

- **Expediente N°: EXP202205819**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO
VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 14 de febrero de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a **GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L.** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202205819

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: **D. A.A.A.** (en adelante, la parte reclamante), en fecha 18 de mayo de 2022, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L. con NIF B87977005 (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante manifiesta que trabaja en la empresa de seguridad denominada GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S. L.

Los miembros de dicha empresa tienen formado un grupo en la aplicación de WhatsApp, entre los que se encuentra el reclamante.

Indica que realizó un servicio concreto en la garita de seguridad de la empresa, lugar donde se encuentran las cámaras de videovigilancia y que su jefe, solicitó que se subiera a dicho grupo de WhatsApp, el vídeo en el momento en el cual, saltó una alarma de una cámara de seguridad de una vivienda.

El vídeo fue subido por otro trabajador.

En dicho vídeo aparece la imagen de la parte reclamante durante su jornada laboral.

Considera que no se le ha pedido consentimiento para tal difusión y que el vídeo fue difundido con el propósito de vejarse ante el resto de los trabajadores integrantes del grupo de WhatsApp del trabajo.

Aporta imagen del grupo de WhatsApp donde se publicó la grabación, copia de la grabación difundida y denuncia presentada ante la Guardia Civil por los hechos objeto de reclamación.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), mediante notificación electrónica, fue recibido en fecha 27 de mayo de 2022, como consta en el certificado que obra en el expediente.

En fecha 24 de junio de 2022, se recibe en esta Agencia escrito de respuesta indicando:

-Que el responsable del tratamiento y titular de las cámaras de videovigilancia es la Comunidad de Propietarios de A.A.A..

-Que el responsable del Tratamiento y Grupo de Seguridad y Control Global, S.L., como encargado del tratamiento, han formalizado un contrato de prestación de servicios de vigilancia y protección entre las partes y un contrato de encargado de tratamiento de datos personales.

-Que la reclamación y solicitud de información sobre los sistemas de videovigilancia debe dirigirse al responsable del tratamiento: Comunidad de Propietarios de A.A.A..

-Que el pasado 15 de mayo de 2022, sobre las 23:20 horas aproximadamente, el jefe de Seguridad de (...), recibió una llamada desde el centro de control del servicio de vigilancia alertando de la intrusión de varios individuos dentro de una de las viviendas, de la urbanización de A.A.A..

El vigilante que se encontraba en el centro de control en ese momento detectó en las cámaras, como cuatro encapuchados huían de la urbanización y procedió a dar instrucciones tanto a la patrulla de (...) como a la Guardia Civil, donde se produjo un intento de persecución sin suerte en la detención.

- Que el jefe de Seguridad inició una investigación de los hechos dentro de sus funciones, revisando cámaras y coordinando la actuación con la Guardia Civil y los Vigilantes de Seguridad que formaban parte del servicio facilitando a la propia Guardia Civil, toda la información solicitada.

En dicha investigación se solicitó al centro de control que facilitara las imágenes de los hechos acontecidos para coordinar al equipo y tomar las decisiones oportunas a través de la aplicación de mensajería interna en la que los miembros del equipo son coordinados.

A través de dicho Grupo de WhatsApp se solicitaron las imágenes relacionadas con la intrusión para informar a la Guardia Civil de la situación actual y cumplir con sus obligaciones profesionales de colaboración con las Fuerzas y Cuerpos de Seguridad del Estado ante una situación de emergencia y riesgo ante las personas y el inmueble.

-Que los trabajadores de Grupo de Seguridad y Control Global que prestan servicios en esa urbanización se comunican a través de la citada aplicación de mensajería para compartir archivos e información relevante para el servicio y a través de un circuito cerrado de banda privada por walkies profesionales. Todos son conocedores de sus obligaciones y firman un acuerdo de confidencialidad, por lo que conocen que las imágenes y datos personales objeto de tratamiento deben ser tratados de manera totalmente confidencial y con la única finalidad de dar cumplimiento al encargo profesional.

-Indica que en los vídeos se observa un comportamiento inusual del vigilante y reclamante ante la AEPD, por lo que el jefe de Seguridad pone en conocimiento y denuncia a la Delegación Territorial de la Policía Nacional, en concreto del Departamento de Seguridad Privada, los hechos acontecidos para que se investigue si pudiese existir una colaboración o vinculación entre el vigilante y la intrusión acontecida.

El trabajador y reclamante fue posteriormente despedido disciplinariamente. La Policía Nacional acepta la denuncia a trámite y se abren diligencias al respecto que actualmente son objeto de investigación judicial.

- Estima que los motivos de esta reclamación son un intento de represalia por parte del reclamante fruto del despido disciplinario, al incumplir negligentemente sus obligaciones, ausentándose de su puesto de trabajo el día y hora de los hechos y siendo denunciado ante las autoridades.

- En base a lo anterior, expone que la solicitud de las grabaciones a través de la aplicación de mensajería con la finalidad de facilitárselas urgentemente a la Guardia Civil es adecuada, pertinente, proporcional, no excesiva e idónea para garantizar los fines previstos.

TERCERO: En fecha 18 de agosto de 2022, de conformidad con el artículo 65 de la LOPDGDD, se comunica la admisión a trámite de la reclamación presentada por la parte reclamante.

CUARTO: de acuerdo con el informe recogido de la herramienta AXESOR, la entidad GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L es una pequeña empresa, constituida en el año 2017, con un volumen de negocios estimado de *****CANTIDAD. €** en el año 2021.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento, la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: *"Los procedimientos tramitados por la Agencia Española de Protección de Datos se registrarán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."*

II

Obligación incumplida

En el presente caso, se procede a examinar la reclamación presentada, por medio de la cual se traslada el presunto acceso no consentido a las imágenes obtenidas por el sistema de grabación de la Comunidad de Propietarios, siendo objeto, según manifestación de la parte reclamante, de su difusión en un grupo de WhatsApp. Es, por tanto, pertinente analizar si el tratamiento de datos personales llevado a cabo a través de su difusión en un grupo de WhatsApp es acorde con lo establecido en el RGPD.

La imagen física de una persona, a tenor del artículo 4.1 del RGPD, es un dato personal y su protección, por tanto, es objeto de dicho Reglamento, entendiendo por dato de carácter personal: *"toda información sobre una persona física identificada o identificable"*.

Se considera persona física identificable aquella cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

El RGPD define «*encargado del tratamiento*» o «*encargado*» como la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento; Y «*responsable del tratamiento*» o «*responsable*» es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

En el presente caso, la Comunidad de propietarios ostenta la condición de "responsable del tratamiento" (artículo 4 punto 7º RGPD), encomendando a la empresa de seguridad, como encargado del tratamiento, la prestación del servicio de seguridad: vigilancia y protección de la Urbanización de A.A.A..

Para la correcta prestación de dicho servicio, el encargado del tratamiento debe acceder a datos de carácter personal.

En el cumplimiento de la prestación a la que se compromete mediante el contrato de arrendamiento de servicio, la parte reclamada tendrá todas las obligaciones propias establecidas, respetando en todo caso la normativa vigente en materia de protección de datos de carácter personal, así como las restantes normas del ordenamiento jurídico en vigor. Entre ellas, la de que los datos personales sean tratados de tal manera que se garantice una seguridad adecuada de los mismos, 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.

III

Artículo 5.1.f) del RGPD

Establece el artículo 5.1.f) del RGPD lo siguiente:

“Artículo 5 Principios relativos al tratamiento:

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»).”

En relación con este principio, el Considerando 39 del referido RGPD señala que:

“[...]Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento”.

La videovigilancia en una comunidad consiste en la instalación de cámaras en los elementos comunes del edificio que permita mejorar la vigilancia y por tanto la seguridad dentro del mismo. A la hora de su instalación hay que cumplir con las obligaciones recogidas en el Reglamento Europeo de Protección de Datos y la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de Derechos Digitales.

El acceso a las grabaciones de los sistemas de videovigilancia solo puede producirse en los supuestos determinados legalmente y por persona debidamente autorizada en su caso, siendo igualmente “excepcional” la difusión de las imágenes que se hayan obtenido con los mismos, respetando en todo caso la normativa vigente en materia de protección de datos de carácter personal, así como las restantes normas del ordenamiento jurídico en vigor.

En el vídeo anexo a la reclamación, que tiene una duración de 21 segundos, se puede observar la existencia de una cámara instalada en la parte superior pudiéndose visualizar la imagen del interior de la garita con un trabajador en su interior.

La documentación obrante en el expediente ofrece indicios evidentes de que la parte reclamada vulneró el artículo 5.1 del RGPD, *principios relativos al tratamiento*, toda vez que procedió al envío de datos de carácter personal (imágenes) de la parte reclamante a un grupo de personas, vulnerando el principio de confidencialidad, establecido en el citado artículo 5.1.f) del RGPD.

De conformidad con las evidencias de las que se dispone en el presente momento de acuerdo de inicio del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 5.1.f) del RGPD.

IV

Tipificación de la infracción del artículo 5.1.f) del RGPD

De confirmarse, la citada infracción del artículo 5.1.f) del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.5 del RGPD que bajo la rúbrica “*Condiciones generales para la imposición de multas administrativas*” dispone:

“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 “*Infracciones*” 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 “*Infracciones consideradas muy graves*” de la LOPDGDD indica:

“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. (...)*”

V

Artículo 32 del RGPD

Establece el artículo 32 del RGPD, *seguridad del tratamiento*, lo siguiente:

“1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de

probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

- a) la seudonimización y el cifrado de datos personales;*
- b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;*
- c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;*
- d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de 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.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros”.

Los hechos puestos de manifiesto suponen la falta de medidas técnicas y organizativas al enviar datos de carácter personal (imágenes) de la parte reclamante a un grupo de personas sin garantías adecuadas a través de una conocida aplicación de mensajería con la consiguiente falta de diligencia, permitiendo el acceso a dichos datos.

Tal y como consta en el escrito de respuesta de fecha 24 de junio de 2022, los trabajadores de Grupo de Seguridad y Control Global que prestan servicios en la urbanización, se comunican a través de un grupo de WhatsApp para compartir archivos e información relevante para el servicio, a través de un circuito cerrado de banda privada por walkies profesionales. Como quiera que el uso de la citada aplicación de mensajería es habitual para la comunicación y el envío de documentos e imágenes, debe tenerse en cuenta a quien se envían los mensajes cuando en los mismos se incluyan datos personales, dado que debe existir una justificación para enviar datos personales a los miembros de un grupo de WhatsApp. En este caso concreto no se entra a valorar la utilización del medio, es decir, la aplicación de mensajería instantánea, sino el envío de determinada información con datos personales a un grupo de personas.

Y si además la finalidad era la de informar a la Guardia Civil de la situación y cumplir con su obligación profesional de colaboración con las Fuerzas y Cuerpos de Seguridad

del Estado, no era necesario enviar las imágenes a través de un grupo, sino sencillamente pasárselas al jefe de seguridad y éste a las Fuerzas y Cuerpos de Seguridad del Estado.

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico, reduciendo el número de trabajadores con acceso a la información personal, de modo que no se produzcan accesos no necesarios o excesivos por parte de los trabajadores, así como que se evite la reproducción o el reenvío injustificado de los datos personales.

De conformidad con las evidencias de las que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que existen evidencias suficientes respecto de la ausencia de medidas de seguridad adecuadas.

Los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 32 RGPD.

VI

Tipificación de la infracción del artículo 32 del RGPD

De confirmarse, la citada infracción del artículo 32 del RGPD podría suponer la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *“Condiciones generales para la imposición de multas administrativas”* dispone:

“Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

- a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (...)”*

A este respecto, la LOPDGDD, en su artículo 71 *“Infracciones”* 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 73 *“Infracciones consideradas graves”* de la LOPDGDD indica:

“En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

- f) *La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679.”*

VII

Propuesta de sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos 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, 5 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,*
- 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, el artículo 76 “Sanciones y medidas correctivas” de la LOPDGDD dispone:

“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 con 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.”*

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 2.000 € por infracción del artículo 5.1 f) del RGPD, respecto a la vulneración del principio de confidencialidad y de 1.000 € por infracción del artículo 32 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales.

VIII Adopción de medidas

De confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *“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...”*. La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución sancionadora podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L., con NIF B87977005,

- por la presunta infracción del artículo 5.1.f) del RGPD, tipificada conforme a lo dispuesto en el artículo 83.5 del RGPD, calificada como muy grave a efectos de prescripción en el artículo 72.1 a) de la LOPDGDD.

- por la presunta infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave a efectos de prescripción en el artículo 73 f) de la LOPDGDD.

SEGUNDO: NOMBRAR instructor a **B.B.B.** y, como secretario, a **C.C.C.**, indicando que cualquiera de ellos podrá ser recusado, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

TERCERO: INCORPORAR al expediente sancionador, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, la documentación aportada por la parte reclamada, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería, por la supuesta infracción del artículo 5.1.f) del RGPD, tipificada en el artículo 83.5 de dicha norma, multa administrativa de cuantía 2.000,00 euros y por la supuesta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 de dicha norma, multa administrativa de cuantía 1.000,00 euros

QUINTO: NOTIFICAR el presente acuerdo a GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L., con NIF B87977005, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 2.400,00 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en 2.400,00 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en 1.800,00 euros.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (2.400,00 euros o 1.800,00 euros), deberá hacerlo efectivo mediante su ingreso en la cuenta nº **IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección para continuar con el procedimiento en concordancia con la cantidad ingresada.

El procedimiento tendrá una duración máxima de nueve meses a contar desde la fecha del acuerdo de inicio o, en su caso, del proyecto de acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones; de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

935-121222

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

>>

SEGUNDO: En fecha 24 de febrero de 2023, la parte reclamada ha procedido al pago de la sanción en la cuantía de **1800 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO: El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

Asimismo, el artículo 63.2 de la LOPDGDD determina que: "Los procedimientos tramitados por la Agencia Española de Protección de Datos se regirán por lo dispuesto en el Reglamento (UE) 2016/679, en la presente ley orgánica, por las disposiciones reglamentarias dictadas en su desarrollo y, en cuanto no las contradigan, con carácter subsidiario, por las normas generales sobre los procedimientos administrativos."

II

Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos **RESUELVE:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202205819**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a **GRUPO DE SEGURIDAD Y CONTROL GLOBAL, S.L.**

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

936-040822

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