- Expediente N.º: EXP202309054

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 la parte reclamante) con fecha 20/05/2023 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra ATRIUM LEX SFC, S.L. con NIF ***B87634564*** (en adelante la parte reclamada). Los motivos en que basa la reclamación son los siguientes: la parte reclamante manifiesta que la parte reclamada gestiona diversos proyectos inmobiliarios en los que participan distintos inversores, teniendo la parte reclamante la condición de inversor en varios de los proyectos gestionados por la parte reclamada, señalando que, al pedir información de dichos proyectos, se solicita aportar copia del DNI del solicitante, sin que se informe sobre el tratamiento de datos a realizar.

Aporta copia de correos intercambiados con la entidad reclamada en los que la parte reclamante solicita información de varios proyectos gestionados por la parte reclamada y esta solicita que aporte copia de su DNI para verificar su identidad como inversor en dichos proyectos.

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), el 29/06/2023 se dio traslado de dicha reclamación a la parte reclamada/ALIAS, 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, no fue recogido por el responsable, dentro del plazo de puesta a disposición, entendiéndose rechazada conforme a lo previsto en el art. 43.2 de la LPACAP en fecha 10/07/2023, como consta en el certificado que obra en el expediente.

Aunque la notificación se practicó válidamente por medios electrónicos, dándose por efectuado el trámite conforme a lo dispuesto en el artículo 41.5 de la LPACAP, a título informativo se envió una copia por correo postal que fue notificada fehacientemente en fecha 11/07/2023. En dicha notificación, se le recordaba su obligación de relacionarse electrónicamente con la Administración, y se le informaban de los medios de acceso a dichas notificaciones, reiterando que, en lo sucesivo, se le notificaría exclusivamente por medios electrónicos.

El 02/08/2023 la parte reclamada dio respuesta manifestando, en síntesis, lo siguiente: que el reclamante tiene la condición de socio de tres sociedades de las que

la reclamada ostenta la condición de administrador único y por lo tanto en su condición de administrador de la sociedad, conforme a la legislación vigente, son responsable del Libro Registro de Socios de la Entidad.

Que la sociedad como administrador y responsable del Libro Registro de Socios no ha incumplido ningún precepto que afecte a la privacidad de los socios y que reforzará sus procedimientos y procederá a incluir el uso de las herramientas gratuitas facilitadas por la Agencia Española de Protección de Datos.

TERCERO: Con fecha 20/08/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: Con fecha 27/12/2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción de los artículos 13 y 32.1 del RGPD, tipificadas en los artículos 83.5.a) y 83.4.a) del RGPD, con multas de 50.000 € (cincuenta mil euros), cada una de ellas.

QUINTO: Notificado el acuerdo de inicio, con fecha 19/01/2024 la parte reclamada presento escrito de alegaciones formulando en síntesis, las siguientes: que la reclamación efectuada por la parte reclamante tiene su origen en su condición de socio de tres sociedades de las que la reclamada ostenta la condición de administrador único; que el reclamante se dirigió a la reclamada en su condición de inversor, si bien el mismo reconoció que se había equivocado a la hora de decir en que proyectos era inversor, razón que ahondaba aún más en la necesidad de confirmar su identidad; que los hechos declarados en su reclamación por el reclamante son falsos y constitutivos de un posible delito de denuncia falsa; solicita prueba testifical.

SEXTO: Con fecha 03/10/2024 se inició un período de práctica de pruebas, acordándose las siguientes

- Dar por reproducidos a efectos probatorios la reclamación interpuesta por la parte reclamante y su documentación, los documentos obtenidos y generados por los Servicios de Inspección que forman parte del expediente.

- Dar por reproducido a efectos probatorios, las alegaciones al acuerdo de inicio presentadas por la parte reclamada y la documentación que a ellas acompaña.

- Solicitar a la reclamada: la Política de Privacidad o Aviso Legal de la empresa, medidas implantadas para adecuarla al artículo 13, fechas de implantación y controles efectuados para comprobar su eficacia; el Registro de Actividades de Tratamiento y el Análisis de riesgos y evaluación de impacto en el tratamiento de los datos.

Por otra parte, se le comunicaba en relación con la prueba testifical solicitada que la declaración del reclamante acerca de la motivación de la reclamación, que no es competencia de la AEPD el indagar o averiguar los estímulos o razones psicológicos que impulsan a presentar una reclamación o denuncia ante la misma; su competencia se limita a determinar si las conductas pueden ser o no objeto de

reproche por no ser conformes con la normativa sobre protección de datos de carácter personal.

Y en relación con la declaración del administrador de las Sociedades que son objeto del expediente como el careo entre dicha parte y la reclamante, se consideraban impertinentes y no adecuadas a los efectos de la resolución del presente procedimiento sancionador.

- A la parte reclamante se le solicitaba que aportara la documentación que acreditara su condición de inversor y proyectos en los que participa y si se encontraba dado de alta como usuario en la Plataforma de financiación Participativa *Housers Global Properties PFP, S.L.*

En fecha 03/10/20224 la parte reclamante dio respuesta a la prueba practicada cuyo contenido obra en el expediente.

SEPTIMO: En fecha 13/11/2024 fue emitida Propuesta de Resolución en el sentido de que por la Directora de la Agencia Española de Protección de Datos se sancionara a la parte reclamada por infracción de los artículos 13 y 32.1 de la RGPD, con multa de 50.000 € (cincuenta mil euros), cada una de ellas.

Con fecha 10/12/2024, la parte reclamada presento escrito de alegaciones contra la Propuesta de Resolución alegando en síntesis: cual es la posición de la parte reclamada en relación con el tratamiento de los datos personales y de la pretendida vulneración del artículo 13 del RGPD; sobre la pretendida vulneración del artículo 32.1 del RGPD; la vulneración del principio de proporcionalidad; que se dicte resolución acordando el archivo del presente procedimiento.

OCTAVO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO. El 20/05/2023 tiene entrada en la AEPD escrito de reclamación de la parte reclamante en el que manifiesta que la parte reclamada gestiona proyectos inmobiliarios en los que participan distintos inversores, teniendo la parte reclamante la condición de inversor en algunos de los proyectos, señalando que, al solicitar información de los mismos, se le pide aportar copia del DNI, sin que se informe sobre el tratamiento de datos a realizar.

SEGUNDO. Constan aportados correos electrónicos intercambiados entre las partes:

- 28/06/2022
La parte reclamante:
"(…)
Quisiera saber el estado de cuentas y si están o no alquilados y en venta los proyectos de ******PROYECTO.1*** *y* ******PROYECTO.2.***
(...).
(…)"

- 04/07/2022
La parte reclamada
"(…)
Con el fin de poder confirmar que aparece en la base de socios de dicho proyecto, necesitaríamos que nos remitiera el DNI escaneado para poder cotejarlo y facilitarle la información.
(…)"

- 04/07/2022
La parte reclamante:
"(…)
Me equivoqué, en ******PROYECTO.2*** *no tengo participación, quisiera recibir información de* ******PROYECTO.1*** *y* ******PROYECTO.3****, gracias.*
(…)"
- 12/07/2022
La parte reclamante
"(…)
También quisiera conocer el estado del proyecto ******PROYECTO.4*** *y proponer junta parta poner precio de mercado para que no les pague yo el piso a los inquilinos que vivirán muy bien pagando yo varios años.*
(…)"

-13/09/2022
La parte reclamante
"(…)
Soy socio de las empresas que estoy pidiendo documentos desde junio, entiendo que se ha traspapelado y lo remitís de inmediato. Gracias.
(…)"

TERCERO. La parte reclamada en escrito de 02/08/2023 ha manifestado que *"La reclamación efectuada por* el reclamante *tiene su origen en su condición de socio de tres sociedades de las que* la reclamada *ostenta la condición de administrador único y por lo tanto en su condición de administrador de la sociedad, conforme a la legislación vigente, somos responsable del Libro Registro de Socios de la Entidad.*
Ante la solicitud del reclamante es obligación del administrador comprobar la identidad de las personas que solicitan datos en su condición de socios por lo que se solicita que justifique su identidad y así se le ha explicado en el correo electrónico que el mismo reclamante adjunta, donde se le explica el tratamiento del dato que se le pide para cotejo" (el subrayado corresponde a la AEPD).

CUARTO. La parte reclamante en escrito de 04/1/2024 ha aportado información como inversor en determinados proyectos.

QUINTO. La parte reclamada no ha dado respuesta a las pruebas practicadas en las que se le solicitaba que aportara la Política de Privacidad o Aviso Legal y medidas implantadas para adecuarla al artículo 13 del RGPD, controles efectuados para comprobar su eficacia; el RAT y Análisis de riesgos y evaluación de impacto llevados a cabo en el tratamiento de los datos

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
Poderes de la autoridad de control

El artículo 58 del RGPD, *Poderes,* señala:

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

(…)
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;
(…)"

III
Alegaciones a la Propuesta de Resolución

1. La parte reclamada ha alegado sobre la pretendida vulneración del artículo 13 del RGPD.

La parte reclamada en su escrito de alegaciones manifiesta que la parte reclamante ostenta la condición de inversor en determinados proyecto de inversión desarrollados por la entidad *Housers Global Properties PFP. S.L.,* siendo la parte

reclamada administrador de los citados proyectos, por lo que ostenta con relación a la citada entidad la condición de encargado del tratamiento.

No obstante, tales argumentos no pueden aceptarse; hay que señalar que la parte reclamada no ha aportado evidencia alguna que acredite su argumentación.

La citada alegación no se sustenta en elemento probatorio alguno; se limita a señalar que el deber de informar de conformidad con el artículo 13 del RGPD corresponde al responsable del tratamiento, cuestión que por tanto no le atañe al tener la condición de encargado.

El art. 4 del RGPD, Definiciones, en su apartado 8 define al *"encargado del tratamiento" o" encargado*": *"la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento".*

El artículo 28 del RGPD, *Encargado del tratamiento*, establece que:

"1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.

2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:

a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;
b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza legal;
c) tomará todas las medidas necesarias de conformidad con el artículo 32;
d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;

e) asistirá al responsable, teniendo en cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;
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;
g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;
h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.
En relación con lo dispuesto en la letra h) del párrafo primero, el encargado informará inmediatamente al responsable si, en su opinión, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

5. La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refieren los apartados 1 y 4 del presente artículo.

6. Sin perjuicio de que el responsable y el encargado del tratamiento celebren un contrato individual, el contrato u otro acto jurídico a que se refieren los apartados 3 y 4 del presente artículo podrá basarse, total o parcialmente, en las cláusulas contractuales tipo a que se refieren los apartados 7 y 8 del presente artículo, inclusive cuando formen parte de una certificación concedida al responsable o encargado de conformidad con los artículos 42 y 43.

7. La Comisión podrá fijar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.

8. Una autoridad de control podrá adoptar cláusulas contractuales tipo para los asuntos a que se refieren los apartados 3 y 4 del presente artículo, de acuerdo con el mecanismo de coherencia a que se refiere el artículo 63.

9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.

10. Sin perjuicio de lo dispuesto en los artículos 82, 83 y 84, si un encargado del tratamiento infringe el presente Reglamento al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

Y la LOPDGDD en su artículo 33, *Encargado del tratamiento*, establece que:

"(…)
2. Tendrá la consideración de responsable del tratamiento y no la de encargado quien en su propio nombre y sin que conste que actúa por cuenta de otro, establezca relaciones con los afectados aun cuando exista un contrato o acto jurídico con el contenido fijado en el artículo 28.3 del Reglamento (UE) 2016/679. Esta previsión no será aplicable a los encargos de tratamiento efectuados en el marco de la legislación de contratación del sector público.
Tendrá asimismo la consideración de responsable del tratamiento quien figurando como encargado utilizase los datos para sus propias finalidades".

Pues bien, como se señalaba anteriormente no figura documento o evidencia que confirme que la parte reclamada actuaba como encargado del tratamiento de Housers; es más, ni en el requerimiento de información realizado por el inspector actuante ni en las alegaciones posteriores al acuerdo de inicio ha realizado manifestación o alegación en este sentido.

Por otra parte, tanto en fase de actuaciones previas, como en fase probatoria se le requirió para que aportara su *"Política de Privacidad"*, la/s fecha/s de implantación de la misma, medidas implantadas para adecuarla al artículo 13 del RGPD, controles efectuados para comprobar su eficacia, sin que aportara documentación ni diera respuesta alguna a los citados requerimientos.

Esa ausencia de colaboración no parece ser muy compatible con lo señalado en el artículo 5.2 del RGPD, que establece:

"2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»)".

La parte reclamada está obligada a desplegar la actividad adecuada para cumplir los principios de protección de datos y a estar en condiciones de demostrar su cumplimiento.

2. La parte reclamada ha alegado sobre la pretendida vulneración del artículo 32.1 del RGPD

Considera la parte reclamada que la Propuesta de Resolución parte de una premisa falsa ya que no se requirió a la parte reclamante que remitiera la copia del DNI escaneado a través de correo electrónico y, por lo tanto, no puede imputársele la infracción del artículo 32.1 del RGPD ya que en ningún momento hizo referencia ni mención en el citado correo electrónico al canal a través del cual debía remitirse la documentación acreditativa de la identidad y que tan solo se limitó a solicitar la copia del DNI.

Sin embargo, tal argumento no puede ser aceptado; la parte reclamada en su correo de respuesta a la parte reclamante solicitando información sobre los proyectos en los que participaba en la condición de inversor, señala:

"(…)
Con el fin de poder confirmar que aparece en la base de socios de dicho proyecto, necesitaríamos que nos remitiera el DNI escaneado para poder cotejarlo y facilitarle la información.
(…)"

Es cierto que en el citado texto no figura que la remisión de la copia del DNI escaneado sea a través de correo electrónico, aunque tal condición se sobreentiende dado que las comunicaciones entre ambos se estaba llevando a término a través de dicho canal.

Y también es cierto, que si en ningún momento la parte reclamada hizo mención al canal a través del cual la parte reclamante debía remitir la citada documentación (copia escaneada del DNI), habría que entenderlo en el hecho de que el canal utilizado, correo electrónico, era considerado como el valido y veraz, pues de lo contrario habría ofrecido a la parte reclamante otro medio o canal alternativo para efectuarlo y, en este caso, a la vista de la respuesta ofrecida si no le estaba ofreciendo esa oportunidad de remisión por otra vía era porque estaba dando por sentado que la del correo electrónico era la adecuada y pertinente para ello.

Por último, la parte reclamada parece contradecirse pues alegado lo anterior manifiesta que la seguridad de sus comunicaciones se encuentra debidamente aseguradas al tener contratado para la provisión de los servicios de correo electrónico el Servicio Office 365, cuya aplicación de correo electrónico, como describe el CCN, tiene implementadas garantías encaminadas a garantizar la seguridad del correo electrónico, a fin de evitar que pueda verse afectada la integridad del mismo.

Sin embargo, tampoco esto es cierto porque las comunicaciones a través de correo se realizan en *"texto en claro",* lo que significa que si se intercepta la comunicación llevada a cabo se puede tener acceso a los datos remitidos, ya que lo que verdaderamente garantiza Office es que el depósito o almacenamiento de los correos en sus sistemas es seguro porque tiene implantadas medidas de seguridad adecuadas, pero no que las comunicaciones de dichos correos sean seguras.

3. La parte reclamada ha alegado sobre la vulneración del principio de proporcionalidad.

La parte reclamada alega que en el caso de que se considere que ha existido infracción a la normativa de protección de debe particularmente tenerse en consideración en la determinación de la sanción que pudiera imponerse la aplicación del principio de proporcionalidad.

Hay que señalar que el artículo 83.1 del RGPD previene que "*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 disuasoria".*

Las multas por tanto según se deduce del precepto invocado han de ser efectivas, proporcionadas y disuasorias para la consecución de la finalidad pretendida por el RGPD.

Es cierto, que para que dicho sistema funcione con todas sus garantías es necesario que varios elementos se desplieguen de forma íntegra y completa. La aplicación de reglas ajenas al RGPD respecto de la determinación de las multas en cada uno de los Estados miembros aplicando su derecho nacional, ya sea por circunstancias agravantes o atenuantes no previstas en el RGPD -o en la LOPDGDD en el caso español al permitirlo el propio RGPD-, restaría efectividad al sistema que perdería su sentido, su finalidad teleológica, la voluntad del legislador, resultando que las multas impuestas por distintas infracciones dejarían de ser efectivas, proporcionadas y disuasorias. Y de esta forma también se hurtaría a los interesados de la garantía efectiva de sus derechos y libertades, debilitando la aplicación uniforme del RGPD. Se disminuirían los mecanismos de protección de los derechos y las libertades de los ciudadanos y sería contrario con el espíritu del RGPD.

El RGPD está dotado de su propio principio de proporcionalidad que ha de ser aplicado en sus estrictos términos.

En cuanto al principio de proporcionalidad de las sanciones, la Audiencia Nacional en numerosas sentencias ha señalado que el principio de proporcionalidad no puede sustraerse al control jurisdiccional, pues el margen de apreciación que se otorga a la Administración en la imposición de sanciones dentro de los límites legalmente previstos, debe ser desarrollado ponderando en todo caso, las circunstancias concurrentes, al objeto de alcanzar la necesaria y debida proporción entre los hechos imputados y la responsabilidad exigida, dado que toda sanción, debe determinarse en congruencia con la entidad de la infracción cometida y según un criterio de proporcionalidad en relación con las circunstancias del hecho. De modo que la proporcionalidad constituye un principio normativo que se impone a la Administración y que reduce el ámbito de sus potestades sancionadoras.

Pues bien, de conformidad con las circunstancias que concurren en el presente caso, las cuales han sido evaluadas meticulosamente, la presente resolución no vulnera el principio de proporcionalidad en la determinación de las sanciones impuestas, resultando ponderada y proporcionada a la gravedad de las infracciones cometidas, la importancia de los hechos, así como las circunstancias tenidas en cuenta para graduar la sanción, sin que se aprecien razones que justifiquen aún más la minoración efectuada, sobre todo teniendo en cuenta la cuantía a la que pueden

ascender dichas sanciones de conformidad con el artículo 83.5 del RGDP, que prevé para la infracción del artículo 13 del RGDP*, "con multas administrativas de 20.000.000€ 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"* o en el caso del artículo 32.1 del *RGPD* de conformidad con el artículo 83.4 del RGDP *"4. 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".*

- En su escrito de alegaciones la parte reclamada ha manifestado que solicitó y trato los datos del interesado en cumplimiento de unas diligencias de Housers, en nombre y por cuenta de èsta.

Sin embargo, la parte reclamada no ha aportado prueba alguna que evidencie lo alegado, por más que no resulte verosímil que cualquiera vaya solicitando de terceros su copia del DNI, en nombre y por cuenta de otro.

A mayor abundamiento, la parte reclamada que ostenta la condición de administrador único de la sociedad, en el escrito de contestación al acuerdo de inicio de fecha 19/01/2024 manifestaba que: *"Dicho esto, debemos recalcar que ante la solicitud del reclamante, o de cualquier inversor, es obligación del administrador comprobar la identidad de las personas que solicitan datos en su condición de socios o inversores por lo que se solicita que justifique su identidad y así se le ha explicado en el correo electrónico que el mismo reclamante adjunta, donde se le explica el tratamiento del dato que se le pide para cotejo.*

2. Que el reclamante se dirigió a esta entidad en su condición de inversor de los proyectos a los que hace referencia en sus correos, si bien el mismo reconoce que se ha "equivocado" a la hora de decir en que proyectos es inversor, razón que ahonda aún más en la necesidad de confirmar su identidad, …"

Es decir, que la petición de la copia del DNI estaba relacionada con la acreditación de la identidad del reclamante, en su condición de inversor de diferentes proyectos, ante el administrador único de la sociedad.

Y ya se le indicaba en la Propuesta de Resolución que, en un principio, la solicitud de la copia del DNI podía tener una finalidad legítima, puesto que de lo que se trataba era comprobar la condición de inversor de la parte reclamante; sin embargo, no figura que se le informara de conformidad con lo señalado en el artículo 13 del RGPD, es decir, que se le facilitara información alguna en relación con el tratamiento de sus datos de carácter personal.

Y en Considerandos del RGPD se reitera la misma idea. Así, el Considerando 61 indica que *"Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso(...)"*

Y el considerando 62 *"Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, (...)."*

- La parte reclamada ha manifestado que el razonamiento de la AEPD en relación con la apreciación de negligencia en la conducta resulta inadecuado, dado que una cosa en la apreciación de la culpa como requisito para que una determinada conducta pueda ser constitutiva de infracción y otra apreciar que ese elemento debe ser siempre considerado como agravante.

Teniendo en cuenta que en la conducta de la parte reclamada concurre el elemento de culpabilidad, que es indispensable para poder exigir responsabilidad sancionadora, en este caso se concreta, además, en una muy grave falta de diligencia vulnerando la obligación de informar al afectado sobre el tratamiento de sus datos de carácter personal.

Esto, porque no hay ningún elemento que permita concluir que observó alguna mínima diligencia para garantizar el citado principio como consta acreditado y así se recoge en los fundamentos de derecho de la Propuesta de Resolución, en ningún caso desvirtuados.

Hechos que resultan agravados por la ausencia de colaboración con este centro directivo, pues requerida la parte reclamada, tanto en fase de actuaciones previas (en dos ocasiones), como en fase probatoria para que informara sobre las medidas adoptadas para adecuar su *"Política de Privacidad"* al artículo 13 del RGPD, la/s fecha/s de implantación, controles efectuados para comprobar su eficacia, sin que aportara documentación ni diera respuesta alguna a los citados requerimientos.

Además, la falta de diligencia demostrada en la conducta infractora de la que se le responsabiliza debe calificarse de muy grave; la parte reclamada está obligada en virtud del artículo 5.2 del RGPD a desplegar la actividad adecuada para cumplir los principios de protección de datos, por lo que aquí interesa, el de informar, y a estar en condiciones de demostrar su cumplimiento.

- Por último, considera la parte reclamada que la manifestación de la AEPD señalando que *"estamos ante la ausencia de medidas técnicas y organizativas como consecuencia de la ausencia de diligencia en la actuación llevada a cabo",* es infundada ya que no es posible alcanzar dicha conclusión por el hecho de haber solicitado copia del DNI por correo electrónico.

Ya se le indicaba con respecto al DNI que su identificador numérico junto con el carácter de verificación correspondiente al número de identificación fiscal identifica a una persona física de modo indubitado. Esta cualidad lo convierte en un dato particularmente sensible, y este carácter se agrava cuando nos referimos a una copia escaneada del DNI, pues un tercero que tenga acceso al mismo puede suplantar la identidad de su titular con total facilidad, y perpetrar conductas que supongan un alto riesgo para la privacidad, el honor y el patrimonio del suplantado.

La parte reclamada no ha aportado prueba alguna que acredite que tenía implantadas medidas adecuadas dirigidas a eliminar los riesgos del tratamiento del DNI escaneado, sin que haya aportado un medio seguro a la parte reclamante para el

envío de la citada documentación. No consta acreditado que haya realizado un análisis de los riesgos que supone la solicitud del DNI escaneado, a través del correo electrónico, enfocado a la protección de los derechos y libertades de los interesados, ni de las medidas técnicas y organizativas que tuviera implementadas para tratar tales riesgos.

Además, hay que señalar que requerida la parte reclamada para que aportara en periodo probatorio el Registro de Actividades de Tratamiento, Análisis de Riesgos y la Evaluación de Impacto en el tratamiento de los datos, la respuesta es que no hubo respuesta al requerimiento.

Por tanto, de lo que antecede las alegaciones formuladas por la parte reclamada a la Propuesta de Resolución, no pueden ser aceptadas y deben decaer.

IV
Primera obligación incumplida: infracción del artículo 13 del RGPD

Los hechos denunciados se materializan en que la parte reclamante, inversor en algunos de los proyectos gestionados por la parte reclamada, al solicitar información sobre los mismos se le pidió que debía aportar copia escaneada del DNI, sin que se le informara sobre el tratamiento de datos a realizar de conformidad con lo señalado en el artículo 13 del RGPD, lo que podría vulnerar la normativa en materia de protección de datos de carácter personal.

El artículo 13 del RGPD, *Información que deberá facilitarse cuando los datos personales se obtengan del interesado,* establece lo siguiente:

"1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;
b) los datos de contacto del delegado de protección de datos, en su caso;
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses
legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos

personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea

posible, los criterios utilizados para determinar este plazo;

b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;

c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;

d) el derecho a presentar una reclamación ante una autoridad de control;

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitarlos datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;

f) la existencia de decisiones automatizas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

Este precepto, además de determinar en sus apartados 2 y 3 la información que el responsable del tratamiento deberá ofrecer, determina que ésta ha de facilitarse en el momento de la recogida de los datos. No obstante, la previsión del artículo 13, apartados 1 y 2, hay que ponerla en relación con el artículo 13.4 que dispensa de la obligación a la que se refieren ambas disposiciones *"cuando y en la medida en que el interesado ya disponga de la información."*

Los considerandos del RGPD reiteran la misma idea. Así, el considerando 61 indica que *"Se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso(...)" Y el considerando 62 dice que "Sin embargo, no es necesario imponer la obligación de proporcionar información cuando el interesado ya posea la información, (...)."*

En todo caso debe tenerse en cuenta que conforme al considerando 60 incumbe al responsable la obligación de *"facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente,*

habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales".

Por otra parte, los principios recogidos en el artículo 5.1.a) del RGPD, relativos al tratamiento licito, leal y transparente de los datos personales, exigen que se informe al interesado de la existencia del tratamiento y de sus fines y de la información añadida para garantizar un tratamiento leal y transparente. El responsable del tratamiento debe facilitar al interesado cuanta información sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en el que se traten los datos personales.

El considerando 39 del RGPD afirma que: *«El principio de transparencia exige que toda información y comunicación relativa al tratamiento de dichos datos sea fácilmente accesible y fácil de entender, y que se utilice un lenguaje sencillo y claro. Dicho principio se refiere en particular a la información de los interesados sobre la identidad del responsable del tratamiento y los fines del mismo y a la información añadida para garantizar un tratamiento leal y transparente con respecto a las personas físicas afectadas y a su derecho a obtener confirmación y comunicación de los datos personales que les conciernan que sean objeto de tratamiento. Las personas físicas deben tener conocimiento de los riesgos, las normas, las salvaguardias y los derechos relativos al tratamiento de datos personales, así como del modo de hacer valer sus derechos en relación con el tratamiento. En particular, los fines específicos del tratamiento de los datos personales deben ser explícitos y legítimos, y deben determinarse en el momento de su recogida. […]»* .

Por ello, se debe facilitar a los interesados la información sobre el tratamiento de sus datos personales en el momento en que se obtengan de ellos o, si se obtienen de otra fuente, en un plazo razonable, dependiendo de las circunstancias del caso.

Cuando se obtengan del interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, debe facilitarle toda la información sobre el tratamiento de sus datos tal como se indica en el artículo 13 del RGPD.

En el presente caso, como consta en los correos intercambiados, la parte reclamante, inversor en determinados proyectos gestionados por la parte reclamada y ante la solicitud de aquel para que se le aportara información acerca de los mismos, le pidió que aportara copia escaneada del DNI y aunque en un principio parece una solicitud con una finalidad legítima, como era comprobar la condición de inversor del solicitante de la información, sin embargo, no figura que se le informara de conformidad con lo señalado en el artículo 13 del RGPD, es decir, que se le facilitara información alguna relativa al tratamiento de los datos de su DNI.

Es más, requerida la parte reclamada, en fase de actuaciones (en dos ocasiones), para que informara sobre las medidas adoptadas para adecuar su *"Política de Privacidad"* al artículo 13 del RGPD, fechas de implantación y controles efectuados para comprobar su eficacia, sin que aportara documentación alguna.

Y en fase probatoria se requirió nuevamente para que aportara la Política de Privacidad o Aviso Legal de la empresa, las medidas pertinentes para su adecuación de conformidad con el artículo 13, sin que tampoco se diera respuesta a la misma.

Dicha conducta se considera que vulnera el artículo 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD.

V

Tipificación de la infracción del articulo 13 RGPD

La infracción del artículo 13 del RGPD, está tipificada en el artículo 83.5.b) del RGPD que 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% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*

(...)
b) los derechos de los interesados a tenor de los artículos 12 a 22; (...)"
(…)"

A efectos de prescripción, la LOPDGDD califica esta conducta en el artículo 72.1.h) de infracción muy grave y fija para ella un plazo de prescripción de tres años. El precepto dispone:

"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:

(...)
h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."
(...)"

VI

Segunda obligación incumplida: infracción del artículo 32.1 del RGPD

En segundo lugar, el artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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".

1. El RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, derivado de la ausencia de diligencia al no adoptar medidas técnicas y organizativas adecuadas que garanticen un nivel de seguridad adecuado al riesgo del tratamiento, como consecuencia de la solicitud de copia escaneada del DNI por correo electrónico para acreditar la identidad de socio, forma o método no muy seguro de solicitar este tipo de documentación.

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un

incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como 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, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

2. En el caso analizado, tal y como consta en los hechos la AEPD trasladó al reclamado la reclamación presentada para su análisis solicitando la aportación de información relacionada con la incidencia reclamada.

El reclamado en su escrito de 02/08/2023 manifestaba que *"Ante la solicitud del reclamante es obligación del administrador comprobar la identidad de las personas que solicitan datos en su condición de socios por lo que se solicita que justifique su identidad y así se le ha explicado en el correo electrónico que el mismo reclamante adjunta, donde se le explica el tratamiento del dato que se le pide para cotejo".*

Como se señalaba en el acuerdo de inicio el Libro Registro es un listado que recoge los nombres de los que son socios de una sociedad anónima o limitada en cada momento y corresponde a los administradores de la sociedad su llevanza permitiéndole saber a quién tiene que considerar socio en cada momento a efectos, a modo de ejemplo, de permitirle participar en las reuniones sociales, pagarle un dividendo, etc. Por eso se dice que el libro-registro tiene una función de legitimación.

Ahora bien, no parece que el método utilizado de solicitar copia del DNI escaneada a través de correo electrónico sea un método muy seguro de solicitar la identidad del socio solicitante de la información, a la vista de los riesgos que puede provocar.

Sobre este particular conviene recordar que los considerandos 51 y 75 del RGPD distinguen un grupo de datos personales que por su naturaleza son particularmente *"sensibles"* por el importante riesgo que puede entrañar su tratamiento

para los derechos y libertades fundamentales. Su denominador común es el riesgo que comporta para los derechos y las libertades fundamentales, pues su tratamiento puede llegar a provocar daños y perjuicios físicos, materiales o inmateriales.

Se incluyen en este grupo o categoría los datos especialmente protegidos que regula el artículo 9 del RGPD -considerando 51 del RGPD- y, además, otros muchos que no se citan en ese precepto. El considerando 75 menciona con detalle los datos personales cuyo tratamiento puede entrañar un riesgo de gravedad y probabilidad variables para los derechos y libertades de las personas físicas como consecuencia de que pueden provocar daños y perjuicios físicos, materiales o inmateriales. Entre ellos se refiere a aquellos cuyo tratamiento "pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo;"

El identificador numérico del DNI junto con el carácter de verificación correspondiente al número de identificación fiscal identifica a una persona física de modo indubitado. Esta cualidad lo convierte en un dato particularmente sensible, y este carácter se agrava cuando nos referimos a una copia escaneada del DNI, pues un tercero que tenga acceso al mismo puede suplantar la identidad de su titular con total facilidad, y perpetrar conductas que supongan un alto riesgo para la privacidad, el honor y el patrimonio del suplantado.

La parte reclamada debió adoptar las medidas técnicas y organizativas adecuadas encaminadas a paliar los riesgos del tratamiento del DNI escaneado, previo análisis de dichos riesgos, ofreciendo un medio seguro a la parte reclamante para el envío de la documentación. Sin embargo no ha acreditado que haya realizado un análisis de los riesgos que supone la solicitud del DNI escaneado, a través del correo electrónico, enfocado a la protección de los derechos y libertades de los interesados, ni de las medidas técnicas y organizativas que tuviera implementadas para tratar tales riesgos

La responsabilidad del reclamado viene determinada por la ausencia de medidas adecuadas puestas de manifiesto, 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, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

Se cuestiona por tanto que el correo electrónico constituya una vía segura para el envío de documentación, como en el presente caso la copia escaneada del DNI, cuando debe garantizarse la seguridad. Se considera que el envío de la información solicitada mediante un simple correo electrónico no es una medida adecuada en función del riesgo para los derechos y libertades de las personas físicas por el uso descuidado que pudiera hacerse del correo, por lo que la parte reclamada debería de hacer adoptado medidas de seguridad apropiadas en función del riesgo para proteger los derechos y libertades de la parte reclamante en relación con el tratamiento de los datos objeto del presente procedimiento

De conformidad con lo que antecede, se estima que el reclamado sería responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

VII
Tipificación de la infracción del artículo 32.1 del RGPD

La vulneración del artículo 32 del RGPD se encuentra tipificada en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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.
(…)"

Por su parte, la LOPDGDD en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

"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:

(…)
g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679. (…)"
(…)"

VIII
Sanción por incumplimiento de las infracción cometidas

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 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, 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, 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".

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76*, "Sanciones y medidas correctivas",* establece que:

"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."

- 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 del artículo 13 del RGPD, tipificada en el artículo 83.5.a) del RGPD de la que se responsabiliza al reclamado, se estiman concurrentes los siguientes factores:

La naturaleza y gravedad de la infracción pues no hay que olvidar que estamos ante la vulneración de la omisión del deber de informar al afectado acerca del tratamiento de sus datos personales cuyo reproche se hace en el RGPD con la mayor gravedad; la parte reclamante no ha aportado elemento probatorio que acredite que había adoptado medidas para adecuar el tratamiento a lo establecido en el artículo 13, su fecha de implantación, controles para comprobar su eficacia sobre el tratamiento de los datos de la parte reclamante, etc. (artículo 83.2.a) del RGPD).

El grado de cooperación con la autoridad de control con el fin de poner remedio y mitigar los posibles efectos adversos de la infracción; requerido en fase de investigación (en dos ocasiones) y en fase probatoria para que aportara información sobare la Política de Privacidad o Aviso legal la parte reclamada no dio respuesta en ningún momento a los requerimientos efectuados (artículo 83.2.a) del RGPD).

La intencionalidad o negligencia en la infracción; se observa una grave falta de diligencia en la actuación de la entidad derivado sobre el tratamiento de los datos del reclamante. Conectado también con el grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la SAN de 17/10/2007, que después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...). el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto"* (artículo 83.2. b) del RGPD).

La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros. El reclamado, dada la naturaleza de su actividad le resulta imprescindible el tratamiento de datos de carácter personal de clientes como de terceros por lo que la transcendencia de su conducta objeto del presente procedimiento es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

Con arreglo a las citadas circunstancias se considera adecuado establecer una sanción de 50.000 euros.

- 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 del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD de la que se responsabiliza al reclamado, se estiman concurrentes los siguientes factores:

La naturaleza y gravedad de la infracción pues la parte reclamante muestra ausencia de medidas técnicas y organizativas provocando una ausencia de diligencia en la conducta desarrollada y cuyo reproche se hace en el RGPD con la categoría de grave, considerándose que las entidades que por su actividad tratan datos personales deben adecuarse a los requisitos contenidos en la norma y adoptar la diligencia debida en la aplicación de medidas adecuadas al riesgo del tratamiento para los derechos y libertades de los interesados. La parte reclamada no ha aportado elementos probatorio alguno que acredite que tenía implantadas medidas de seguridad adecuadas al riesgo que conlleve el tratamiento de los datos de la parte reclamante, solicitando copia escaneada del DNI por correo electrónico, sin acreditar medidas (artículo 83.2.a) del RGPD).

El grado de cooperación con la autoridad de control con el fin de poner remedio y mitigar los posibles efectos adversos de la infracción; así, requerida en fase probatoria para que aportara el RAT, Análisis de riesgos y evaluación de impacto llevados a cabo en el tratamiento de los datos, la parte reclamada no dio respuesta en ningún momento a dicho requerimiento (artículo 83.2.a) del RGPD).

La intencionalidad o negligencia en la infracción; se observa una grave falta de diligencia en la actuación de la entidad derivado de la ausencia de medidas en relación con el método utilizado para verificar la identidad. Conectado también con el grado de diligencia que el responsable del tratamiento está obligado a desplegar en el cumplimiento de las obligaciones que le impone la normativa de protección de datos puede citarse la SAN de 17/10/2007, que después de aludir a que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisaba que *"(...). el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto"* (artículo 83.2. b) del RGPD).

La actividad de la entidad presuntamente infractora está vinculada con el tratamiento de datos tanto de clientes como de terceros. El reclamado, dada la naturaleza de su actividad le resulta imprescindible el tratamiento de datos de carácter personal de clientes como de terceros por lo que la transcendencia de su conducta objeto del presente procedimiento es innegable (artículo 76.2.b) de la LOPDGDD en relación con el artículo 83.2.k).

Con arreglo a las citadas circunstancias se considera adecuado establecer una sanción de 50.000 euros.

IX
Adopción de medidas

Los poderes correctivos que el RGPD atribuye a la AEPD como autoridad de control se relacionan en su artículo 58.2, apartados a) a j).

En este caso, procede ordenar 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.

Por tanto, se considera procedente ordenar al reclamado que en el plazo de seis meses a partir de la firmeza de la resolución sancionadora que, en su caso, se dicte adecúe los tratamientos objeto del presente procedimiento a la normativa aplicable. En el texto de esta resolución se establecen cuáles han sido los hechos que han dado lugar a la vulneración de la normativa de protección de datos, de lo que se infiere con claridad cuáles serían las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte reclamada, pues es quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD, entre ellas medidas que garantice el cumplimiento de lo señalado en el artículo 13 y 32.1 del RGPD y que impidan una nueva vulneración.

Se advierte que no atender la orden impuesta por este organismo 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, 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 ATRIUM LEX SFC, S.L., con NIF ***B87634564***,

- Por una infracción del artículo 13 del RGPD tipificada en el artículo 83.5.a) del RGPD, una multa de 50.000 € (cincuenta mil euros).
- Por una infracción del artículo 32.1 del RGPD tipificada en el artículo 83.4.a) del RGPD, una multa de 50.000 € (cincuenta mil euros).

SEGUNDO: ORDENAR a ATRIUM LEX SFC, S.L., con NIF ***B87634564***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de seis meses desde que la presente resolución sea firme y ejecutiva, acredite haber procedido al cumplimiento de las medidas que garantice el cumplimiento de lo señalado en el artículo 13 y 32.1 del RGPD

TERCERO: NOTIFICAR la presente resolución a ATRIUM LEX SFC, S.L. con NIF ***B87634564.***

CUARTO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la

notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte 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 ***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.. 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.

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