- **Expediente N.º: EXP202100318**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha 2 de julio de 2021, la Subdirección General de Inspección de Datos (SGID) recibió para su valoración un escrito de notificación de brecha de seguridad de los datos personales remitido por AFIANZA ASESORES, S.L con NIF B83117804 (en adelante, AFIANZA), recibido en fecha 30 de junio de 2021 en el que informa a la Agencia Española de Protección de Datos de lo siguiente:

(…)

SEGUNDO: A tenor de lo previsto en los artículos 34.4 del RGPD y a la vista de que la brecha afecta a la confidencialidad de datos personales ***(…)***, lo que puede suponer un riesgo alto para los derechos y libertades de las personas afectadas, con fecha 2 de julio de 2021, se ordena, por la Directora, a AFIANZA que lleve a cabo la comunicación de la mencionada brecha de datos personales a los interesados, sin dilación indebida, para que, una vez tengan conocimiento de esta, puedan adoptar las medidas que consideren oportunas para evitar aquellos riesgos que pudieran afectar a su persona, de conformidad con lo previsto en el artículo 34 del RGPD.

Asimismo, se le requiere confirmación del cumplimiento de la orden de comunicación a los afectados en el plazo máximo de 30 días

TERCERO: Con fecha 2 de julio de 2021, se ordena por la Directora a la Subdirección General de Inspección de Datos que valore la necesidad de realizar las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

CUARTO: Mediante escrito presentado el 8 de julio de 2021, AFIANZA indica que ha procedido a solicitar al ******JUZGADO.1***, que se proporcione información sobre la brecha de seguridad sufrida a todas las personas cuyos datos personales aparecen ***(…).***

QUINTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

Fecha de notificación de la brecha de seguridad de datos personales (en adelante brecha): 30 de junio DE 2021, por parte del AFIANZA ASESORES, S.L., responsable del tratamiento.

Fecha de detección de brecha: 17/06/2021
Fecha de inicio de la brecha: 17/06/2021.
Fecha resolución brecha: 17/06/2021.
Modo detección brecha: Empleados de la entidad responsable.
Brecha de confidencialidad

Resumen de la notificación:

(…)

Durante las presentes actuaciones se han investigado las siguientes entidades:

AFIANZA ASESORES, S.L, con NIF B83117804 y domicilio en c/ Alfonso XII, 20, 1ª Planta - 28014 MADRID

La entidad responsable manifiesta que, por culpa de un error al comunicar la incidencia, se ha comunicado como nombre de la empresa AFIANZA AUDITORES, S.L., cuando, en realidad, el nombre de la sociedad es AFIANZA ASESORES, S.L. Se trata de un mero error tipográfico, que afecta solo al nombre, siendo correctos el NIF y el domicilio que se han comunicado en el incidente de AFIANZA ASESORES, S.L.,

Respecto de la comunicación a los afectados:

Con fecha 2 de julio de 2021, la Directora de la Agencia Española de Protección de Datos firma resolución ordenando la comunicación de la brecha a los interesados sin dilación indebida.

(…)

1.- Se ha solicitado información y documentación a la entidad notificante, y de la respuesta recibida se desprende lo siguiente:

(…)

SEXTO: Con fecha 24 de junio de 2022**,** la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, con arreglo a lo dispuesto en los artículos 63 y 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), por la presunta infracción del Artículo 5.1.f) del RGPD y Artículo 32 del RGPD, tipificadas respectivamente en el Artículo 83.5 del RGPD y Artículo 83.4 del RGPD.

SÉPTIMO: Notificado el citado acuerdo de inicio 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), con fecha 14 de julio de 2022 AFIANZA presentó, en tiempo y forma, escrito de alegaciones en el que, en síntesis, manifiesta lo siguiente:

I. BRECHA DE SEGURIDAD

Señala Afianza que el artículo 4.12) del Reglamento General de Protección de Datos (en adelante, "RGPD") define la «violación de la seguridad de los datos personales», como toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

Indica además que la Guía para la notificación de brechas de datos personales de la AEPD, establece tres tipologías de brechas, indicando que afecta a la confidencialidad, *cuando produce una revelación no autorizada o accidental de los datos personales, o su acceso*.

A continuación, indica que esta Autoridad de Control, en su Acuerdo de inicio de procedimiento sancionador manifiesta que AFIANZA ha sufrido una brecha de confidencialidad, es decir, bajo el criterio de la AEPD, se ha producido una revelación no autorizada o accidental de los datos personales, o su acceso.

Señala AFIANZA que, si se atiende a los hechos probados y manifestados, la única certeza es que ha habido un robo de una mochila, en la que, además de documentación personal, había un USB con información bajo el control de AFIANZA como responsable del tratamiento. Si bien, un año después, no existe ninguna prueba que acredite que algún tercero ha accedido a la información contenida en ese USB, por lo que el "acceso" o la "revelación accidental" quedan en meras suposiciones.

AFIANZA puso en conocimiento de la AEPD el hecho delictivo actuando de forma diligente y en pro de su responsabilidad proactiva. En ningún caso, ni en el momento de la notificación, ni ahora (un año después) se ha comprobado el tratamiento ulterior por parte de terceros de la información contenida en el USB.

Por tanto, concluye que ni AFIANZA, ni la AEPD, ni ningún otro tercero tienen capacidad para probar que, a día de hoy, se ha producido un "acceso indebido" o una "revelación accidental" a la información contenida en el USB, constando, únicamente, el robo de una mochila, donde dentro había un USB, por lo que, afirmar con total rotundidad que se ha producido una brecha de confidencialidad resulta totalmente desproporcionado en relación a los hechos probados.

II. MEDIDAS DE SEGURIDAD IMPLEMENTADAS POR AFIANZA

Sin detrimento de lo anterior, y en el supuesto en el que esta Autoridad de Control entienda que se ha producido una brecha de seguridad, AFIANZA quiere poner de manifiesto las medidas de seguridad que tiene implementadas, en tanto que en el Acuerdo de inicio de procedimiento Sancionador, la AEPD sostiene que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa (…), ya que es necesario analizar la diligencia de responsables y

encargados y las medidas de seguridad aplicadas. En este sentido, AFIANZA manifiesta, lo siguiente:

I. En el año 2018, con la directa aplicación del Reglamento General de Protección de Datos y, posteriormente, con la entrada en vigor de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, AFIANZA, llevó a cabo un procedimiento de adecuación de la compañía al nuevo marco jurídico e implementó las medidas de seguridad tanto técnicas como organizativas asociadas a cada uno de los tratamientos realizados y recogidos en su Registro de Actividades de Tratamiento (Anexo II)

II. Todo el personal de AFIANZA que accede a datos personales ha recibido formación y tiene conocimiento de sus obligaciones con relación a los tratamientos de datos personales (Anexo III)

III. Se ha realizado Auditoría IT en la que se ha analizado el nivel de cumplimiento técnico de los tratamientos de datos personales que son llevados a cabo bajo la responsabilidad de AFIANZA, verificando el grado de adecuación de AFIANZA a las medidas y controles dispuestos a la normativa en materia de protección de datos personales, y normativa de seguridad asociada (Anexo IV)

IV. En AFIANZA se han implementados todas las medidas posibles para que no accedan personas no autorizadas a los datos personales, a tal fin:

(…)

Señala AFIANZA que, tal y como pone de manifiesto el considerando 83 del RGPD, a fin de mantener la seguridad y evitar infracciones, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos. 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, y ello es justamente lo que ha venido haciendo AFIANZA desde la directa aplicación del RGPD.

Indica ALIANZA que el artículo 32 no regula un listado de las medidas de seguridad que sean de aplicación, 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, por lo que, hacer pivotar el argumento sancionador en la falta del cifrado del USB robado, no resulta apropiado, porque

> (i) no es una medida de seguridad obligatoria y
> (ii) no se tienen en consideración ninguna de las medidas de seguridad implementadas por AFIANZA y previamente comunicadas.

A tenor de lo expuesto, AFIANZA entiende que trata los datos personales de manera que se garantiza 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 las medidas técnicas u organizativas indicadas.

Por lo expuesto, considera AFIANZA que ha quedado probado que cumple con todos y cada uno de los principios relativos al tratamiento del RGPD, especialmente con el principio de confidencialidad, del mismo modo que ha cumplido con su obligación de implementación de la seguridad en todos y cada uno de los tratamientos de datos que realiza, indicando que esta Autoridad de Control debe saber que la seguridad no es inexpugnable, y por ello, la normativa pone en valor las medidas de seguridad que se adoptan para que, en caso de producirse un incidente de seguridad, este tenga las mínimas consecuencias posibles. No se puede responsabilizar a AFIANZA por haber sido víctima de un hecho delictivo, al igual que tampoco se le puede responsabilizar por la vulneración de un tercero de las medidas de seguridad implementadas. Del mismo modo, la AEPD tampoco puede garantizar ni probar que ha habido una vulneración en los derechos y libertades de terceros.

III. PLAZO DE NOTIFICACIÓN DE LA BRECHA DE SEGURIDAD

Señala AFIANZA que el artículo 33 del RGPD, recoge que, en caso de violación de la seguridad de los datos personales, el responsable del tratamiento lo notificará a la Autoridad de Control competente sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

En este sentido, entiende AFIANZA que es importante recordar que en los 13 días que pasaron desde el robo del USB hasta que se notificó a la AEPD, AFIANZA presentó la correspondiente denuncia y en pro de su responsabilidad proactiva, inició un procedimiento de investigación interna con el fin de averiguar y valorar los posibles daños derivados del robo de la mochila. ***(…)***. Además de lo anterior, se realizó y envió comunicaciones a la comunidad de propietarios información del hecho delictivo. Es decir, sostiene AFIANZA que actuó proactiva y diligentemente los días posteriores a la realización del robo y que no hubo una dilación indebida, pues la norma refiere expresamente “y de ser posible, a más tardar, 72 horas”, no siendo un plazo imperativo.

Entiende AFIANZA que, del Acuerdo de la AEPD parece inferirse una crítica por el tiempo que trascurrió entre el robo y la notificación, sin poner en valor la justificación que dio lugar a la dilación, así como tampoco, la realización de la propia notificación. Cualquier otro responsable del tratamiento podría haber optado por no haber comunicado nunca a la AEPD el hecho delictivo, sin embargo, AFIANZA cumpliendo con su diligencia debida, así como con su Protocolo interno, lo informó a la AEPD tan pronto cuanto tuvo la valoración del posible daño suscitado, no habiéndose producido en ningún caso un mayor riesgo o una mayor difusión de los datos.

Pone AFIANZA de relieve que, más de un año después de la fecha del robo, no ha habido publicación o cualquier otro uso indebido de la información contenida en el USB, por lo que la brecha de seguridad a los efectos jurídicos indicados en el RGPD

no se ha materializado en tanto, como ya se ha informado, ni AFIANZA, ni la AEPD, ni ningún otro tercero tienen capacidad para probar que se ha producido un acceso indebido a la información contenida en el USB, constando, únicamente, el robo de una mochila, donde dentro había un USB, lo que prueba que el plazo de los 13 días trascurridos desde el robo hasta la notificación, no han supuesto una merma en los derechos de terceros.

IV. AGRAVANTES

Recuerda AFIANZA que en el Acuerdo de inicio del procedimiento sancionador se propone sancionarla por:

- Infracción del artículo 5.1.f) RGPD una sanción de 100.000€
- Infracción del artículo 32 RGPD una sanción de 60.000€

Y que ambas infracciones se ven agravadas por:

- Art. 83.2.b) RGPD intencionalidad o negligencia en la infracción. Según la AEPD, si bien no se aprecia intencionalidad, sí se observa negligencia porque “se produjo un almacenamiento de datos personales en un dispositivo extraíble sin estar cifrado”.

En este punto, reitera AFIANZA lo manifestado en el apartado relativo a las “Medidas de Seguridad implementadas”, entendiendo que, hacer pivotar el argumento sancionador en la falta del cifrado del USB robado, no resulta apropiado, porque:

- no es una medida de seguridad obligatoria y
- no se han tenido en consideración ninguna de las medidas de seguridad implementadas por AFIANZA

Por ello, sostiene AFIANZA que no se puede cuestionar la diligencia en el cuidado de la protección de los datos de carácter personal de los que es responsable, únicamente, por no tener cifrado un USB que ha sido robado, cuando existen y existían otras tantas medidas de seguridad.

Asimismo, continúa alegando que, según lo previsto en los artículos 1.104, 1.101 y 1.089 del Código Civil, y la doctrina que los interpreta, la “negligencia” es la omisión de aquella diligencia que exija la naturaleza de la obligación y corresponde a las circunstancias de las personas, del tiempo y del lugar. El reproche legal es la falta de un comportamiento propio y adecuado de una persona medianamente responsable, de acuerdo con las circunstancias del caso concreto. Hay también sentencias que califican la negligencia como “descuido” actuación contraria al deber objetivo de respeto y cuidado del bien jurídico protegido por la norma, incluyendo aquí el “desprecio” o “menoscabo” de los deberes de vigilancia o cuidado.

Es importante no olvidar en qué circunstancia se producen los hechos, y es que el extravío del USB ocurre durante un delito de robo con fuerza en las cosas, previsto en el artículo 237 del Código Penal. Si no hubiere acontecido el delito nadie habría podido acceder al USB. No estamos ante un descuido o negligencia, puesto que había medidas de seguridad (importante, recordar que la ubicación del soporte USB estaba dentro de una mochila, en una estantería de un despacho particular, a su vez ubicado

en unas oficinas a las que solo se puede entrar tras traspasar dos puertas generales en la entrada del edificio, una más de acceso a AFIANZA, transitar por un pasillo de veinte metros y finalmente abrir y entrar en ese despacho).

- Art. 83.2.c) RGPD cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.

Manifiesta AFIANZA que, según esta Autoridad de Control "no consta que AFIANZA reaccionara lo más rápido posible y procediera a tomar medidas necesarias para paliar los efectos y el riesgo", sin embargo, desde la notificación de la brecha de seguridad, la AEPD tiene en su poder la denuncia presentada por AFIANZA cuando ni siquiera habían trascurrido 24 horas desde el robo. La forma más útil para paliar los efectos de un delito es denunciarlos, y eso es justamente lo que hizo AFIANZA. Ello sin detrimento de la activación de las medidas de seguridad pertinentes, el envío de comunicaciones a la comunidad de propietarios, así como, la propia notificación a la AEPD.

Además de lo anterior, recuerda AFIANZA que, con fecha 2 de julio de 2021, la Directora de la AEPD le requiere la comunicación de la brecha a los interesados, comunicación que AFIANZA realiza a través de la Audiencia Nacional e informa a la AEPD con fecha 8 de julio de 2021. Cuestión que tampoco se ha puesto en valor por parte de esta Autoridad de Control.

Reitera que, más de un año después, no ha habido daño o/y perjuicio sufrido por ningún interesado, por lo que agravar una infracción con este argumento resulta del todo desproporcionado.

- Art. 83.2.g) RGPD las categorías de los datos de carácter personal afectados por la infracción.

Señala AFIANZA que la AEPD establece este agravante por entender que en el USB había datos "relativos a infracciones y sanciones penales", si bien, ***(...)***, incluía las diligencias previas del procedimiento, es decir, la información era relativa al proceso de investigación, no habiendo sanciones penales en el mismo.

V. ATENUANTES

Alega AFIANZA que, si bien la AEPD ha acordado incluir los agravantes indicados en el punto anterior en ambas infracciones, no ha tomado en consideración ninguno de los posibles atenuantes que pudieran ser aplicación al caso:

- Art. 83.2.a) RGPD la naturaleza, gravedad y duración de la infracción. La supuesta brecha de confidencialidad se desarrolla en el contexto de un delito realizado por un tercero ajeno a la organización, burlando las medidas de seguridad establecidas. Además, como se ha venido reiterando no existe constancia alguna de que algún tercero haya hecho un uso de la información contenida en el USB, por lo que la gravedad del acceso desde la óptica de la protección de datos es inexistente.

- Art. 83.2.c) RGPD cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados y el Art.83.2.

f) RGPD, 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. Como se indicó en el apartado anterior, la AEPD ha utilizado este argumento como agravante, si bien, ambos preceptos deberían ser tomados en consideración dada la actitud proactiva que ha demostrado AFIANZA en todo momento, no sólo colaborativa con la AEPD (facilitando la información adicional, informando sobre las comunicaciones a los afectados…), sino también con los afectados.

- Art. 83.2.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. La AEPD jamás hubiera tenido constancia del hecho, de no haber sido porque AFIANZA, en pro del cumplimiento de su responsabilidad proactiva, lo comunicó directamente. El tiempo transcurrido ha demostrado que, si AFIANZA no lo hubiera notificado, la AEPD nunca hubiera sido conocedora del hecho, en tanto, no ha habido nadie que haya visto mermados sus libertades o derechos por este suceso.

- Art. 83.2.k) cualquier otro factor atenuante aplicable a las circunstancias del caso, aplicados por la AEPD en otros procedimientos, tales como:

> -El alcance inexistente del daño. Ninguna persona física ha visto mermados sus derechos y libertades.
> -AFIANZA ha adoptado medidas para evitar que se produzcan incidencias similares.
> -AFIANZA ha respondido al requerimiento informativo de la Agencia, lo que incide en la cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la misma.
> -No se tiene constancia de que AFIANZA hubiera obrado dolosamente ni tampoco con falta de diligencia.
> -AFIANZA es una pequeña empresa.

VI. NO CONCURRENCIA DEL PRINCIPIO DE CULPABILIDAD

Alega AFIANZA que los hechos acaecidos implicarían un resultado no perseguido por ella, en tanto fue motivado por la comisión de un hecho delictivo de un tercero totalmente ajeno al responsable del tratamiento y a su personal y que hay de tener en cuenta que, como pone de manifiesto la Audiencia Nacional, y en la medida en que:

> (i) no concurre voluntariedad en el acto,
> (ii) no se ha producido un resultado especialmente lesivo,
> (iii) no consta la falta de cuidado en la actuación de AFIANZA en sus actividades y funciones,

Sería contrario a la naturaleza del ámbito sancionador administrativo, sujeto a los principios de intervención mínima y proporcionalidad, imponer una sanción al respecto del hecho acaecido, no merecedor de actuación sancionadora al no concurrir el elemento de la culpabilidad.

Indica AFIANZA que la Sentencia de la Audiencia Nacional de 14 de diciembre de 2006, recurso nº 1363/2005, señala en sus Fundamentos Jurídicos lo siguiente: “La resolución del presente recurso pasa por recordar, en primer lugar, que la culpabilidad

es un elemento indispensable para la sanción que se le ha impuesto a la actora, tal como lo prescribe el artículo 130.1 de la Ley 30/1.992 de 26 de noviembre , que establece que sólo pueden ser sancionados por hechos constitutivos de infracción administrativa los responsables de los mismos, aún a título de simple inobservancia."

Por tanto, alega que lo comunicado por parte de AFIANZA, no puede ser motivo que rija la responsabilidad objetiva para establecer sanción en el marco del derecho administrativo. Efectivamente, en materia sancionadora rige el principio de culpabilidad (SsTC 15/1999, de 4 de julio; 76/1990, de 26 de abril; y 246/1991, de 19 de diciembre), lo que significa que ha de concurrir alguna clase de dolo o culpa.

Como dice la sentencia del Tribunal Supremo de 23 de enero de 1998 , "...*puede hablarse de una decidida línea jurisprudencial que rechaza en el ámbito sancionador de la Administración la responsabilidad objetiva, exigiéndose la concurrencia de dolo o culpa, en línea con la interpretación de la STC 76/1990, de 26 de abril , al señalar que el principio de culpabilidad puede inferirse de los principios de legalidad y prohibición de exceso (artículo 25 de la Constitución) o de las exigencias inherentes al Estado de Derecho*".

Este argumento ya ha sido esgrimido por la AEPD en procedimientos similares, donde se ha acordado el archivo de las actuaciones (Procedimiento N.º: PS/00112/2021), y es que:

> (i) El robo de la mochila no responde a un acto voluntario de AFIANZA sino de un tercero ajeno a la entidad.
> (ii) No se ha producido ningún tipo de lesión a los derechos y libertades de terceros. El alcance del daño es totalmente inexistente.
> (iii) La actuación de AFIANZA en todo momento responde a la diligencia debida exigida a un responsable del tratamiento.

Por todo ello, AFIANZA solicita:

I. El archivo del procedimiento sancionador de la AEPD en la medida en la que, no ha lugar sanción por unas supuestas infracciones del RGPD que no han supuesto merma en los derechos y libertades de ningún tercero. El alcance del daño no es medible ni cuantificable porque es inexistente. Como ha quedado probado ni la AEPD, ni ningún otro tercero tienen capacidad para probar que, a día de hoy, se ha producido un "acceso indebido" o una "revelación accidental" a la información contenida en el USB, por lo que, la brecha de seguridad a los efectos jurídicos indicados en el RGPD, no se ha materializado. Del mismo modo, no concurre en modo alguno el principio de culpabilidad, por lo que toda sanción sería contraria a la naturaleza del ámbito sancionador administrativo, sujeto a los principios de intervención mínima y proporcionalidad.

II. Se tomen por ciertas y aplicadas las medidas de seguridad implementadas por AFIANZA y coherentes con el actual marco normativo.

III. Se ponga en valor las actividades realizadas por AFIANZA durante todo el procedimientos y puestas de manifiesto en los atenuantes esgrimidos.

OCTAVO: con fecha 23 de enero de 2023, el órgano instructor del procedimiento sancionador formuló propuesta de resolución, en la que propone que por la Directora de la AEPD se sancione a AFIANZA ASESORES, SL, con NIF B83117804:

-por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, con una multa de NOVENTA MIL EUROS (90.000 euros)

-por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, con una multa de CINCUENTA Y CINCO MIL EUROS (55.000 euros)

Esta propuesta de resolución, que se notificó a AFIANZA conforme a las normas establecidas en la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP), fue recogida en fecha 26 de enero de 2023, como consta en el acuse de recibo que obra en el expediente.

En dicha propuesta de resolución, frente a las alegaciones formuladas por AFIANZA, se dio la siguiente respuesta:

1.Brecha de seguridad

Alega la entidad que no ha sufrido una brecha de confidencialidad por cuanto que no se ha podido acreditar que se haya producido un acceso por un tercero no autorizado a la información contenida en el USB robado, pues el único hecho probado es el robo de tal dispositivo, pero no el acceso al contenido del mismo.

A este respecto, procede señalar que en el caso que nos ocupa, se produjo la sustracción de un dispositivo de almacenamiento externo (USB) con numerosa información de carácter personal, relativa a un procedimiento de investigación judicial penal, y que el mismo no estaba cifrado ni contaba con ninguna otra medida dirigida a impedir el acceso a dicha información por terceros no autorizados en caso de pérdida o sustracción, lo cual supone sin duda alguna una vulneración de la confidencialidad de los datos personales contenidos, pues se ha visto claramente comprometida debido a la inexistencia de protección alguna del dispositivo.

En este sentido, el Comité Europeo de Protección de Datos (en adelante, el Comité) lo deja claro y sin ningún tipo de duda cuando, en las Directrices 01/2021 <<sobre ejemplos con respecto a la violación de datos personales. Notificación>>, adoptado el 14 de diciembre de 2021, señala precisamente, en su apartado 5.2, Caso nº11: *Material robado que almacena datos personales no cifrados*, que "*Esta violación de datos se refiere a la confidencialidad de los datos almacenados en el dispositivo robado*" (punto 94).

A este respecto, el Comité es claro al indicar, a continuación, que el dispositivo que contenía los datos personales era "*vulnerable en este caso porque no poseía ninguna protección por contraseña o cifrado*" (punto 95)

Asimismo, continúa en Comité valorando que, debido a estas circunstancias, también es necesaria la notificación a la Autoridad de Control y la notificación a los interesados (punto 98).

Por ello, sostener que aunque se sustrajo un dispositivo con datos personales almacenados en el mismo sin ningún tipo de protección de su acceso no es una vulneración de la confidencialidad porque no se puede demostrar que alguien haya accedido al mismo, supondría lo mismo que afirmar que, en el caso de haberse robado una carpeta o Libro conteniendo la misma documentación en papel, no supondría vulneración de la confidencialidad argumentando la imposibilidad de acreditar fehacientemente que el que la sustrajo u otro tercero no la hubiera abierto. En ambos casos, lo relevante para entender vulnerada la confidencialidad es que la información se encuentra totalmente a la libre disposición de terceros no autorizados.

Pero es que, además, en el caso de los dispositivos electrónicos de almacenamiento portátiles existe la facultad y posibilidad de protegerlos mediante medidas de seguridad técnicas que imposibiliten o dificulten considerablemente el acceso a los mismos por terceros, por lo que, en el presente caso, al no haber existido ninguna de estas medidas establecida en el USB sustraído, supone una vulneración de la confidencialidad y, por tanto, del artículo 5.1 f) del RGPD, que exige precisamente que los datos personales *sean 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»).*

Por tanto, no puede defenderse de ninguna manera que la confidencialidad de los datos personales se mantuvo intacta, pues al no haberse adoptado medidas de seguridad previas, los datos personales almacenados en ese dispositivo son accesibles.

El deber de confidencialidad obliga no sólo al responsable del tratamiento sino a todo aquel que intervenga en cualquier fase del tratamiento. Este deber de secreto comporta que el responsable de los datos almacenados no pueda revelar ni dar a conocer su contenido teniendo el “deber de guardarlos”. Es una exigencia elemental y anterior al propio reconocimiento del derecho fundamental a la libertad informática a que se refiere la Sentencia del Tribunal Constitucional 292/2000, de 30/11, y por lo que ahora interesa, comporta que los datos tratados no pueden ser conocidos por ninguna persona o entidad ajena fuera de los casos autorizados por la Ley, pues en eso consiste precisamente el secreto.

Este deber de sigilo, de confidencialidad, resulta esencial en las sociedades actuales cada vez más complejas, en las que los avances de la técnica sitúan a la persona en zonas de riesgo para la protección de derechos fundamentales, como la intimidad o el derecho a la protección de los datos que recoge el artículo 18.4 de la Constitución Española. En efecto, este precepto contiene un “instituto de garantía de los derechos de los ciudadanos que, además, es en sí mismo un derecho o libertad fundamental, el derecho a la libertad frente a las potenciales agresiones a la dignidad y a la libertad de la persona provenientes de un uso ilegítimo del tratamiento mecanizado de datos” (Sentencia del Tribunal Constitucional 292/2000, de 30/11). Este derecho fundamental

a la protección de datos persigue garantizar a esa persona un poder de control sobre sus datos personales, sobre su uso y destino que impida que se produzcan situaciones atentatorias con la dignidad de la persona, es decir, el poder de resguardar su vida privada de una publicidad no querida.

En el caso que nos ocupa, ha quedado acreditado que AFIANZA ha vulnerado este deber de confidencialidad en relación con los datos personales contenidos en el USB y relativos a una causa penal. Esta información no puede ser facilitada a terceros, salvo consentimiento de los afectados o que exista una habilitación legal que permita su comunicación, circunstancias que no concurren en el presente caso. Todo ello supone una infracción del artículo 5.1. f) RGPD al haber posibilitado, por la ausencia de medidas de protección, que terceras personas puedan tener acceso a datos personales de los clientes afectados.

2.Medidas de seguridad implementadas

Alega AFIANZA que tiene implementadas todas las medidas técnicas y organizativas necesarias para garantizar un nivel de seguridad adecuado al riesgo que conlleva el tratamiento de los datos personales, refiriendo en su escrito de alegaciones un listado de las mismas y afirmando que con ello cumple con lo exigido en el artículo 32 del RGPD, así como con todos y cada uno de los principios relativos al tratamiento, especialmente con el de confidencialidad, recordando que la seguridad no es inexpugnable y que no se le puede responsabilizar por haber sido víctima de un hecho delictivo y tampoco por la vulneración por un tercero de las medidas de seguridad implantadas.

En este sentido, indica además que el citado precepto no regula un listado de las medidas de seguridad que sean de aplicación, por lo que entiende AFIANZA que no resulta adecuado pivotar el procedimiento sancionador en la falta de cifrado del USB robado, pues no es una medida obligatoria por el artículo 32 RGPD y, además, considera que no se han tenido en cuenta ninguna de las medidas de seguridad implementadas por FIANZA y previamente comunicadas.

Frente a ello, procede señalar que, de los hechos acaecidos, se deduce lo contrario. Así, en el caso que nos ocupa, se produjo el acceso de una persona ajena a la entidad a las dependencias de la misma sin que funcionaran o se observaran las medidas de seguridad implantadas y la sustracción de un dispositivo USB no cifrado (o sin ninguna otra medida de protección), conteniendo numerosos datos personales relativos a un procedimiento de investigación judicial penal.

En cuanto a que tenía todas las medidas de seguridad adecuadas y que éstas no se han tenido en cuenta por esta Agencia, se significa que, tal y como ya se indicó en el Acuerdo de Inicio del presente procedimiento sancionador, las medidas de seguridad que refiere AFIANZA que tenía implantadas no se estaban cumpliendo en el momento de los hechos.

Así, del análisis de la documentación aportada por AFIANZA en contestación al requerimiento de información respecto de las causas que hicieron posible la brecha, y de las medidas de seguridad existentes antes de la misma manifestadas por la ésta en aquel momento, resulta lo siguiente:

(…)

Sin embargo, en el caso que nos ocupa, el dispositivo no se encontraba cifrado ni contaba con ninguna otra medida de protección de la información.

Por tanto, de todo ello se deduce una falta de la debida diligencia tanto en el cumplimiento de las medidas de seguridad establecidas, así como en la supervisión o comprobación de su observancia y/o de la idoneidad de las mismas.

A este respecto, se señala que el artículo 32 del RGPD se infringe tanto si no se adoptan por el responsable las medidas de índole técnica y organizativas apropiadas que garanticen la seguridad de los datos personales, como si, establecidas éstas, las mismas no se observan. Es precisamente esta falta de observancia la que supone la infracción señalada en el artículo 73 de la LOPDGDD, al indicar que, 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". (…)

Por último, en cuanto a que el artículo 32 no regula un listado de medidas de seguridad concretas, no siendo el cifrado una medida de seguridad obligatoria, procede indicar que dicho precepto establece, en su apartado 1, la obligación a responsables y encargados del tratamiento de aplicar las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, *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*.

Asimismo, el apartado 3 del mismo precepto determina que, *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*.

Por tanto, el artículo 32, efectivamente, no establece medidas de seguridad concretas y estáticas, sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales. En consecuencia, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

Asimismo, el Considerando 83 del RGPD establece: 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.

En definitiva, el primer paso para determinar las medidas de seguridad que deben aplicarse al tratamiento concreto será la evaluación del riesgo. Una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

Y se insiste, de conformidad con el artículo 32.1 del RGPD, las medidas técnicas y organizativas a aplicar para garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Por ello, derivado de la actividad a la que se dedica y de los datos personales que trata, AFIANZA está obligada realizar un análisis de los riesgos y una implantación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de su actividad para los derechos y libertades de las personas, teniendo en cuenta especialmente que su actividad conlleva tratar datos personales relativos a condenas e infracciones penales.

Cuando se habla de datos relativos a “condenas e infracciones penales”, se está refiriendo a una categoría que incluye datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

El tratamiento de esta categoría de datos personales supone un riesgo alto para los derechos y libertades de las personas físicas titulares de los mismos, riesgo cuya evaluación y análisis por parte del responsable del tratamiento exige el RGPD en varios de sus preceptos y considerandos, además de en su artículo 32, y que conllevará la adopción de las medidas de seguridad apropiadas.

Asimismo, debe evaluarse el riesgo que supone su almacenamiento en dispositivos externos y portátiles (contexto concreto del tratamiento), entre ellos, claramente el riesgo de pérdida o sustracción (riesgo de probabilidad alta) y adoptar las medidas de seguridad adecuadas, de conformidad con el estado de la técnica y los costes de aplicación. En relación con esto último, el estado de la técnica permite de forma fácil y

poco costosa implementar una medida de seguridad de protección en caso de almacenamiento de datos personales en dispositivos externos y portátiles tipo USB: su cifrado o cualquier otra medida técnica de protección frente al acceso por parte de terceros no autorizados (cifrado de los datos, contraseña para el acceso, etc). Es una medida básica, accesible y de implantación sencilla, de conformidad, como se ha dicho, con el estado actual de la técnica.

En el presente caso, como se ha señalado anteriormente, AFIANZA sufrió la sustracción de un dispositivo USB en el que se había almacenado, sin ningún tipo de protección, datos personales ***(…).***

Por tanto, lo que se está reprochando es el almacenamiento de esta categoría de datos personales en un USB totalmente desprotegido, es decir, en un dispositivo externo sin ningún tipo de medida técnica de seguridad, sin ningún tipo de protección para evitar el acceso a terceros no autorizados, lo que supone claramente un incumplimiento del artículo 32 del RGPD.

3. Plazo de notificación de la brecha de seguridad

En este apartado, AFIANZA realiza diversas manifestaciones.

Así, sostiene que el plazo establecido en el artículo 33 del RGPD no es un plazo imperativo.

Frente a ello, procede señalar que el plazo de notificación a esta Agencia en caso de violación de la seguridad de los datos personales es un plazo imperativo: sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella. Por tanto, este es el plazo máximo que se tiene para realizar la notificación. Asimismo, y en congruencia con que es un plazo imperativo, en artículo 74 m) de la LOPDGDD, tipifica como infracción leve la notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

Asimismo, indica AFIANZA que tan pronto tuvo la valoración del posible daño o riesgo de la brecha, lo notificó a la Agencia y que, al no haberse producido publicación o cualquier otro uso indebido de la información contenida en el USB, la brecha de seguridad no se ha materializado.

A este respecto, se señala que el hecho de que no se haya tenido constancia de algún daño o publicación de los datos no significa que la brecha no se haya materializado, pues ello ocurre desde el mismo momento en que se produce el incidente de seguridad que provocó una vulneración de la confidencialidad de los datos.

Por último, manifiesta AFIANZA que cualquier responsable del tratamiento podría haber optado por no haber comunicado nunca a la AEPD el hecho delictivo y que, al hacerlo, demostró con ello una actitud proactiva.

Frente a ello, se recuerda que la notificación de las brechas de seguridad a las autoridades de control y las comunicaciones a los afectados, cuando se dan los

supuestos establecidos por los artículos 33 y 34 del RGPD, no son una opción sino una obligación impuesta por imperativo legal, en este caso, por un reglamento europeo directamente aplicable y que, el no hacerlo, supone una vulneración al mismo tipificada como infracción en su artículo 83.4.

4.Agravantes

Manifiesta AFIANZA no estar de acuerdo en cuanto a las circunstancias agravantes tenidas en cuenta a la hora de determinar el cálculo de la sanción. Así:

-Art. 83.2b) RGPD. Intencionalidad o negligencia en la infracción

Señala AFIANZA que no procede que se observe la existencia de negligencia al producirse un almacenamiento de datos personales en un dispositivo extraíble sin estar cifrado, pues entiende de nuevo que no resulta apropiado hacer pivotar el argumento sancionador en la falta de cifrado del USB robado y el que no se hayan tenido en cuenta el resto de las medidas.

A este respecto, procede remitirse a lo argumentado en el apartado anterior (apartado 2) del presente Fundamento de Derecho, respecto a la falta de observancia o de cumplimiento de las medidas organizativas y técnicas de seguridad que AFIANZA manifiesta tener implantadas (lo que permitió a una persona ajena acceder sin problema, sin forzar nada, a las dependencias de AFIANZA y sustraer el USB), así como a la falta de adopción de una medida básica de seguridad como es la de haber almacenado datos personales relativos a un procedimiento judicial penal en un dispositivo extraíble totalmente desprotegido, pese al riesgo de sustracción o pérdida que ello supone.

Todo ello pone de manifiesto una clara falta de diligencia por parte de AFIANZA en la comprobación y seguimiento de la observancia y cumplimiento de las medidas de seguridad implantadas y/o de su eficacia e idoneidad continuas, tal y como se indicó en el Acuerdo de Inicio y que se reproduce en esta propuesta de resolución en el momento de motivar las circunstancias a tener en cuenta en la graduación de las sanciones (Fundamentos de Derecho VI y IX) y a las que nos remitimos en aras de evitar reiteraciones.

-Art. 83.2 c) RGPD. Cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.

Alega AFIANZA no estar de acuerdo que se haya considerado como circunstancia agravante el que “no reaccionara lo más rápido posible y procediera a tomar medidas necesarias para paliar los efectos y los riesgos sobre los derechos y libertades de las personas físicas afectadas, entre ellas, el notificar a esta Agencia y comunicar a los afectados el incidente sin dilación indebida”.

A este respecto, procede señalar que el notificar a las autoridades de control y comunicar a los afectados la violación de la seguridad son obligaciones impuestas al responsable del tratamiento por el RGPD (artículos 33 y 34 respectivamente), es decir, su observancia viene por imperativo legal, por lo que su cumplimiento o

incumplimiento, de conformidad con lo requerido en dichos preceptos, puede suponer infracciones al mismo.

La circunstancia a tener en cuenta contenida en el artículo 83.2 c), por tanto, ha de referirse a otro tipo de medidas que puedan adoptar el responsable o encargado del tratamiento en aras de reducir en lo posible el impacto de una infracción o de una violación de la seguridad.

Por lo expuesto, no resulta adecuado, en el presente caso, considerar la agravante señalada en el Acuerdo de Inicio, por lo que procede rebajar, en consecuencia, la cuantía de las sanciones de ambas infracciones.

-Art. 83.2 g) RGPD. Las categorías de los datos de carácter personal afectados.

Señala AFIANZA a este respecto que los datos contenidos en el USB era información relativa al proceso de investigación penal, por lo que no había datos relativos a sanciones penales.

A este respecto, se significa que cuando se menciona datos relativos a “condenas e infracciones penales”, se está haciendo referencia a una categoría que incluye datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales. Categoría a la que pertenece la información almacenada en el USB sustraído, pues contenía datos personales ***(…).***

5.Atenuantes

Alega AFIANZA que a la hora de valorar la cuantía de la infracción deberían tenerse en cuenta las circunstancias atenuantes que señala. Si embargo, frente a ello se señala lo siguiente:

-En cuanto a considerar como atenuante el art. 83.2.a) RGPD (naturaleza, gravedad y duración de la infracción), en el sentido de que, al no poder acreditarse que un tercero haya accedido al USB, la gravedad del acceso desde la óptica de la protección de datos es inexistente, se significa que no procede aceptar tal interpretación. Así, por un lado, ya se ha expuesto en el apartado 1 de este Fundamento de Derecho que la sustracción de un dispositivo externo sin ningún tipo de medida de protección frente a su acceso y con datos personales contenidos en el mismo ya supone una violación de la confidencialidad de los mismos, suponiendo ello una vulneración del art. 5.1 f) del RGPD, tipificada como infracción muy grave en el art. 83.5 del citado Reglamento.

-En cuanto a que deban ser considerados como atenuantes las circunstancias recogidas en los arts. 83.2 c) RGPD (cualquier medida tomada por el responsable o encargado del tratamiento para paliarlos daños y perjuicios sufridos por los interesados) y 83.2 f (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), por entender AFIANZA que actúo en todo momento con actitud proactiva y colaborativa con esta Agencia al notificarle la brecha de seguridad y al atender el requerimiento de notificación a los afectados e informándola de ello, procede aclarar que todo ello no es reflejo de una actitud proactiva y colaborativa, sino que son

exigencias legales que AFIANZA está obligada a cumplir como responsable del tratamiento de datos personales, so pena de incurrir en infracciones del RGPD.

Por tanto, el grado de cooperación con la Agencia no puede considerarse un atenuante toda vez que las órdenes y requerimientos que ésta emite son de obligado cumplimiento. La consideración de la cooperación con la Agencia como atenuante, tal y como pretende la entidad, no está ligada a ninguno de los supuestos en los que pueda existir una colaboración o cooperación o requerimiento por mor de un mandato legal, cuando las actuaciones son debidas y obligadas por la Ley, como en el caso que nos ocupa.

6.No concurrencia del principio de culpabilidad

Alega AFIANZA que los hechos acaecidos suponen un resultado no perseguido por AFIANZA, pues fueron producidos mediante la comisión de un acto delictivo de un tercero totalmente ajeno al responsable del tratamiento y a su personal, así como que hubo involuntariedad en el acto, no se produjo un resultado especialmente lesivo y no consta falta de cuidado en la actuación de AFIANZA, por lo que no concurre el elemento de culpabilidad necesario para imponerle una sanción.

Frente a ello, tal y como se ha expuesto en apartados anteriores de este fundamento de derecho, no se sanciona a AFIANZA por haber sufrido un hecho delictivo (sustracción del dispositivo), sino por la falta de medidas adecuadas tanto para salvaguardar la confidencialidad de los datos personales que maneja (almacenamiento de datos personales relativos a infracciones y sanciones penales en un dispositivo externo sin ninguna medida de protección frente a accesos por terceros no autorizados) como por la inobservancia o incumplimiento de las medidas de seguridad que tenían implantadas (controles físicos y lógicos en sus dependencias).

Todo ello pone de manifiesto una falta de la diligencia debida en las medidas que AFIANZA, como responsable del tratamiento de datos personales, está obligada a adoptar de manera efectiva y a verificar que las mismas se observan y que son efectivas y adecuadas, entre ellas, sobre todo, las dirigidas a impedir el acceso no autorizado por parte de terceros a los datos personales de cuyo tratamiento es responsable.

El principio de culpabilidad es exigido en el procedimiento sancionador, pero el principio de culpa no implica que sólo pueda sancionarse una actuación intencionada. El Tribunal Supremo (STS 16 de abril de 1991 y STS 22 de abril de 1991) considera que del elemento culpabilista se desprende “que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable.” El mismo Tribunal razona que “no
basta...para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa” sino que es preciso “que se ha empleado la diligencia que era exigible por quien aduce su inexistencia.” (STS 23 de enero de 1998).
A mayor abundamiento, la Audiencia Nacional en materia de protección de datos de carácter personal, ha declarado que “basta la simple negligencia o incumplimiento de

los deberes que la Ley impone a las personas responsables de ficheros o del tratamiento de datos de extremar la diligencia...” (SAN 29de junio de 2001).

Por todo lo expuesto, procede desestimar las alegaciones formuladas.

NOVENO: Con fecha 9 de febrero de 2023, se recibe en esta Agencia, en tiempo y forma, escrito de AFIANZA en el que aduce alegaciones a la propuesta de resolución en el que, en síntesis, manifiesta que:

I. BRECHA DE SEGURIDAD Y MEDIDAS DE SEGURIDAD IMPLEMENTADAS

Trae a colación la AEPD en su Propuesta de Resolución que, el Comité Europeo de Protección de Datos (en adelante, Comité), en sus Directrices 01/2021 indica que:

> (i) Esta violación de la seguridad de los datos afecta a la confidencialidad de los datos almacenados en el dispositivo robado (punto 94).
> (ii) los datos personales eran vulnerables en este caso porque carecía de protección mediante contraseña o cifrado (punto 95).
> (iii) Debido a estas circunstancias, es necesaria la notificación de la AC, por lo que también es necesaria la notificación de los interesados afectados (punto 98).

Es esencial que se tenga en cuenta que estos argumentos esgrimidos por la AEPD apuntan a un ejemplo específico planteado en esas Directrices del Comité y no responden a la realidad del hecho acontecido y comunicado por AFIANZA, por lo que utilizar los mismos como soporte de la argumentación jurídica de esta Autoridad de Control supone una indefensión absoluta por parte de AFIANZA quien, utilizando este mismo criterio podría esgrimir que en las Directrices sobre la notificación de las violaciones de la seguridad de los datos personales de acuerdo con el Reglamento 2016/679 del Grupo de Trabajo del art.29 (Directrices sobre las que fundamentan las Directrices 01/2021), indica a modo igualmente de ejemplo que i. Un responsable del tratamiento que guardó una copia de seguridad de un archivo de datos personales cifrados en una llave USB. La llave desaparece durante un robo, no debería notificar ni a la Autoridad de Control ni a los afectados. Ciertamente, como se viene informando desde el inicio, el USB no estaba cifrado, pero sí existían otras medidas de seguridad en AFIANZA encaminadas a imposibilitar o dificultar considerablemente el acceso a la información.

Del mismo modo, en la mochila robada también había un IPad, cuyas condiciones se ajustan al 5.1 CASO N.º 10: material robado que almacena datos personales cifrados de las Directrices 01/2021, y en las que, según se concluye en las mismas:

> (i) En este caso concreto, el responsable del tratamiento de datos adoptó las medidas adecuadas para prevenir y mitigar los efectos de una posible violación de la seguridad de los datos mediante el cifrado de dispositivos, la introducción de una protección adecuada de las contraseñas y la protección de los datos almacenados en las tabletas (punto 88).

(ii) La violación de la seguridad de los datos descrita anteriormente habría afectado a la confidencialidad, la disponibilidad y la integridad de los datos en cuestión, sin embargo, debido a los procedimientos adecuados del responsable del tratamiento antes y después de la violación de la seguridad de los datos, ninguno de estos aspectos se vio afectado (punto 89).

Así las cosas, resulta llamativa la actitud sancionadora y señaladora de la AEPD por relación al USB, mientras que, en lo que respecta al IPad, ni siquiera se reconocen, se ponen en valor o se toman en consideración las medidas de seguridad implementadas.

La AEPD en su Propuesta de Resolución manifiesta que “lo relevante para entender vulnerada la confidencialidad es que la información se encuentra totalmente a la libre disposición de terceros no autorizados” afirmar esto, es asumir que AFIANZA no ha cumplido con ninguna de las obligaciones inherentes a su rol de responsable del tratamiento y que no sólo no ha establecido medidas de seguridad, sino que además “facilita” a terceros el acceso a la información de la que es responsable.

Aludiendo a las Directrices 01/2021, esta Autoridad de Control debe conocer que, en la mismas, además de múltiples ejemplos prácticos de situaciones concretas sobre qué es o no es una violación de seguridad, se recoge una listade medidas que, no es en modo alguno exclusiva ni exhaustiva, sobre qué medidas organizativas y técnicas resultan recomendables para prevenir o mitigar el impacto de la pérdida o robo de dispositivos, entre las que se incluyen:

- Utilizar un código de acceso o contraseña en todos los dispositivos.
- Usar autenticación de múltiples factores.
- Activar las funcionalidades de los dispositivos móviles que permiten revocar los permisos de acceso en caso de pérdida o extravío.
- Si el puesto de trabajo está conectado a la LAN corporativa, hacer una copia de seguridad automática de las carpetas de trabajo siempre que sea inevitable que los datos personales se almacenen allí.
- Utilizar una VPN segura (por ejemplo, que requiera una clave de autenticación de segundo factor independiente para el establecimiento de una conexión segura) para conectar los dispositivos móviles a servidores back-end.

Todas y cada una de estas medidas estaban implantadas en AFIANZA a fecha 17 de junio de 2021, prueba de ello se encuentra en cómo se procedió a la desactivación en remoto y la consiguiente revocación de los accesos del IPad que también se encontraba en la mochila.

Además de lo anterior, en las Directrices también se incluyen como medidas de seguridad recomendables: proporcionar cerraduras físicas a los empleados para que puedan proteger físicamente los dispositivos móviles que utilizan mientras estos permanecen sin vigilancia e instalar controles de acceso físico, medidas que, como se ha venido argumentado y probando a lo largo de todo este procedimiento también estaban implantadas en AFIANZA1.

En todo caso, estas Directrices son sobre la notificación de las violaciones de la seguridad, lo que implican que son meras herramientas para determinar si estamos o

no ante una brecha de seguridad, y en caso de haberse producido cómo se debe actuar con respecto a la comunicación de la misma. En ningún caso, el deber notificar un incidente de seguridad va adherido a un incumplimiento o falta de medidas de seguridad, ni del incumplimiento del principio de confidencialidad y mucho menos a una imposición automática de sanciones.

II. INFRACCIÓN DEL ARTÍCULO 32 DEL RGPD

Entiende esta Autoridad de Control que AFIANZA ha incumplido claramente con el art. 32 del RGPD por almacenar datos personales en el USB totalmente desprotegido, es decir, en un dispositivo externo sin ningún tipo de medida técnica de seguridad, sin ningún tipo de protección para evitar el acceso a terceros no autorizados.

El primer paso para determinar las medidas de seguridad que deben aplicarse al tratamiento concreto será la evaluación del riesgo, una vez realizado este, será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar riesgos para el tratamiento de los datos.

En este sentido, AFIANZA, con carácter previo a la comisión del robo, y en cumplimiento del principio de responsabilidad proactiva, había realizado su análisis de riesgos y definido sus medidas de seguridad, medidas tanto técnicas como organizativas, medidas que van más allá del mero cifrado que, si bien, reiteramos, estaba implantado en otras herramientas de AFIANZA (como en el propio IPad). El afirmar que “no existía ningún tipo de medida de seguridad o protección” es negar los hechos probados y actuar de forma punitiva.

AFIANZA asume que, en el momento exacto del robo se produjeron una serie de circunstancias que dieron lugar a la falta de aplicabilidad de algunas de las medidas de seguridad implementadas y ya comentadas, pero esto es muy diferente a afirmar que no existía ninguna. La prueba clara es la comparación entre el tratamiento que se ha dado al IPad y al USB.

Que se pretenda sancionar con 55.000€, resulta absolutamente desproporcionado, y no sólo por la nula valoración de la AEPD de las medidas de control de AFIANZA, o el nulo impacto que ha tenido el hecho, sino por la propia comparación con las resoluciones sancionadores que esta Autoridad de Control ha venido imponiendo a otras entidades por la comisión de la misma infracción. Y es que, tras analizar el total de 61 Resoluciones disponibles través del sitio web de la AEPD relativas a la infracción del art. 32 del RGPD en los procedimientos sancionadores, se desprende que, por relación al sector privado:

(I) En supuestos en los que se ha producido un incidente de seguridad, en los que se ha vulnerado el artículo 32 del RGPD, derivado del abandono de documentos que, incluso, en algunos casos contienen datos personales sensibles, permitiendo, el acceso a los mismos por terceros con quebrantamiento de las medidas establecidas la sanción impuesta por la AEPD ha sido de 3.000€.

En estos casos, si bien no existe la acreditación de acceso a la información por parte de terceros, sí que la actitud del responsable del

tratamiento es activa en el sentido de abandonar la documentación (incluse de carácter médico) al libre acceso de terceros.

(II) Existen otros tantos supuestos en los que, según la AEPD, se ofrecen indicios evidentes de que el sancionado, ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad en su sistema permitiendo el acceso a datos personales de un tercero, permitiendo el acceso a información que contenía datos de terceros, con quebrantamiento de las medidas establecidas. Estas sanciones van desde el Apercibimiento a los 5.000€ en empresas de pequeña dimensión, mientras que, para las grandes empresas, las sanciones oscilan entre los 30.000 y los 60.000€:

Llegados a este punto, AFIANZA se plantea por qué si en el presente caso, la AEPD sostiene que ha habido una infracción del art.32 del RGPD, la sanción propuesta a AFIANZA es semejante a la que se impone a grandes empresas de la talla de XFERA MÓVILES, S.A o VODAFONE ONO, S.A.U, aún cuando en el presente caso y a diferencia de estos:

(i) no existe ninguna prueba que acredite que algún tercero ha accedido efectivamente a la información contenida en ese USB;
(ii) la AEPD ha tenido conocimiento el asunto a través de AFIANZA, no de terceros que hayan podido haber vistos vulnerados sus derechos como si sucede en la amplísima mayoría de los supuestos analizados y aquí recogidos y,
(iii) 20 meses después del robo, no se han visto mermado los intereses y libertades de ninguno de los afectados, no existiendo ninguna denuncia o reclamación en ninguna entidad o institución competente a estos efectos.
(III) Además de los anteriores supuestos, a continuación, se presenta una comparación entre dos acontecimientos muy similares en cuanto al hecho y la tipología de datos, pero absolutamente diferentes con respecto a la sanción, la aplicación de atenuantes, el número de afectados y, en general, la valoración de la AEPD:

AFIANZA se vuelve a plantear por qué (i) si el volumen de datos afectados en el caso de CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA es 100 veces superior el de los datos afectados en el caso de AFIANZA;

(ii) si la tipología de datos en el caso de CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA afecta a muchísimas más categorías especiales de datos (datos de afiliación a sindicato; de salud, sentencias completas; notificaciones de embargo; de plan de pensiones, etc) que en el caso de AFIANZA y (iii) si ha habido reclamación de afectados ante esta Autoridad de Control en el caso de CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA, cuestión no ha acontecido en el caso de AFIANZA,
(i) ¿Por qué en el caso de CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA se toman en consideración atenuantes y no sucede así en el caso de AFIANZA?

(ii) ¿Por qué se penaliza a AFIANZA con la infracción del art. 32 y, además, con la del art.5.1.f) del RGPD y no así a CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA?
(iii) ¿Por qué la sanción propuesta a AFIANZA, por relación únicamente al artículo 32 del RGPD es prácticamente idéntica, y por relación al total propuesto es casi tres veces más que la finalmente impuesta a CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA?

A través de este ejercicio comparativo ha quedado demostrado el carácter absolutamente desproporcionado de la sanción propuesta por la AEPD a AFIANZA, y es que, ante situaciones similares la AEPD llega -incluso- a imponer el apercibimiento cuando considera que la multa administrativa que pudiera recaer constituiría una "carga desproporcionada".

Además, la AEPD tiende a poner en valor en sus resoluciones el que no se haya cometido ninguna infracción anterior en materia de protección de datos, hecho que también origina un resultado sin multa, cuestión que tampoco se ha tenido en consideración con AFIANZA.

III. INFRACCIÓN DEL ARTÍCULO 5.1.F) DEL RGPD

El art. 5.1.f) del RGPD indica que los datos personales serán 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.

Este principio de "seguridad" que impone el RGPD a quienes tratan datos hace necesaria la realización de un análisis de riesgos orientado a determinar las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales. Medidas tanto técnicas como organizativas que, como se ha venido manifestando, existían en AFIANZA. Cuestión diferente es que un día concreto a una hora concreta y por circunstancias concretas se produjo una falta de aplicabilidad de algunas de las medidas de seguridad implementadas y ya comentadas, pero esto es muy diferente a afirmar que no existía ninguna, así como es muy diferente a asumir que se ha incumplido con el principio de confidencialidad.

En el caso anteriormente expuesto de CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA, esta Autoridad de Control, ni siquiera entra a valorar el posible incumplimiento de este artículo.

Todo el hecho aquí valorado se produce como consecuencia de una actividad delictiva, previsiblemente organizada y planeada. No estamos ante una falta de cumplimiento de medidas por AFIANZA, y es que las Sentencias de la Audiencia Nacional (en lo sucesivo, SAN) (Sala de lo Contencioso Administrativo, en adelante, SCA) de 25 de febrero de 2010 [JUR 2010/82723] y de 10 de noviembre de 2017 [JUR 2018/3170]) indican que (…). Así pues, el hecho de que un tercero haya superado dichas medidas

no implica, per se, haber incumplido la obligación o, en su caso, el principio de integridad y confidencialidad. El responsable del tratamiento está sujeto a una obligación de medios, no a una obligación de resultado en el sentido de entender que todo incidente es un incumplimiento del deber de "garantizar un nivel de seguridad adecuado al riesgo" (artículo 32 del RGPD).

Este argumento parece ir de la mano con las resoluciones que la AEPD ha impuesto a aquellos que han infringido el art.5.1.f) del RGPD, y es que de la realización de un análisis somero se desprende que, la AEPD viene imponiendo la infracción del art.5.1.f) en aquellos casos en los que efectivamente ha habido un acceso a la información por parte de terceros no autorizados, es decir, aquellos casos en los que, es hecho probado que terceros han accedido a información de la no eran titulares, elemento que no se produce en el caso que aquí debatimos.

Con todo, AFIANZA reitera el cumplimiento del principio de confidencialidad y requiere a esta Autoridad de Control que difiera entre fallas en la aplicabilidad de las medidas de seguridad en el momento del robo, del incumplimiento del principio de confidencialidad. Ambas infracciones no tienen por qué ir de la mano, y así lo ha manifestado en reiteradas ocasiones la AEPD, no cabe más que revisar sus resoluciones. Es más, ante hecho muy similares (CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA y AFIANZA), los resultados propuestos por la AEPD son totalmente diferentes.

IV. AGRAVANTES

La propuesta de Resolución de la AEPD, a pesar de haber reconsiderado la aplicación del agravante contemplado por el artículo 83.2.c), mantiene las siguientes circunstancias agravantes:

- Art. 83.2 b) RGPD: Intencionalidad o negligencia en la infracción.

En el presente supuesto, existe una evidente falta de “culpabilidad” por parte de AFIANZA, un requisito esencial al objeto de determinar la aplicación del agravante recogido por el art. 83.2.b). La culpabilidad requiere la apreciación de dolo (descartado en todo momento), imprudencia o negligencia, siendo estos dos últimos utilizados conceptos indistintamente por la AEPD.

La AEPD aprecia una conducta negligente en las dos vulneraciones imputadas a AFIANZA relativas a los artículos 5.1.f) y 32 RGPD. No obstante, AFIANZA desconoce los motivos y argumentos correspondientes a cada una de las presuntas infracciones. La Resolución de la AEPD no ha expuesto a que acciones u omisiones de AFIANZA se le han de imputar ninguna de las circunstancias agravantes, simplemente se ha limitado a juzgar ambas vulneraciones de manera conjunta, sin desglosar ni desarrollar cuales son las razones por las que se aprecia negligencia respecto a la vulneración del principio de confidencialidad (artículo 5.1.f) RGPD), ni respecto a la toma de medidas de seguridad adecuadas (artículo 32 RGPD).

Habida cuenta de las circunstancias de este caso, no cabe apreciar una conducta negligente. Tal y como se expuso en anteriores alegaciones, la negligencia implica una

omisión de aquella diligencia que exija la naturaleza de la obligación y corresponde a las circunstancias de las personas, del tiempo y del lugar, de conformidad con los artículos 1.104, 1.101 y 1.089 del Código Civil.

En el presente caso AFIANZA, no ha llevado a cabo un comportamiento activo que haya infringido el principio de confidencialidad o haya quebrantado las medidas de seguridad oportunas, como supondría la publicación de datos personales en una página web o el envió de un correo a múltiples destinatarios sin la función CCO (tal y como sucede con los casos expuestos en el Anexo I).

AFIANZA en ningún momento llevo a cabo actos que pusieran en riesgo la seguridad y confidencialidad de los datos, es decir, no tomó decisiones de manera consciente a sabiendas de que pudieran acarrear consecuencias perjudiciales. Todo lo contrario. AFIANZA ha demostrado una responsabilidad proactiva, habiendo establecido tanto barreras físicas relativas a la infraestructura del edificio y personal de seguridad, como técnicas con el cifrado de la mayor parte de los dispositivos, si bien, AFIANZA reconoce y así lo ha informado desde el primer momento, que algunas de esas medidas de seguridad no se aplicaron en el día y hora exactos del robo, que es diferente a asumir que no existían o nunca antes se habían aplicado.

A este tenor, las Directrices sobre la aplicación y el establecimiento de límites administrativos a efectos del RGPD emitidas por el Comité Europeo de Protección de Datos, realizan las siguientes observaciones respecto al mencionado agravante. El Comité afirma que, de conformidad con el RGPD, “las rutinas y la documentación de las actividades de tratamiento se basan en el riesgo”. Asimismo, “las empresas deben ser responsables de adoptar estructuras y recursos adecuados a la naturaleza y complejidad de su negocio”.

En este punto, no cabe más que reiterar la escasa probabilidad de que se cometiese un robo de una mochila en unas instalaciones en las que existen cientos de dispositivos de mayor valor, todos ellos protegidos con sistemas de cifrado. El riesgo de que un delito de este calibre se llevase a cabo en las circunstancias dadas en este caso concreto parece prácticamente inimaginable.

- Art. 83.2.g) RGPD las categorías de los datos de carácter personal afectados por la infracción.

En lo que se refiere a este agravante, AFIANZA se ve en la necesidad de manifestar que los datos relativos a infracciones y condenas penales (la investigación penal) ya habían sido hechos manifiestamente públicos en fecha anterior al día del robo. ***(…).***

Es decir, aun siendo los datos contenidos en el USB que estaba dentro de la mochila robada relativos a infracciones y condenas penales, la práctica totalidad de lo ahí incluido ya había sido publicado en diarios, radio y TV. El riesgo de que se filtre o se conozca algo nuevo es inexistente.

Este criterio es defendido la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011 (asuntos acumulados C-468/10 y C469/10), la cual indica, en sus Considerandos 44 y 45, que cuando los datos figuran en fuentes accesibles al público, el responsable del tratamiento y, en su caso, el tercero o terceros a quienes se

comuniquen los datos no acceden a datos relativos a la vida privada del interesado, dado que la información ya es de público conocimiento. Como consecuencia, hay un impacto menor en los derechos del interesado, lo que debe ser apreciado en su justo valor en la ponderación con el interés legítimo perseguido por el responsable del tratamiento o por el tercero o terceros a los que se comuniquen los datos. Lo mismo puede decirse en el caso de los datos hechos manifiestamente públicos por el interesado (artículo 9.2. e) RGPD) que también concurre en el presente caso en tanto muchos de los investigados han salido en medios de comunicación haciendo declaraciones sobre el caso.

V. ATENUANTES

A pesar de los hechos expuestos y la patente actitud cooperadora y favorable de AFIANZA, la Resolución de la AEPD rechaza la consideración de las siguientes circunstancias atenuantes, que a nuestro tenor han de ser valoradas:

- Art. 83.2.a) RGPD la naturaleza, gravedad y duración de la infracción. Resulta oportuno subrayar que, dos años después de la brecha de seguridad, no se ha constatado la revelación de ninguno de los datos contenidos en el Pendrive robado. Asimismo, ninguna de las casi cien personas afectadas ha interpuesto reclamación alguna al respecto. Si bien es cierto que el USB con un volumen considerable de datos fue robado, el impacto ha sido prácticamente inexistente. No se ha generado consecuencia alguna para las personas afectadas, quienes tampoco han manifestado su malestar o desaprobación.

- Art. 83.2.c) RGPD cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados.

Desde el momento en que AFIANZA tuvo constancia del robo de la mochila actúa de manera inminente y efectiva. En primer lugar, bloqueando por completo el contenido del IPad, medida que ha reducido notoriamente el acceso a determinada información. Acto seguido AFIANZA identificó los datos personales implicados, las personas afectadas y se puso en contacto con las mismas informando de lo sucedido. Igualmente, se pusieron en marcha protocolos de seguridad y prevención en cuanto a la privacidad y confidencialidad de la información recabada por el despacho, así como el acceso a sus instalaciones; medidas de formación y concienciación. Ninguna de estas medidas ha sido considerada por la AEPD, a diferencia de lo que sucedió en el caso de CORPORACION DE RADIO Y TELEVISION ESPAÑOLA SA, anteriormente mencionado.

- Art.83.2. f) RGPD, 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.

Estrechamente ligado a lo recientemente expuesto, resulta pertinente reiterar la actitud colaboradora de AFIANZA. La AEPD expone en la Resolución que el hecho de colaborar y proporcionar la información requerida resulta una obligación legal y, consecuentemente, no ha de ser premiada. Efectivamente, AFIANZA ha cumplido en tiempo y forma con todas las obligaciones y requerimiento de la AEPD desde el momento en que notifica la brecha de seguridad. Desde esta parte, no alcanzamos a comprender cuál debe ser entonces el grado de cooperación para que sea

considerado como atenuante, más aún, cuando existen casos en los que la entidad reclamada no ha cumplido con las obligaciones impuestas y no se ha implementado el consecuente agravante.

- Art. 83.2.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.

Indica AFIANZA que fue quien puso en conocimiento de la AEPD la brecha de seguridad, nota patente de la responsabilidad proactiva y actuar diligente de la entidad reclamada. Si bien, existió cierto retraso en el plazo de notificación, durante el presente procedimiento ha sido suficientemente acreditado (transcurso del fin de semana, recabado de información y personas afectadas, limitación del daño, etc.).

En este sentido, entiende que la notificación de la brecha por parte de AFIANZA demuestra una proactividad. Es decir, la pérdida o robo de un USB (dispositivo de pequeño tamaño), puede pasar fácilmente inadvertido, no haber sido detectado. Sin embargo, AFIANZA sí ha demostrado tener un control sobre los dispositivos de la empresa de forma que, cuanto menos, su pérdida o robo es detectada, de manera que se han podido adoptar medidas desde etapas tempranas. No se trata de haber sido cumplidor porque se haya notificado la brecha a la AEPD, sino de que se ha sido capaz de detectar de inmediato que, entre los bienes sustraídos, había un USB con datos personales. Esto en sí mismo denota una diligencia debida ante una brecha de seguridad de datos personales.

Asimismo, habida cuenta del nulo impacto y la ausencia de reclamaciones por parte de las personas afectadas si AFIANZA no lo hubiera notificado, la AEPD nunca hubiera sido conocedora del hecho.

- Art. 83.2.k) cualquier otro factor atenuante aplicable a las circunstancias del caso, aplicados por la AEPD en otros procedimientos, tales como:

- El alcance inexistente del daño. Ninguna persona física ha visto mermados sus derechos y libertades.
- AFIANZA ha adoptado medidas para evitar que se produzcan incidencias similares en el futuro, y, a día de hoy, han resultado ser efectivas.
- AFIANZA ha respondido a todos los requerimientos de la AEPD, lo que incide en la cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la misma.
- No se tiene constancia de que AFIANZA hubiera obrado dolosamente ni tampoco con falta de diligencia.
- AFIANZA es una pequeña empresa.
- AFIANZA no ha cometido ninguna infracción anterior en materia de protección de datos.
- AFIANZA fue víctima de un robo premeditado, aprovechando una situación de vulnerabilidad espontánea de las medidas de seguridad. Esto implica que, además de haber sufrido las consecuencias intrínsecas como víctima de un delito, ha sido juzgada por el mismo.

VI. NO CONCURRENCIA DEL PRINCIPIO DE CULPABILIDAD

En cuanto al principio de culpabilidad se refiere, AFIANZA sostiene, al igual que hizo en las alegaciones al acuerdo de inicio del procedimiento sancionador que no ha actuado culposamente, por lo que no procede la imposición de sanción alguna.

El artículo 28.1 de la Ley 40/2015, de 1 de octubre, regula el principio de culpabilidad, indicando que sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa".

Siguiendo con la interpretación realizada por el Tribunal Supremo, para la exculpación no bastará la invocación de la ausencia de culpa, sino que será preciso que se haya empleado la diligencia que era exigible por quien aduce su inexistencia (entre otras, la Sentencia del Tribunal Supremo de 23 de enero de 1998 [RJ 1998\601]). Asimismo, la Audiencia Nacional ha entendido, en casos similares al presente, en los que un tercero ha accedido, mediante actividades delictivas, a datos de los interesados custodiados por un responsable del tratamiento, que imputar tales hechos al responsable del tratamiento podría conllevar la vulneración del principio de culpabilidad. A título de ejemplo, la SAN (SCA, Sección 1ª) de 25 de febrero de 2010 [JUR 2010/82723]. "Así, aun cuando el artículo 9 de la LOPD establece una obligación de resultado, consistente en que se adopten las medidas necesarias para evitar que los datos se pierdan, extravíen o acaben en manos de terceros, tal obligación no es absoluta y no puede abarcar un supuesto como el analizado. En el caso de autos, el resultado es consecuencia de una actividad de intrusión, no amparada por ordenamiento jurídico y en tal sentido ilegal, (…). Y, tales hechos, no pueden imputarse a la entidad recurrente pues, de otra forma, se vulneraría el principio de culpabilidad".

En ningún caso el robo de la mochila puede suponer la consideración de que AFIANZA ha obrado culposamente. En consecuencia, ha actuado con la diligencia debida que es exigible y conforme dispone el derecho sancionador, no procede la imposición de sanción alguna.

Por otro lado, cabe señalar que la SAN -Sala Contencioso-Administrativo392/2015, de17 de noviembre que en su Fundamento Jurídico Tercero recoge la doctrina del Tribunal Constitucional sobre la aplicación al derecho administrativo sancionador de los principios del orden penal, en los siguientes términos: "El Tribunal Constitucional ha declarado reiteradamente que los principios del orden penal, entre los que se encuentra el de culpabilidad, son de aplicación, con ciertos matices, al derecho administrativo sancionador, al ser ambos manifestaciones del ordenamiento punitivo del Estado (STC 18/1987 , 150/1991), y que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo de culpabilidad aun a título de mera negligencia (SSTC 76/1990 y 164/2005).

El principio de culpabilidad, garantizado por el artículo 25 de la Constitución, limita el ejercicio del "ius puniendi" del Estado y exige, según refiere el Tribunal Constitucional en la sentencia 129/2003, de 20 de junio, que la imposición de la sanción se sustente en la exigencia del elemento subjetivo de culpa, para garantizar el principio de

responsabilidad y el derecho a un procedimiento sancionador con todas las garantías (STS de 1 de marzo de 2012, Rec 1298/2009).

En el supuesto que nos atañe resulta notoria la inexistencia de antijuridicidad y culpabilidad en la conducta de AFIANZA, a diferencia de los casos presentados en los apartados II y III de las presentes alegaciones, AFIANZA no realiza ninguna actuación dirigida a incumplir sus obligaciones como responsable del tratamiento; AFIANZA no facilita/envía/comunica/ datos personales de afectados a terceros no autorizados; AFIANZA no incumple el principio de confidencialidad; AFIANZA no realiza una actuación culposa. AFIANZA ha cumplido siempre con todas las obligaciones inherentes a la normativa protectora de datos de carácter personal, se ha demostrado mediante la aportación de documentación, la denuncia, la comunicación de la brecha y demás comunicaciones con la AEPD que su conducta siempre ha sido conforme la diligencia que le era exigible, además se ha acreditado la adopción de las cautelas exigibles para evitar el tratamiento no consentido de los datos y se ha informado a todas las personas afectadas del hecho, si bien, reiteramos, hecho que, 20 meses después, ha supuesto un impacto nulo o inexistente a los afectados.

Con todo, en el presente caso, los hechos acaecidos implicarían un resultado no perseguido por AFIANZA, en tanto fue motivado por la comisión de un hecho delictivo de un tercero totalmente ajeno al responsable del tratamiento y a su personal, por lo que no se dan los elementos necesarios determinados por la Audiencia Nacional para asumir que, efectivamente, la conducta de AFIANZA ha sido culposa, esto es:

> (i) no concurre voluntariedad en el acto,
> (ii) no se ha producido un resultado especialmente lesivo,
> (iii) no consta la falta de cuidado en la actuación de AFIANZA en sus actividades y funciones.

Este argumento ya ha sido esgrimido por la AEPD en procedimientos similares, donde se ha acordado el archivo de las actuaciones (Procedimiento N.º: PS/00112/2021), y es que:

> (i) El robo de la mochila no responde a un acto voluntario de AFIANZA sino de un tercero ajeno a la entidad.
> (ii) No se ha producido ningún tipo de lesión a los derechos y libertades de terceros. El alcance del daño es totalmente inexistente.
> (iii) La actuación de AFIANZA en todo momento responde a la diligencia debida exigida a un responsable del tratamiento.

Por todo ello, AFIANZA solicita:

I. El archivo del procedimiento sancionador de la AEPD contra AFIANZA en la medida en la que no ha lugar sanción por unas supuestas infracciones del RGPD que no han supuesto merma en los derechos y libertades de ningún tercero. El alcance del daño no es medible ni cuantificable porque es inexistente. Del mismo modo, no concurre en modo alguno el principio de culpabilidad, por lo que toda sanción sería contraria a la naturaleza del ámbito sancionador administrativo, sujeto a los principios de intervención mínima y proporcionalidad.

II. Que, en el caso de no dar por válidos los argumentos esgrimidos por relación a la no concurrencia del principio de culpabilidad, se tenga en cuenta los argumentos aportados con respecto a la imposición de las sanciones relativas al art.51.f) y 32 del RGPD. AFIANZA considera suficientemente probado su cumplimiento por relación al principio de confidencialidad (art. 5.1.f) del RGPD, no existen argumentos jurídicos suficientes como para determinar lo contrario, máxime teniendo en cuenta cómo ha venido sancionando en los últimos años esta Autoridad de Control.

III. Que, se tenga en consideración el agravio que resulta de comparar la cantidad económica propuesta a AFIANZA con la que la AEPD viene imponiendo a otras entidades, máxime si se toma en consideración un caso similar, como el que se ha expuesto en el apartado II, donde la afectación ha sido 100 veces superior a la que ha podido tener AFIANZA y, sin embargo, el tratamiento en la determinación de la sanción y la valoración de otros elementos como los atenuantes o la no imposición de otras infracciones ha sido absolutamente negativa para AFIANZA. Por lo que, se solicita a esta AEPD que cuantifique las sanciones en orden a sus propias resoluciones.

IV. Que, si finalmente procede la sanción, se evite la publicación de la resolución por dos motivos fundamentales:

> a. En primer lugar, porque vinculando los hechos que van a quedar irremediablemente relatados en la resolución con AFIANZA es bastante fácil identificar a las personas físicas afectadas por la brecha.
>
> b. Dado que no hay constancia de que la información del USB se haya utilizado por quien cometió el robo, es muy posible que no sea consciente del contenido del USB. Cuando se haga publica la resolución podría llegar a ser consciente de la información que contiene y entonces querer aprovecharla de algún modo que
> conlleve, ahora sí, algún perjuicio para los afectados. Se estaría así agravando las consecuencias de la brecha por la publicación de la resolución sin haber disociado la información.

V. Que, si la AEPD tiene la obligación de publicar la resolución de la sanción, se omita cualquier referencia expresa ***(...)***, así como a la mercantil Afianza Asesores, S.L, por los mismos motivos esgrimidos en el punto IV anterior.

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

HECHOS PROBADOS

PRIMERO: ***(…).*** El dispositivo USB no está cifrado ni tiene implantadas ninguna otra medida de protección de su contenido frente a terceros no autorizados.

SEGUNDO: AFIANZA notifica la brecha de seguridad a la AEPD el 30 de junio de 2021 y comienza las actuaciones tendentes a la comunicación a los afectados el 8 de julio 2021.

FUNDAMENTOS DE DERECHO

I
Competencia y normativa aplicable

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
Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que AFIANZA realiza, entre otros tratamientos, la recogida, registro, organización, conservación, consulta, acceso y supresión de datos personales de personas físicas, tales como: nombre, número de identificación, fecha de nacimiento, sexo, estado civil, datos de contacto, imagen, voz y datos sobre condenas e infracciones penales, entre otros.

AFIANZA realiza esta actividad en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD.

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las “violaciones de seguridad de los datos personales” (en adelante brecha de seguridad) como “todas aquellas violaciones de la seguridad que ocasionen 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.”

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad al haberse sustraído un dispositivo USB no cifrado ***(...),*** con los datos personales anteriormente referenciados, lo que permite un acceso no autorizado a ellos.

La seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que regulan tanto la seguridad del tratamiento, la notificación de una violación de la seguridad de los datos personales a la autoridad de control, así como la comunicación al interesado, respectivamente.

III
Alegaciones aducidas

En relación con las alegaciones aducidas a la propuesta de resolución del presente procedimiento sancionador, se procede a dar respuesta a las mismas:

1.- Brecha de seguridad y medidas implementadas

Señala AFIANZA que no está de acuerdo en que esta Agencia traiga a colación las Directrices 01/2021 del Comité Europeo de Protección de Datos (en adelante el Comité) para argumentar su postura, entendiendo que con ello se le causa una indefensión absoluta.

A este respecto, procede recordar que AFIANZA, en su escrito de alegaciones al Acuerdo de Inicio del presente procedimiento sancionador, negaba que se hubiese producido una brecha de seguridad y mucho menos que hubiera afectado a la confidencialidad, frente a lo cual, esta Agencia procedió primero, a argumentar claramente por qué sí se dan los presupuestos para entender que se estaba ante dicha brecha de confidencialidad, mencionando, en segundo lugar, las citadas Directrices del Comité como reflejo de que dicho organismo de la Unión Europea sostiene la misma interpretación, pues llega a la misma conclusión en un supuesto básicamente idéntico.

Debe recordarse que el Comité tiene encomendada la función de garantizar la aplicación coherente del RGPD (art. 70.1) y que para ello, entre otras concretas funciones y competencias que se le atribuyen, *examinará, a iniciativa propia, a instancia de uno de sus miembros o de la Comisión, cualquier cuestión relativa a la aplicación del presente Reglamento, y emitirá directrices, recomendaciones y buenas prácticas a fin de promover la aplicación coherente del presente Reglamento* (art. 70.1.e RGPD)

Por tanto, a la hora de interpretar el RGPD, no debe olvidarse la incuestionable preponderancia que dicha norma atribuye a las directrices, recomendaciones, dictámenes, etc, del Comité.

Por otro lado, señala AFIANZA que, si bien el USB no estaba cifrado, sí existían otras medidas de seguridad implementadas en los tratamientos que realiza y que el no tenerlas en cuenta entiende que es como asumir que no ha cumplido con ninguna de las obligaciones inherentes a su rol de responsable del tratamiento y que no sólo no ha establecido medidas, sino que además “facilita” a terceros el acceso a la información de la que es responsable.

Frente a ello, se señala de nuevo que la infracción imputada es precisamente el haberse vulnerado la confidencialidad por no contener ese USB ninguna medida de cifrado o cualquiera otra dirigida a imposibilitar el acceso a su contenido (datos personales) por parte de terceros no autorizados. Como ya se señaló en la Propuesta de Resolución del presente procedimiento sancionador, en el caso de los dispositivos electrónicos de almacenamiento portátiles existe la facultad y posibilidad de protegerlos mediante medidas de seguridad técnicas que imposibiliten o dificulten considerablemente el acceso a los mismos por terceros, por lo que, en el presente

caso, al no haber existido ninguna de estas medidas establecida en el USB sustraído, supone una vulneración de la confidencialidad y, por tanto, del artículo 5.1 f) del RGPD, que exige precisamente que los datos personales sean 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»).

2.- Infracción del artículo 32 del RGPD

Alega AFIANZA que, con anterioridad al incidente, en cumplimiento del principio de responsabilidad proactiva había realizado sus análisis de riesgo y definidas sus medidas de seguridad, tanto técnicas como organizativas (las cuales describe), medidas que van más allá del mero cifrado, por lo que afirmar que no existía ningún tipo de medida de seguridad o protección es contrario a los hechos probados.

Frente a ello, en primer lugar, se significa que es en relación al USB sustraído respecto del que se ha señalado la ausencia de ningún tipo de medida de protección o de impedimento frente al acceso por terceros no autorizados.

En segundo lugar, en cuanto a la imputación de la infracción del artículo 32 del RGPD, tal y como ya se indicó en la Propuesta de Resolución en respuesta a la misma alegación, y que aparece transcrita en el punto 2 del Antecedente de Hecho Octavo y al que nos remitimos en aras de evitar reiteraciones innecesarias, de los hechos acaecidos se deduce que no se estaban observando muchas de las medidas de seguridad implantadas -tal y como reconoce la entidad- y necesarias para una protección y un nivel de seguridad adecuado al riesgo del tratamiento y que ello permitió la sustracción del USB y la brecha de seguridad de los datos personales y que afectara, además, a la confidencialidad de los mismos.

Se reitera de nuevo que el artículo 32 del RGPD se infringe tanto si no se adoptan por el responsable las medidas de índole técnica y organizativas apropiadas que garanticen la seguridad de los datos personales, como si, establecidas éstas, las mismas no se observan. Es precisamente esta falta de observancia la que supone la infracción señalada en el artículo 73 de la LOPDGDD, al indicar que, 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". (…)

3.- Infracción del artículo 5.1f.

Señala AFIANZA que no ha incumplido este precepto por cuanto tras el correspondiente análisis de riesgos, tenía implantadas las medidas técnicas y organizativas necesarias para garantizar la integridad, la disponibilidad y la confidencialidad de los datos personales y que cuestión diferente es que un día concreto, a una hora concreta y por circunstancias concretas se produjo una falta de

aplicabilidad de algunas de las medidas de seguridad implementadas, pero que ello es muy diferente a afirmar que no existía ninguna, así como a asumir que se ha incumplido con el principio de confidencialidad.

Frente a ello, procede reiterarse en todo lo ya argumentado en relación a la falta de observancia de las medidas de seguridad implantadas y que ello supuso una brecha de seguridad afectando a la confidencialidad de los datos almacenados en el USB sin medida de protección frente a accesos ilícitos, suponiendo ello la infracción del artículo 5.1 f. Por tanto, nos remitimos a todo lo contestado en la propuesta de resolución y que aparece reproducido en el Antecedente de Hecho Octavo de la presente resolución.

Por otro lado, sostiene AFIANZA que todo lo acontecido se produjo como consecuencia de una actividad delictiva y que ello no supone una falta de cumplimiento de medidas, pues el hecho de que un tercero haya superado dichas medidas no implica, *per se*, haber incumplido la obligación, pues el responsable del tratamiento está sujeto a una obligación de medios, no a una obligación de resultado.

A este respecto, procede señalar que esa obligación de medios que alude no estaba siendo cumplida, pues implementadas las medidas de seguridad que indica la entidad, tanto técnicas como organizativas, las mismas no estaban siendo observadas, lo que permitió el incidente sin ningún tipo de trabas ni medida que tuviera que solventarse ni violentarse.

4.- Otros procedimientos sancionadores tramitados por esta Agencia.

Refiere AFIANZA una serie Resoluciones de procedimientos sancionadores tramitados con anterioridad por esta Agencia al objeto de alegar desproporcionalidad en las sanciones impuestas, incluso diferencias en la imputación de infracciones ante lo que entiende mismos hechos o grandes similitudes.

Frente a ello, procede señalar que las resoluciones analizadas por AFIANZA, si bien pueden tener similitudes, también tienen diferencias con las circunstancias concretas del presente caso. Así, hay diferencias en cuanto al número de personas afectadas por la vulneración de la confidencialidad (en muchos casos sólo una persona); en cuanto al tratamiento de datos personales que realiza el sancionado (si es su actividad principal, si es accesoria, si es mínima, si se le exige mayor diligencia según el sector, etc); en cuanto a la categoría de datos afectados; en cuanto al número de datos personales afectados (en algunos casos sólo el mail o pocos datos más); momento en que sucedieron los hechos respecto del tiempo que llevaba siendo aplicable el RGPD (en muchos casos apenas meses, lo que es diferente de llevar casi 3 años). En este sentido, no debe olvidarse que a la hora de determinar las sanciones a imponer debe tenerse en cuenta las circunstancias concretas del caso.

Por otro lado, AFIANZA trae únicamente a colación resoluciones de expedientes que fueron tramitados al principio de aplicación el RGPD. Sin embargo, no ha mencionado otros más tardíos que podrían ser más parecidos a su situación en cuanto a las infracciones imputadas y la cuantía de las sanciones -sin olvidar, se insiste, que debe atenderse a las circunstancias concretas del caso- y que, además, debe tenerse en cuenta también que han sido tramitados una vez existen más aclaraciones e

interpretaciones realizadas tanto por las Autoridades de Control como por parte del Comité Europeo de Protección de Datos, así como sentencias de los tribunales que van dictándose, conformándose así jurisprudencia al respecto.

(…)

Por otro lado, no debe olvidarse que AFIANZA es una empresa dedicada a la asesoría legal, siendo su actividad de constante y abundante manejo de datos personales -entre los que se encuentran, se insiste, los relativos a infracciones y sanciones penales-. Ambas circunstancias son relevantes a la hora de valorar el grado de diligencia, debiendo ponderarse especialmente la profesionalidad o no del sujeto, por lo que AFIANZA debe poner mayor rigor y exquisito cuidado por ajustarse a las previsiones legales al respecto.

Por tanto, todas estas circunstancias son las que se han tenido en cuenta y las que han condicionado la cuantía de las sanciones impuestas.

5.- Circunstancias agravantes

Manifiesta de nuevo AFIANZA no estar de acuerdo en cuanto a las circunstancias agravantes tenidas en cuenta a la hora de determinar el cálculo de la sanción. Así:

-Art. 83.2b) RGPD. Intencionalidad o negligencia en la infracción

Reitera de nuevo AFIANZA que no cabe apreciar una conducta negligente, además de que alega que desconoce los motivos y argumentos por los que se aplican las agravantes, pues esta Agencia no ha expuesto a qué acciones y omisiones se le imputan dichas circunstancias agravantes.

Frente a ello, se significa que tanto en el Acuerdo de Inicio, como en la Propuesta de Resolución se indican claramente los motivos y argumentos por los que procede tener en consideración las circunstancias agravantes tenidas en cuenta a la hora de determinar la cuantía de la sanción. Por tanto, procede remitirse a todo lo señalado ya respecto de la falta de observancia de las medidas técnicas y organizativas que en el momento del incidente no estaban siendo observadas, lo cual pone de manifiesto una clara negligencia por parte de AFIANZA.

Asimismo, procede remitirse lo indicado en la Propuesta de Resolución como respuesta a las alegaciones formuladas frente al Acuerdo de Inicio y que aparece transcrito en el Antecedente de Hecho Octavo, así como a los Fundamentos de Derecho VI y IX de la presente resolución.

-Art. 83.2 g) RGPD. Las categorías de los datos de carácter personal afectados.

Respecto de esta agravante, señala AFIANZA que no procede ya que los datos ya habían sido hechos manifiestamente públicos en fecha anterior al día del robo, pues se refieren a un caso penal conocido, trayendo a colación la Sentencia del Tribunal de Justicia de la Unión Europea de 24 de noviembre de 2011, lo que supone un impacto menor en los derechos de los interesados, lo que debe ser apreciado.

(…)

Por tanto, si bien se han podido publicar en los medios de comunicación información relativa a algunos de los investigados, no procede aceptar que todos los datos personales relativos a todas las personas afectadas estuvieran publicados con anterioridad al incidente, además de que no se ha aportado prueba alguna al respecto.

6.- Circunstancias atenuantes

Reitera AFIANZA una serie de circunstancias que considera que deberían haberse tenido en cuenta como atenuantes.

Frente a ello, procede recordar que muchas de ellas no pueden considerarse como tales, y así se señaló en la Propuesta de Resolución del presente procedimiento sancionador en respuesta a esta misma alegación y que aparece transcrita en el Antecedente de Hecho Octavo de la presente resolución y al que procede remitirse en aras de evitar reiteraciones innecesarias.

No obstante, en relación con que debería tenerse en cuenta la atenuante del art. 83.2.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*) pues AFIANZA sostiene que en cuanto tuvo conocimiento del incidente lo notificó a esta Agencia y que, además, identificó a las personas afectadas y se puso en contacto con las mismas informando de lo sucedido, lo cual demuestra una clara proactividad, procede aclarar -además de no suponer ello una circunstancia atenuante, por ser de obligado cumplimiento por imperativo legal- varias cuestiones:

En primer lugar, tal y como ya se indicó en la propuesta de resolución, el plazo de notificación a esta Agencia en caso de violación de la seguridad de los datos personales es un plazo imperativo: *sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella*. Por tanto, este es el plazo máximo que se tiene para realizar la notificación. Asimismo, y en congruencia con que es un plazo imperativo, en artículo 74 m) de la LOPDGDD, tipifica como infracción leve *la notificación incompleta, tardía o defectuosa a la autoridad de protección de datos de la información relacionada con una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679*, infracción que no ha sido imputada a AFIANZA por haberse superado el plazo de prescripción de un año en el momento de dictarse el Acuerdo de Inicio, de conformidad con el citado artículo 74.

El único supuesto que permite el no notificarlo sin dilación indebida y, en su caso, a más tardar 72 horas, es el de no tener constancia o cualquier otro motivo que lo justifique y que debe motivarse. En el caso que nos ocupa, prácticamente desde el mismo momento de la sustracción o, como mucho, al día siguiente (cuando se presenta la denuncia del robo ante la policía y en la que ya se indica el robo del USB y el contenido del mismo), ya se tiene constancia de la brecha de confidencialidad sufrida, momento desde el cual comienza a computarse el plazo indicado. Sin embargo, no se realizó la notificación hasta 13 días más tarde, no siendo aceptables

como motivos de la dilación los argüidos por AFIANZA, pues ninguno de ellos justifica tal retraso.

En segundo lugar, se significa que el artículo 34 exige que *cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida*. No debe olvidarse que el objetivo de las notificaciones y comunicaciones exigidas en los artículos 33 y 34 del RGPD tienen por objeto reducir los riesgos para los derechos y libertades de las personas afectadas cuando una violación de la seguridad puede suponer un riesgo para ello, en el presente caso, un alto riesgo. Por tanto, el retraso en dicha notificación impidió a esta Agencia analizar con la máxima premura la situación y, como ha sucedido, valorar negativamente la decisión de AFIANZA de no comunicarlo a los afectados -desdeñando la gravedad de los posibles efectos adversos-, provocando con este retraso que los mismos no pudieran adoptar tan pronto como sea posible las medidas y reacciones que consideren en aras de salvaguardar sus derechos y libertades.

7.- No concurrencia del principio de culpabilidad

Señala AFIANZA que no cabe en el ámbito sancionador administrativo la responsabilidad objetiva o sin culpa, en cuya virtud se excluye la posibilidad de imponer sanciones por el mero resultado, sin acreditar un mínimo de culpabilidad, aún a título de mera negligencia. Considera a este respecto que no ha actuado culposamente, siendo notoria la inexistencia de antijuridicidad y culpabilidad en su conducta, ya que el incidente fue resultado de una actuación delictiva de un tercero, no pudiendo exigirse una obligación de resultados, sino una obligación de medios.

Frente a ello, procede señalar que esta alegación ya fue respondida en la Propuesta de Resolución del presente procedimiento sancionador, por lo que procede remitirse a la misma.

No obstante, aclarar de nuevo que no se considera a AFIANZA responsable por el resultado, sino por una pérdida de confidencialidad vinculada a la inobservancia de una serie de medidas de seguridad implantadas y, en definitiva, debido a una falta de diligencia de la entidad. En este sentido, la Sentencia del Tribunal Supremo de 15 de febrero de 2022 (Rec. 7359/2020) indica que "*No basta con diseñar los medios técnicos y organizativos necesarios, también es necesaria su correcta implantación y su utilización de forma apropiada, de modo que también responderá por la falta de la diligencia en su utilización, entendida como una diligencia razonable atendiendo a las circunstancias del caso*"

Esa falta de diligencia de AFIANZA, como responsable del tratamiento, a la hora de observar o de verificar la idoneidad de las medidas de seguridad adecuadas es lo que constituye el elemento de la culpabilidad.

Finalmente, en lo referente a que no cabe culpar a AFIANZA de los actos delictivos realizados por terceros, indicar que esta Agencia no extiende la responsabilidad de la entidad más allá de sus obligaciones como responsable del tratamiento.

8.- Otras cuestiones planteadas

Por último, solicita AFIANZA que no se publique la resolución si finalmente procede la sanción alegando que ello facilitará identificar a las personas afectadas por la brecha, así como incentivar a la persona que sustrajo el USB a su acceso y a un posible aprovechamiento de la información en perjuicio de los afectados.

A este respecto, se indica que la presente resolución no se encuentra dentro de los supuestos contemplados en el artículo 50 de la LOPDGDD en los que es obligatorio proceder a su publicación.

Por todo lo anteriormente expuesto, se rechazan las alegaciones aducidas.

IV
Artículo 5.1.f) del RGPD

El artículo 5.1.f) "*Principios relativos al tratamiento*" del RGPD establece:

"1. Los datos personales serán:
(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)."

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas que garanticen la seguridad de los datos personales y eviten su alteración, pérdida, tratamiento o acceso no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no se garantizan la confidencialidad, la integridad y la disponibilidad de los mismos.

De ahí que la seguridad y la confidencialidad de los datos personales se consideren esenciales para evitar que los interesados sufran efectos negativos. Por ello, deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, especialmente para impedir el acceso o uso no autorizados de dichos datos y del equipo o sistema utilizados en el tratamiento.

En definitiva, es el responsable del tratamiento el que tiene la obligación de integrar las garantías necesarias en el tratamiento, con la finalidad de, en virtud del principio de responsabilidad proactiva, cumplir y ser capaz de demostrar el cumplimiento, al mismo tiempo que respeta el derecho fundamental a la protección de datos.

En el presente caso, se ha vulnerado el principio de confidencialidad pues consta que AFIANZA sufrió la sustracción de un dispositivo USB conteniendo datos personales no cifrados ***(…).***

El hecho de que el dispositivo no estuviera cifrado, encriptado, etc, es decir, sin ninguna medida o sistema para impedir el acceso no autorizado y el mismo haya sido

sustraído por un tercero, supone una vulneración de la obligación de garantizar la confidencialidad de los datos, además de reflejar un almacenamiento de datos personales en dispositivos móviles sin protección alguna de dicha información -máxime si se tiene en cuenta la tipología de datos personales tratados-, lo cual pone de manifiesto un incumplimiento de la obligación de tratarlos *de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito*.

Por tanto, de conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a AFIANZA, por vulneración del artículo 5.1.f) del RGPD.

V

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

La citada infracción del artículo 5.1.f) del RGPD supone 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. (…)"*

VI

Sanción por la infracción del artículo 5.1.f) del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone, se considera que la infracción en cuestión es muy grave a los efectos del RGPD y que procede graduar la sanción a

imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- Artículo 83.2.b) RGPD. Intencionalidad o negligencia en la infracción: Si bien se considera que no hubo intencionalidad por parte de AFIANZA, sí puede observarse la existencia de negligencia en el cumplimiento y observancia de las medidas técnicas y organizativas para garantizar la seguridad necesaria para la protección de los datos personales, concretamente para garantizar la confidencialidad de los mismos, puesto que se produjo un almacenamiento de datos personales en un dispositivo extraíble sin estar cifrados, lo que refleja una negligencia en la observancia de medidas básicas y sencillas, máxime si se tiene en cuenta que se trata de datos relativos a condenas e infracciones penales.

Procede recordar, en este sentido, la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…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 previsiones legales al respecto.

-Artículo 83.2.g) RGPD. Categorías de datos personales afectados por la infracción: Han sido afectados datos personales relativos a infracciones y sanciones penales, ***(…).***

Considerando los factores expuestos, la valoración que alcanza la cuantía de la multa por la infracción del art 5.1.f del RGPD imputada es de 90.000 € (noventa mil euros).

VII
Artículo 32 del RGPD

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"*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".

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

No debe olvidarse que, de conformidad con el artículo 32.1 del RGPD, las medidas técnicas y organizativas a aplicar para garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

En este sentido, procede señalar que la actividad de AFIANZA conlleva el tratamiento de datos relativos a condenas e infracciones penales, incluidos datos personales de personas que testifican.

En el presente caso, AFIANZA sufrió la sustracción de un dispositivo USB conteniendo datos personales ***(...)***, causando una brecha de seguridad consistente en una brecha de confidencialidad.

Como se ha expuesto de manera detallada en el apartado 2 del Antecedente de Hecho Octavo, de los hechos acaecidos y del análisis de la documentación que obra en el expediente, se deduce que se produjo el acceso de una persona ajena a la entidad a las dependencias de la misma sin que funcionaran o se observaran las medidas de seguridad implantadas y la sustracción de un dispositivo USB no cifrado (o sin ninguna otra medida de protección), conteniendo numerosos datos personales relativos a un procedimiento de investigación judicial penal.

Por tanto, ello supone un incumplimiento del artículo 32, pues el mismo se infringe tanto si no se adoptan por el responsable las medidas de índole técnica y organizativas apropiadas que garanticen la seguridad de los datos personales, como si, establecidas éstas, las mismas no se observan

Por lo expuesto, de todo ello se deduce una falta de la debida diligencia tanto en el cumplimiento de las medidas de seguridad establecidas, así como en la supervisión o comprobación de su observancia y de la idoneidad o eficacia de las mismas.

De conformidad con las evidencias de las que se dispone, se considera que los hechos conocidos son constitutivos de una infracción, imputable a AFIANZA, por vulneración del artículo 32 del RGPD.

VIII
Tipificación de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de la infracción tipificada 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:*

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". (…)

IX
Sanción por la infracción del artículo 32 del RGPD

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone, se considera que la infracción en cuestión es grave a los efectos del RGPD y que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

Como agravantes:

- Artículo 83.2.b) RGPD. Intencionalidad o negligencia en la infracción: Si bien se considera que no hubo intencionalidad por parte de AFIANZA, sí puede observarse la existencia de negligencia en el cumplimiento y observancia de las medidas técnicas y organizativas para garantizar la seguridad necesaria para la protección de los datos personales, puesto que ni los controles de acceso lógicos ni físicos existentes funcionaron por incumplimiento de los mismos, así como que se produjo un almacenamiento de datos personales en un dispositivo extraíble sin estar cifrados, lo que refleja de nuevo una negligencia en la observancia de tales medidas, máxime si se tiene en cuenta que se trata de datos relativos a condenas e infracciones penales.

Procede recordar, en este sentido, la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…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 previsiones legales al respecto.

-Artículo 83.2.g) RGPD. Categorías de datos personales afectados por la infracción: Han sido afectados datos personales relativos a infracciones y sanciones penales, ***(…)***.

Considerando los factores expuestos, la valoración que alcanza la cuantía de la multa por la infracción del art 32 del RGPD imputada es de 55.000 euros (cincuenta y cinco mil euros).

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

PRIMERO: IMPONER a AFIANZA ASESORES, S.L, con NIF B83117804, por una infracción del Artículo 5.1.f) del RGPD, tipificada en el Artículo 83.5 del RGPD, una multa de NOVENTA MIL EUROS (90.000 euros).

SEGUNDO: IMPONER a AFIANZA ASESORES, S.L, con NIF B83117804, por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, con una multa de CINCUENTA Y CINCO MIL EUROS (55.000 euros)

TERCERO: NOTIFICAR la presente resolución a AFIANZA ASESORES, S.L.

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

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

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

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

938-181022

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