

- Procedimiento N°: PS/00360/2020

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

Del procedimiento instruido por la Agencia Española de Protección de Datos y en base a los siguientes

ANTECEDENTES

PRIMERO: D. **A.A.A.** (en adelante, el reclamante) con fecha 08/06/2020 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **UST GLOBAL ESPAÑA, S.A.**, con NIF **A84816644** (en adelante, UST GLOBAL o la reclamada). Los motivos en que se basa la reclamación son, en síntesis: el reclamante trabaja para la consultora UST GLOBAL, que está prestando servicios a OpenBank; el 08/01/2020 la reclamada comunicó a OpenBank, mediante correo electrónico, que se incorporarían al proyecto dos nuevos empleados (uno de ellos el reclamante), para los que solicitaba se facilitara acceso a la VPN y demás aplicaciones; en dicho correo electrónico, enviado con copia a ambos empleados, se facilitaban sus nombres y apellidos, correos electrónicos profesionales y números de DNI. El reclamante señala al respecto que tal comunicación debería haberse realizado de manera independiente, de modo que no tuviera conocimiento de los datos de su compañero y viceversa.

Aporta copia del correo electrónico que motiva la denuncia, de fecha 08/01/2020, cuyos detalles constan reseñados en el Hecho Probado Cuarto.

SEGUNDO: El 16/06/2020, la reclamación fue trasladada a UST GLOBAL para que procediera a su análisis.

El 15/07/2020, en respuesta a dicho traslado, la entidad reclamada informó que el reclamante estuvo empleado en esa entidad desde el 25/02/2019 hasta el día 03/04/2020.

En cuanto a los hechos denunciados, señaló que su actuación se encontraba dentro de los parámetros de la razonabilidad y del respeto a la privacidad y a la protección de datos bajo un criterio de equilibrio entre la eficiencia empresarial y la implantación de controles rigurosos; que se trataba de dos empleados que iban a incorporarse a la gestión de un proyecto en Grupo Santander conjuntamente y que enviar los datos de ambos al responsable, para otorgarles los privilegios de acceso en el marco del encargo, no parecía constituir una actuación que excediera de los límites que las normas imponen; que para ese tratamiento no era necesario el consentimiento del empleado; y que no resultan vulnerados el artículo 5.1.f) del RGPD ni el 5 de la LOPDGDD. Considera que UST GLOBAL se limitó a cumplir con una obligación contractual contraída con un cliente.

Que ninguna medida se ha adoptado por la reclamada, al considerar que la actuación

referida en la denuncia interpuesta es ajustada a las normas sobre protección de datos. Que se ha procedido a poner la denuncia en conocimiento del responsable de RRHH y se procederá a la valoración de los hechos, junto con el DPD, teniendo en cuenta la posible opinión de la Agencia Española de Protección de Datos, por si en el futuro se considerase necesario evitar que, incluso tratándose de dos personas que van a colaborar en un proyecto con un cliente, sus datos deban enviarse por separado a quien los recibe, o de otro modo encriptar o protegerse mediante medidas de seguridad adecuadas.

TERCERO: El 07/10/2020, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada.

CUARTO: Con fecha 05/11/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5.a) del mismo texto legal, determinando que la sanción que pudiera corresponder ascendería a un total de 5.000 euros (cinco mil euros), sin perjuicio de lo que resulte de la instrucción.

QUINTO: Notificado el citado acuerdo de inicio, la reclamada presentó escrito de alegaciones el 24/11/2020, en el que solicita que se declare la inexistencia de infracción y se proceda al archivo de las actuaciones. Subsidiariamente solicita que se acuerde el apercibimiento con imposición de medidas correctoras. En síntesis, la citada entidad basa su petición en las consideraciones siguientes:

. Invoca la anulabilidad del acuerdo de inicio, considerando que en sus Fundamentos de Derecho se refiere a una posible infracción del artículo 5.1.f) del RGPD y en su parte dispositiva acuerda la apertura de procedimiento sancionador por una presunta infracción del artículo 6 del mismo Reglamento, que no ha resultado infringido, por cuanto el envío realizado de los datos de los empleados en el marco de un contrato de servicios está amparado por el este artículo 6, en su apartado 1.f) (interés legítimo). Considera la reclamada que tampoco el primer artículo citado ha sido vulnerado.

. Declara reproducidas las alegaciones efectuadas con ocasión del trámite de traslado, que constan reseñadas en el Antecedente Segundo. Entiende que el envío del correo objeto de la reclamación, facilitando a la persona responsable de seguridad del banco cliente los datos (nombre y apellidos, DNI y correo electrónico) de las personas que van a prestar servicios en dicha entidad, no constituye un tratamiento que no garantice una seguridad adecuada de los datos, ni en razón a un hipotético tratamiento ilícito, ni por su potencial pérdida, destrucción o daño accidental. Se limitó a cumplir una obligación contractual, identificando a los empleados ante el cliente, en cumplimiento de los pactos contractuales en materia de seguridad de la información.

Señala, además, que tanto la reclamada como su cliente mantienen medidas técnicas y organizativas adecuadas (aporta certificación ISO sobre el sistema de seguridad de la información que la reclamada mantiene en España).

Entiende que no se trata de una filtración de datos personales o que, de considerarse

así por el acceso a los datos del reclamante por parte de un compañero, no produce un daño a la privacidad, habida cuenta el tipo de datos tratados con ocasión del envío corporativo.

. La reclamada mantiene en todo caso una responsabilidad proactiva, habiendo designado un DPD, a pesar de no estar obligada a ello; ha externalizado esta función para que el DPD mantenga una mayor independencia de la compañía; cuenta con recursos internos suficientes en el Área de Calidad, con responsabilidad sobre el cumplimiento de la normativa de protección de datos por la entidad; incluye información sobre seguridad en la intranet corporativa, a disposición de los empleados; el DPD externo ha certificado la finalización de los procesos de adaptación al RGPD y a la LOPDGDD; dispone de un “Manual de Acogida” para nuevos empleados, que incluye información sobre privacidad; mantiene políticas de privacidad y seguridad de la información adecuadas.

Aporta diversa documentación sobre los extremos indicados, para que sea tenida en cuenta al elaborar la propuesta de resolución:

- . Política de uso y seguridad.
- . Formación a empleados.
- . Política de protección de datos.
- . Política de privacidad dirigida a proveedores y subcontratistas.
- . Planes de concienciación dirigido a empleados (2019 y 2020).

. En relación con la graduación de la sanción, considera que concurren los factores siguientes:

- . No existe intencionalidad o negligencia en el envío de información a una empresa del Grupo Santander, que viene obligada a aplicar medidas de control en el tratamiento de los datos.
- . El interesado no ha sufrido daño o perjuicio alguno, tanto por los datos afectados como por el marco en que se compartieron.
- . Se trata de dos empleados que trabajan juntos y se conocían entre ellos.
- . Los envíos de datos a terceros se realizan mediante intercambio de archivos electrónicos, de modo que ninguno de los afectados pueda ver los datos personales de los demás.
- . La reclamada no ha cometido infracción alguna en esta materia.
- . Los datos personales no pertenecen a categorías especiales.
- . La reclamada no tiene especial vinculación con el tratamiento de datos, ni esto constituye su actividad principal. Únicamente es responsable de los datos personales de sus empleados, candidatos, autónomos que le prestan servicio y datos de contacto de empleados de clientes corporativos.
- . La infracción no es continuada.

- . No ha obtenido beneficio alguno de los hechos reclamados.
- . Dispone de DPD sin estar obligado a ello.
- . Tras conocer la denuncia, se trasladó la misma a RRHH y DPD para que se valore un nuevo plan de comunicación; y se comunicó a los responsables de área y supervisores recordándoles la necesidad de vigilar los controles de seguridad.

SEXTO: Con fecha 30/11/2020, el instructor del procedimiento acordó la apertura de un período de práctica de pruebas, acordándose las siguientes:

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por el reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente E/05043/2020.
- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio PS/00360/2020 presentadas por la reclamada y la documentación que a ellas acompaña.

SÉPTIMO: Con fecha 16/03/2021, la entidad reclamada presentó un nuevo escrito de alegaciones señalando que ha continuado desarrollando su programa de cumplimiento en materia de protección de privacidad y datos personales, habiendo impartido nuevamente formación específica a todos los empleados con pruebas de evaluación, en la que se incluyen aspectos relacionados con el envío de información a través del correo electrónico.

Acompaña un documento relativo a esta formación en nivel básico, que incluye una *“Guía de buenas prácticas para el envío de información confidencial y/o datos personales a clientes y/o proveedores”*, en la que se señala que el envío de correos con datos personales de empleados debe realizarse de manera individualizada, lo que evitará que se produzcan hechos similares a los denunciados en el futuro.

OCTAVO: Con fecha 25/05/2021, por la Subdirección General de Inspección de Datos se accede a la información disponible sobre la entidad UST GLOBAL en “Axesor”. En dicha web consta una cifra de negocios en el ejercicio 2018, último ejercicio presentado, de 46.395.898 euros y un resultado del ejercicio de -2.008.626 euros. Asimismo, se indica que es una empresa mediana, con 689 empleados.

Según la información que consta en el Registro Mercantil Central, el “Capital suscrito” asciende a 60.104 euros

NOVENO: Con fecha 27/05/2021 se formuló propuesta de resolución, en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancione a la entidad UST GLOBAL, por una infracción del artículo 5.1.f) del RGPD, en relación con el artículo 5 de la LOPDGDD, tipificada en el artículo 83.5.a) del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72 de la LOPDGDD, con una multa por importe de 5.000 euros (cinco mil euros).

Notificada la citada propuesta de resolución, con fecha 09/06/2021, se recibió en esta Agencia escrito de la entidad UST GLOBAL en el que formula las alegaciones

siguientes:

. Reitera, como causa de indefensión, que el acuerdo de inicio no concretó claramente la infracción presuntamente cometida, lo que le llevó a elaborar su respuesta en torno a la licitud de la cesión de datos realizada a OpenBank en base al interés legítimo concurrente. Solo por diligencia se estimó conveniente hacer referencia al envío del correo electrónico en cuestión a los dos compañeros de trabajo.

. La inclusión del DNI de los dos empleados en ese correo electrónico no supone, en el entorno laboral en el que ocurrieron los hechos, una revelación de datos confidenciales constitutiva de infracción. Añade que es probable que ambos compañeros tuvieran conocimiento del DNI del otro, por el propio desarrollo de su trabajo.

La misma propuesta de resolución considera que *“el interesado no ha sufrido daño o perjuicio alguno, tanto por los datos afectados como por el marco en el que se compartieron”* y que *“se trata de dos empleados que trabajan juntos y se conocían entre ellos”*.

. En cuanto a la graduación de la multa, de forma subsidiaria señala que la sanción propuesta por la revelación del número de DNI de un trabajador a otros es excesiva, más aún considerando que la propuesta mantiene la misma sanción determinada en la apertura del procedimiento, a pesar de corregir las agravantes y aplicar atenuantes no recogidas en el acuerdo de inicio del procedimiento.

Entre las agravantes que UST GLOBAL entiende corregidas menciona la falta grave de diligencia, la vinculación de la actividad de la empresa con el tratamiento de datos personales en el ámbito laboral, que es negada por la entidad reclamada.

También en relación con las agravantes, alega la reclamada que, si no hubo intencionalidad o negligencia, no puede agravarse la sanción por una grave falta de diligencia; y tampoco por la consideración de la entidad como gran empresa, indicada en el acuerdo de inicio, o como mediana empresa, según se indica en la propuesta de resolución, que no se encuentra entre las agravantes o atenuantes del RGPD o la LOPDGDD.

Por otra parte, destaca como atenuantes valoradas en la propuesta que no fueron consideradas al inicio del procedimiento las ya indicadas de ausencia de perjuicios y el entorno en el que se producen los hechos (dos personas que trabajaban juntas), las medidas tomadas por la empresa, la inexistencia de datos personales de categoría especial, o la ausencia de beneficios.

Finalmente, considera que debería tenerse en cuenta al fijar la sanción que la entidad dispone de DPD y la forma en que la Agencia ha tenido conocimiento de los hechos, mediante reclamación de un extrabajador, ocho meses después de causar baja en la entidad.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: El reclamante prestó servicios como empleado en la entidad UST GLOBAL. Esta entidad ha manifestado que el reclamante estuvo empleado en la misma desde el 25/02/2019 hasta el día 03/04/2020

SEGUNDO: UST GLOBAL, en el marco de la actividad económica que desarrolla, fue contratada para la prestación de servicios por la entidad OpenBank.

TERCERO: UST GLOBAL resolvió incorporar al reclamante, junto con otro empleado de esa entidad, a la gestión del proyecto que desarrollaba como prestador de servicios de OpenBank.

CUARTO: Con fecha 08/01/2020, desde el dominio “@ust-global.com”, se remitió un correo electrónico dirigido a dos usuarios con dominio “@gruposantander.com”, con copia a tres usuarios más del dominio “@ust-global.com”, entre ellos el reclamante y el otro el empleado de la reclamada al que se refiere el contenido del correo. Esta comunicación tiene como asunto “Accesos para nuevas incorporaciones” y el siguiente texto:

*“Buenos días... (nombres de los destinatarios del Grupo Santander)
Hemos incorporado hoy dos personas al equipo OpenBank, por lo que necesitaríamos que les solicitarais los accesos a la VPN, Jira, etc.
Los datos son:*

(...) (nombre y apellidos del reclamante, dirección de correo electrónico profesional y DNI)

(...) (nombre y apellidos de otro empleado de la reclamada, dirección de correo electrónico profesional y DNI)”.

Según ha manifestado UST GLOBAL, este correo fue remitido por la supervisora del reclamante.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

Con carácter previo, se estima oportuno analizar las cuestiones formales suscitadas por la reclamada en su escrito de alegaciones.

Tanto en su escrito de respuesta a la apertura del procedimiento como el presentado con ocasión de la propuesta de resolución, alega la citada entidad que el acuerdo de inicio del procedimiento sancionador es anulable considerando que en sus Fundamentos de Derecho se refiere a una posible infracción del artículo 5.1.f) del RGPD y en su parte dispositiva acuerda la apertura de procedimiento por una presunta infracción del artículo 6 del mismo Reglamento, que no ha resultado infringido.

A juicio de esta Agencia, el acuerdo de inicio dictado se ajusta a lo previsto en el artículo 68 de la LOPDGDD, según el cual bastará con que dicho acuerdo concrete los hechos que motivan la apertura, identifique la persona o entidad contra la que se dirige el procedimiento, la infracción que hubiera podido cometerse y su posible sanción.

En el mismo sentido se expresa el artículo 64.2 de la LPACAP, que establece expresamente el contenido mínimo de acuerdo de iniciación. Según este precepto, entre otros detalles, deberá contener *“los hechos que motivan la incoación del procedimiento, su posible calificación jurídica y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción”*.

En este caso, no solo se cumplen sobradamente las exigencias mencionadas, sino en los Fundamentos de Derecho del repetido acuerdo se va más allá ofreciendo razonamientos que justifican la posible calificación jurídica de los hechos valorada al inicio, mencionando, incluso, las circunstancias que pueden influir en la determinación de la sanción.

De acuerdo con lo expuesto, no puede decirse que el error cometido en la parte dispositiva del acuerdo al señalar la posible vulneración del artículo 6 del RGPD, en lugar del artículo 5.1.f) del mismo texto legal al que se refieren los Fundamentos de Derecho, haya limitado las posibilidades de defensa de UST GLOBAL. Esta entidad, en este caso, ha visto respetadas todas las garantías del interesado que prevé la normativa procesal y no puede decirse que dicho error haya supuesto ninguna merma de dichas garantías causante de indefensión.

La reclamada ha conocido la posible calificación de los hechos y ha podido alegar al respecto en su defensa lo que ha considerado oportuno. Prueba de ello es que ha formulado alegaciones sobre la no vulneración de lo dispuesto en el artículo 5.1.f) del RGPD.

Conforme a lo establecido en los artículos 89 y 90 de la LPACAP, son la propuesta de resolución y la resolución las que fijan la exacta calificación jurídica de los hechos que se tengan por probados.

III

El artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *“integridad y confidencialidad”*. Este artículo, en su apartado 1.f), señala lo siguiente:

“1. Los datos personales serán:

(...)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida,

destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).

El artículo 5 de la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), se refiere al “*Deber de confidencialidad*” en los términos siguientes:

“1. Los responsables y encargados del tratamiento de datos, así como todas las personas que intervengan en cualquier fase de este estarán sujetas al deber de confidencialidad al que se refiere el artículo 5.1.f) del Reglamento (UE) 2016/679.

2. La obligación general señalada en el apartado anterior será complementaria de los deberes de secreto profesional de conformidad con su normativa aplicable.

3. Las obligaciones establecidas en los apartados anteriores se mantendrán aun cuando hubiese finalizado la relación del obligado con el responsable o encargado del tratamiento”.

En el presente caso, el reclamante estuvo vinculado a la reclamada como empleado, en virtud de una relación de carácter laboral.

Bajo el amparo de esa relación, el reclamante fue asignado al proyecto que la reclamada desarrolló, como prestadora de servicios, para la entidad OpenBank.

Con ese motivo, la reclamada comunicó a OpenBank los datos personales del reclamante relativos a nombre y apellidos, dirección de correo electrónico profesional y DNI, con el propósito de que la entidad financiera dispusiera lo necesario para dar al reclamante acceso al sistema de información que le permitiera realizar las tareas que conllevara la prestación del servicio.

Estos tratamientos de datos personales del reclamante por parte de la reclamada, incluida la comunicación de aquellos datos a OpenBank, se estiman necesarios para el cumplimiento de las respectivas relaciones que vinculan a los intervinientes en los hechos.

No obstante, dicha comunicación de datos a la entidad financiera se realizó por parte de la reclamada mediante un correo electrónico, de fecha 08/01/2020, en el que no solo se incluían los datos personales indicados relativos al reclamante, sino también los datos correspondientes a otro empleado. Este correo electrónico se dirigió a OpenBank, pero se incluyó entre los destinatarios a los dos empleados titulares de los datos transmitidos, de forma que cada uno de ellos pudo tener acceso a los datos personales del otro, según los detalles que constan reseñados en el Hecho Probado Cuarto.

Se trata de una difusión de datos personales para la que la reclamada no dispone de base jurídica que la legitime.

En consecuencia, la documentación obrante en el expediente acredita que la reclamada vulneró el artículo 5 “*Principios relativos al tratamiento*” del RGPD, apartado 1.f), en relación con el artículo 5 “*Deber de confidencialidad*” de la LOPDGDD, al haber remitido un correo electrónico que incorporaba los datos personales identificativos de dos interesados, sus cuentas de correo y, especialmente, los datos del DNI, posibilitando que cada uno de ellos tuviera conocimiento de los datos del otro.

Este deber de confidencialidad, con anterioridad deber de secreto, debe entenderse que tiene como finalidad evitar esas filtraciones de los datos no consentidas por los titulares de los mismos. Se trata de una obligación que incumbe al responsable y encargado del tratamiento, así como a todo aquel que intervenga en cualquier fase del tratamiento; y que es complementaria del deber de secreto profesional.

Frente a este incumplimiento no puede oponerse simplemente, como hace la reclamada en sus alegaciones, la responsabilidad mostrada en el cumplimiento de la normativa de protección de datos personales. Se trata de unos hechos que han quedado debidamente acreditados, cuyo alcance y efecto es el expresado anteriormente.

Debe, igualmente rechazarse la alegación realizada por la reclamada a la propuesta de resolución, cuando señala que los hechos no constituyen una revelación de datos dado el entorno laboral en que se producen; y considerando como probable que ambos compañeros tuvieran conocimiento de los datos personales del otro. No existe ninguna razón legal para que un trabajador pueda tener acceso a los datos personales de otro trabajador por el solo hecho de pertenecer a la misma organización empresarial; ni la organización puede darlos a conocer a los compañeros en base a la mera suposición de que ya son conocidos por éstos.

Por otra parte, es preciso señalar que no es cierto lo indicado por la reclamada en su escrito de alegaciones a la propuesta de resolución al señalar que en esta propuesta se ha considerado que *“el interesado no ha sufrido daño o perjuicio alguno, tanto por los datos afectados como por el marco en el que se compartieron”* y que *“se trata de dos empleados que trabajan juntos y se conocían entre ellos”*. Estas afirmaciones aparecen en el Antecedente Quinto de la propuesta de resolución (también en el presente acto), en el que se extractan las alegaciones formuladas por la entidad interesada. Nada que ver con las circunstancias de hecho y jurídicas valoradas para determinar la infracción o para la graduación de la sanción que se impone.

IV

Para el caso de que concurra una infracción de los preceptos del RGPD, entre los poderes correctivos de los que dispone la Agencia Española de Protección de Datos, como autoridad de control, el artículo 58.2 de dicho Reglamento contempla los siguientes:

“2 Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(...)

b) dirigir a todo responsable o encargado del tratamiento un apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;”

(...)

d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado;

(...)

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;”

Según lo dispuesto en el artículo 83.2 del RGPD, la medida prevista en la letra d) anterior es compatible con la sanción consistente en multa administrativa.

V

En el presente caso, ha quedado acreditado el incumplimiento de lo establecido en el artículo 5.1.f) del RGPD, en relación con el artículo 5 de la LOPDGDD, con el alcance expresado en los Fundamentos de Derecho anteriores, lo que supone la comisión de una infracción tipificada en el artículo 83.5.a) del RGPD, que bajo la rúbrica *“Condiciones generales para la imposición de multas administrativas”* dispone lo siguiente:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9;”.

A este respecto, la LOPDGDD, en su artículo 71 establece que *“Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica”.*

A efectos del plazo de prescripción, el artículo 72 de la LOPDGDD indica:

“Artículo 72. Infracciones consideradas muy graves.

1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

a) El tratamiento de datos personales vulnerando los principios y garantías establecidos en el artículo 5 del Reglamento (UE) 2016/679”.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones del artículo 83, apartados 1 y 2 del RGPD, que señalan:

“1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;

- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*
- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*
- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción”.*

Por su parte, en relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, “Sanciones y medidas correctivas”, establece:

“1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

- a) El carácter continuado de la infracción.*
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.*
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.*
- f) La afectación a los derechos de los menores.*
- g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.*
- h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado”.*

En este caso, considerando las circunstancias concurrentes, se considera procedente la imposición de multa. No cabe aceptar la solicitud formulada por la reclamada para que se impongan otros poderes correctivos, como es el apercibimiento, que está previsto para personas físicas y cuando la sanción constituya una carga desproporcionada (considerando 148 del RGPD).

De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción de

multa a imponer en el presente caso por la infracción tipificada en el artículo 83.5.a) del RGPD, de la que se responsabiliza a la reclamada, se estiman concurrentes en calidad de agravantes los siguientes factores que revelan una mayor antijuridicidad y/o culpabilidad en la conducta de la entidad reclamada:

. La negligencia apreciada en la comisión de la infracción: no se tiene constancia de que la entidad haya obrado dolosamente, aunque la actuación revela una grave falta de diligencia.

En relación con esta circunstancia, entiende la reclamada que la falta de diligencia no puede agravar la sanción, considerando que el artículo 83.2 del RGPD se refiere a intencionalidad o negligencia. A este respecto, esta Agencia entiende que la indicada falta de diligencia expresa una falta de cuidado, asimilable en su definición al concepto de negligencia.

. La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal en el ámbito laboral.

Teniendo en cuenta el número de personas (689) que prestan servicio como empleados de UST GLOBAL, es innegable la vinculación de esta entidad con el tratamiento de datos personales en el ámbito indicado.

. La condición de mediana empresa de la entidad responsable y su volumen de negocio.

Entiende la reclamada que este factor no puede tomarse en consideración al no figurar entre las circunstancias enumeradas en el RGPD o la LOPDGDD. Sin embargo, no tiene en cuenta lo dispuesto en la letra k) del artículo 83.2 del RGPD, que admite la valoración, a efectos de graduar la multa a imponer, de *“cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso”*.

. Las categorías de los datos de carácter personal afectados por la infracción. En contra de lo señalado en la propuesta de resolución, que valora esta circunstancia como una atenuante, esta Agencia viene considerando reiteradamente que la implicación en los hechos de datos identificativos de los interesados debe apreciarse en la graduación de la sanción como un factor agravante.

Asimismo, se aprecian como atenuantes, las circunstancias siguientes:

. La naturaleza, gravedad y duración de la infracción: la infracción resulta de una operación de tratamiento aislada de alcance meramente local.

. La infracción no tiene carácter continuado.

. El escaso volumen de datos y tratamientos que constituye el objeto del expediente.

. El número de interesados, dado que solo se han visto afectados por la conducta infractora dos personas.

. La entidad reclamada ha adoptado medidas para evitar que se produzcan incidencias similares, impartiendo instrucciones a sus unidades y mediante acciones formativas a sus empleados.

. La entidad responsable no ha obtenido beneficios como consecuencia de la comisión de la infracción.

No se estiman como atenuantes la designación de DPD por parte de la reclamada, que no es sino el cumplimiento de una obligación legal; o la forma en que la Agencia ha tenido conocimiento de la infracción, que tuvo lugar mediante reclamación de uno de los afectados por la infracción, y no por comunicación directa del responsable.

Considerando los factores expuestos, especialmente, las medidas tomadas durante la tramitación del procedimiento para evitar incidencias similares, se estima procedente reducir la sanción propuesta e imponer una multa por importe de 3.000 euros.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **UST GLOBAL ESPAÑA, S.A.**, con NIF **A84816644**, por una infracción del artículo 5.1.f) del RGPD, en relación con el artículo 5 de la LOPDGDD, tipificada en el Artículo 83.5 del RGPD, y calificada como muy grave a efectos de prescripción en el artículo 72 de la LOPDGDD, una multa por importe de 3.000 euros (tres mil euros).

SEGUNDO: NOTIFICAR la presente resolución a **UST GLOBAL ESPAÑA, S.A.**

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-131120

Mar España Martí
Directora de la Agencia Española de Protección de Datos