de Datos



Analizamos dos situaciones distintas que han dado lugar a sendas sanciones en torno a la figura del Delegado de Protección de Datos

junio 2020

En el presente número de Breves:

Analizamos dos situaciones distintas que han dado lugar a sendas sanciones en torno a la figura del Delegado de Protección de Datos, (en adelante "DPD").

Es relativamente frecuente la designación como DPD de un profesional en plantilla que a su vez asume otros cargos o roles de cierta relevancia dentro la organización. En otras ocasiones en cambio, se incumple con la designación de la figura del DPD contemplada en el art. 37 RGPD.

En el presente número, analizamos la reciente resolución de la Autoridad de Protección de Datos Belga mediante la cual se sanciona a una compañía que nombró como DPD a una persona que ocupaba en la compañía otros cargos incompatibles con dicho rol, desde la óptica de la normativa de protección de datos y la resolución de la AEPD impuesta a una compañía que, realizando tratamiento de datos a gran escala, no había designado ante la Agencia a un DPD.

Resolución de la Autoridad Belga

El pasado 28 de abril de 2020, la Autoridad de Protección de Datos Belga, impuso una sanción de 50.000 euros a una compañía por el incumplimiento del deber de evitar un conflicto de intereses previsto en el artículo 38 del Reglamento General de Protección de Datos (el "**RGPD**").

Hechos que motivan el inicio del expediente sancionador

El expediente sancionador que nos ocupa trae causa en un incidente de seguridad consistente en el error cometido por la compañía infractora en el envío de comunicaciones a distintas cuentas de correo electrónico "secundarias", vinculadas en su base de datos a un mismo cliente, cuando en realidad, no tenían ninguna conexión directa con dicho cliente.

A raíz de dicho incidente, se lleva a cabo por parte de la autoridad de control belga, una investigación para conocer la forma en la que la compañía gestiona y resuelve las brechas de seguridad que pueda sufrir.

Concluida la investigación, la Autoridad Belga, en su informe de Inspección señala 3 posibles incumplimientos por parte del responsable del tratamiento:

1. **Incumplimiento de la obligación de cooperar con la autoridad de control** (Artículo 31 del RGPD).
2. **Incumplimiento del principio de responsabilidad proactiva** (Artículo 5.2 del RGPD) en lo que respecta a la aplicación del enfoque de riesgos para el análisis y evaluación de una brecha de seguridad (Artículo 24.1 y 33 del RGPD).
3. **Incumplimiento de la obligación de garantizar que las funciones y cometidos del DPD no den lugar a un conflicto de intereses** por el nombramiento del DPD (Artículo 38.6).

Tras el análisis del informe por parte del correspondiente órgano competente, se descarta la existencia de las infracciones relativas a la falta de cooperación y al principio de responsabilidad proactiva, estimando probada la **vulneración del artículo 38.6 del RGPD**, por los motivos que analizamos a continuación.

Fundamentos jurídicos de la resolución belga

En primera lugar, la resolución indica que la posible existencia de un conflicto de intereses **debe valorarse caso por caso**,

y no se limita únicamente a que el DPD decida o no sobre los fines y los medios del tratamiento.

En ese sentido, la resolución fundamenta el incumplimiento del art. 38.6 del RGPD y la imposición de la consecuente sanción, principalmente, porque el DPD asume, al mismo tiempo, roles de superior jerárquico o jefe de otros departamentos dentro de la entidad (i.e. cumplimiento, gestión de riesgos y auditoría interna), roles estos que le otorgan poder de decisión sobre los fines y los medios del tratamiento dentro del departamento en cuestión.

En este sentido, **el hecho de que el DPD tenga poder de decisión sobre determinados tratamientos impide que pueda ejercer sus funciones de supervisión** en materia de protección de datos de forma independiente respecto de dichos tratamientos, derivándose en consecuencia el conflicto de intereses que la norma sanciona, a pesar de los argumentos expuestos por la empresa respecto de la supuesta función meramente consultiva de las posiciones ostentadas en los distintos departamentos.

Al respecto estima que no puede sostenerse la exigida independencia en la persona que no sólo forma parte de un determinado departamento, si no que **es responsable de asesorarle y, al mismo tiempo, ejerce la función de DPD,** máxime cuando no se prueba la existencia de medidas encaminadas a impedir el conflicto de intereses que se pretende evitar.

Por otra parte, al objeto de la calificar la **sanción como grave,** la autoridad de control aplica los criterios habituales de volumen de datos tratados por el responsable, tipología de datos y duración y riesgo del tratamiento, etc.

Adicionalmente, y a pesar de no estimar la existencia de intencionalidad, la resolución determina que el responsable **contaba con los medios suficientes para conocer que se podía producir un conflicto de intereses.**

Y lo anterior por cuanto, a pesar de estar frente a una figura no obligatoria en Bélgica hasta la aplicación efectiva del RGPD, el hecho de que la misma ya se contemplara en los ordenamientos jurídicos internos de algunos Estados Miembro, y que existieran distintas guías y recomendaciones respecto de las funciones y régimen de independencia del DPD emitidas por el antiguo GT 29 (ahora el Comité Europeo de Protección de Datos), permitía al responsable conocer su alcance y régimen de incompatibilidades, máxime tratándose de una organización en la que el tratamiento de datos constituye una actividad esencial que le exige, con mayor intensidad si cabe, el cumplimiento del principio de responsabilidad proactiva.

El importe de la sanción asciende a 50.000 euros.

Conflicto de intereses que pueden afectar al DPD

Tal y como acabamos de apuntar, el Comité Europeo de Protección de Datos en sus directrices sobre los DPD publicadas en el año 2016, establece que el conflicto de intereses está estrechamente vinculado a la independencia del DPD.

En este sentido, aunque la figura del DPD pueda asumir otras funciones dentro de las compañías, solamente podrán confiárseles otras tareas y cometidos si éstas no entrañan o pueden comportar un conflicto de intereses.

Según lo dispuesto en dichas directrices, los cargos o posiciones que tengan funciones de gestión de un departamento o de alta dirección en la compañía pueden suponer un conflicto de intereses con la asunción de la figura del rol del DPD. A título de ejemplo, los cargos de director general, director de operaciones, director financiero, director médico, jefe del departamento de mercadotecnia, jefe de recursos humanos o director del departamento de TI, podrían ser posiciones incompatibles por darse ese potencial conflicto de intereses.

Esto supone, en definitiva, que el DPD no puede ocupar un cargo adicional en la organización que le lleve a determinar los fines y medios del tratamiento de datos personales ya que dicha determinación afectaría a su independencia como DPD y a la responsabilidad operacional en cuanto a la supervisión y monitorización de los tratamientos de datos de la entidad.

En este mismo sentido se pronunció también la Agencia Española de Protección de Datos (en adelante "AEPD") en su informe 170/2018 en el que declaraba la incompatibilidad entre el rol de DPD y la asunción del cargo de responsable de seguridad a efectos del Esquema Nacional de Seguridad (en adelante, "**ENS**").

Dos de los principales argumentos de la AEPD para declarar la incompatibilidad entre estas dos figuras son:

- La independencia del DPD es más estricta que la del responsable de seguridad ENS. El primero no puede recibir instrucciones del responsable o el encargado del tratamiento, mientras que no existe ese impedimento en el segundo caso.
- Existe un conflicto de interés entre ambas figuras, dado que el DPD debe supervisar el trabajo realizado por el responsable de seguridad ENS.

Igual que la autoridad de control belga y el antiguo GT29, la AEPD pone el foco en la independencia del DPD y en las tareas de supervisión de éste respecto de otras áreas a la hora de determinar la existencia de un posible conflicto de intereses con la asunción de roles adicionales dentro de la organización.

Resolución de la AEPD

El 9 de junio de 2020, la Agencia Española de Protección de Datos, sancionó a una compañía por el incumplimiento de la obligación de designar a un DPD, prevista en el art. 37.1b) del RGPD en relación con el 34 de la LOPDGDD.

En esta ocasión la infracción entorno a la figura del DPD no lo es por la existencia de conflicto de intereses en el desempeño de sus funciones, sino que en el supuesto analizado por la AEPD, la infracción se produce por la ausencia de dicha figura, esto es, su falta de nombramiento y comunicación a la autoridad de control por parte de una plataforma e-commerce.

Hechos que motivan el inicio del expediente sancionador

Los hechos que motivan el inicio del procedimiento sancionador son las denuncias formuladas por distintos usuarios por la falta de nombramiento de un DPD al que dirigir sus reclamaciones en mayo y noviembre de 2019.

Tras recibir la primera reclamación, la AEPD dió traslado de la misma a la compañía e-commerce en julio 2019, para que formulase las oportunas alegaciones, respondiendo ésta que no estaba obligada a designar a un DPD al no encuadrarse los tratamientos realizados en los supuestos previstos en el art. 37 RGPD ni en el 34 LOPDGDD.

Recordemos que de acuerdo con el art. 37.1 del RGPD, es obligatoria la designación de un DPD cuando:

"a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;

b) las actividades principales del responsable o del encargado consistan ***en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala,*** *o*

c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10."

Procedimiento sancionador

En enero de 2020 la AEPD acuerda el inicio del procedimiento sancionador por presunta infracción del art. 37 RGPD tipificada en el art, 83.4 RGPD.

La plataforma e-commerce alegó que las actividades de tratamiento que llevaba a cabo no se encontraban entre las previstas en el art. 37 RGPD, y que por tanto no estaba obligada a proceder a la designa formal de un DPD, pero que no obstante contaba con un Comité de Protección de Datos que desempeñaba las funciones propias de un DPD, desde junio de 2018.

Tras la práctica de prueba, en febrero de 2020 la AEPD mantiene su posición y formula propuesta de resolución, planteando que se sancione a la compañía e-commerce por una infracción del art. 37 RGPD, tipificada en el art. 83.4 RGPD.

Con posterioridad, la e-commerce alega que procedió a la designa de un DPD en mayo de 2019 pero que no fue hasta febrero de 2020 cuando se comunicó oficialmente ante el Registro de la AEPD dicha designa.

Fundamentos jurídicos de la resolución

A tenor de lo dispuesto en la resolución publicada por la AEPD, son hechos probados que la plataforma e-commerce no había nombrado un DPD porque, aunque consideraba que no estaba obligada a designarlo, contaba con un Comité de Protección de datos que llevaba a cabo las funciones propias del DPD, procediendo finalmente a designarlo en febrero de 2020

En los Fundamentos de Derecho se considera vulnerado el art. 37.1 b) del RGPD al realizar la entidad reclamada **tratamiento de datos personales a gran escala.** El importe de la sanción es de 25.000 euros.

Como hemos tenido ocasión de comentar en distintas ocasiones, no existen parámetros previamente definidos en cuanto a qué se considera tratamiento a gran escala, y habría sido una buena oportunidad que en la propia resolución se adelantaran cuáles han sido los criterios que han permitido a la AEPD entender que el tratamiento llevado a cabo por la plataforma e-commerce que ofrece servicio a sus usuarios a través de una app, es un tratamiento a gran escala, y los criterios para determinar **las circunstancias agravantes**, como son que alude al número de interesados afectados sin indicar cuantos, o que se encuentren afectados identificadores personales básicos (83.2 a) y (83.2 g) RGPD, así como conocer si la condición de entidad prestadora de servicios de la sociedad de la información del art.34 d) LOPDGDD ha determinado igualmente la exigencia de nombramiento de un DPPD para la plataforma e-commerce.

En el presente Breves han colaborado:

Assumpta Zorraquino Rico
Socia responsable de Regulación Digital
Departamento New Law
assumpta.zorraquino@pwc.com

Alejandra Matas Brancós
Directora de Regulación Digital
Departamento New Law
alejandra.matas.brancos@pwc.com

Galindo Pérez Sánchez
Departamento New Law
galindo.perez.sanchez@pwc.com

Gonzalo Pérez Bargueño
Departamento New Law
gonzalo.perez.bargueno@pwc.com

Conclusiones

Es necesario analizar cuales son las actividades de tratamiento principales que lleva a cabo la compañía para determinar si existe o no la obligación de designar un DPD, no solo de acuerdo con las previsiones contempladas en el art. 37 del RGPD, sino también la relación de entidades recogidas en el art. 34 de la LOPDGGD.

Del mismo modo, a la hora de designar un DPD dentro de una organización, se debe establecer de forma clara las funciones de esta figura, así como delimitar las posibles incompatibilidades que pudieran darse con otras posiciones asumidas por la misma persona.

Para ello, deben adoptarse medidas de responsabilidad proactiva para evitar la existencia de un eventual conflicto de intereses:

- Definir un modelo de gobierno de la privacidad eficaz en el que se asignen funciones y roles al DPD y al resto de empleados.
- Elaborar un estatuto de la figura del DPD en el que se indiquen sus funciones, su posición dentro de la entidad y el órgano al que debe reportar.
- Elaborar una política de conflicto de intereses en materia de protección de datos o incluir un apartado en esta materia en la política de conflicto de intereses corporativa. Es aconsejable que se indiquen los roles que la entidad considera incompatibles con la figura del DPD.
- Declaración del órgano de dirección de la inexistencia de un conflicto de intereses respecto del DPD designado.

El DPD podrá desempeñar otras funciones y cometidos. Deberá analizarse caso a caso la concurrencia en la misma persona de la figura del DPD y de otros roles adicionales dentro de la misma entidad para evitar que dicha concurrencia derive en un conflicto de intereses.

Cuando la compañía tenga la obligación de nombrar a un DPD en virtud de lo establecido en el RGPD y la LOPDGDD, la existencia de un Comité de Protección de Datos que desarrolle dichas funciones no exime del cumplimiento de la norma y puede dar lugar a la comisión de la infracción.