- **Expediente N.º: EXP202309790**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 7 de junio de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A. y SEUR GEOPOST, S.L.*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

Expediente N.º: EXP202309790

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: Con fecha 26 de mayo de 2023, se notificó a la División de Innovación Tecnológica de esta Agencia una brecha de seguridad de los datos personales remitido por AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A. con NIF A78465267 como responsable del tratamiento.

En dicha notificación se indica lo siguiente:

Fecha de los hechos: 11/05/2023

Fecha de detección de brecha: 24/05/2023

Los hechos objeto de brecha de confidencialidad son los siguientes:

Como consecuencia de la notificación a la División de Innovación Tecnológica de esta Agencia de una brecha por parte del AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A., ***(…)***, se ordena a la Subdirección General de Inspección de Datos que realice las oportunas investigaciones previas con el fin de determinar una posible vulneración de la normativa de protección de datos.

Dicha notificación se resume del siguiente modo:

(…)

SEGUNDO: 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:

Respecto de las empresas

La entidad notificante es una sociedad anónima española filial del Grupo AXA cuya empresa matriz es AXA REAL ESTATE INVESTMENT MANAGERS S.A. Según los datos obrantes en AXESOR tiene 23 empleados y un volumen de ventas de más de 7 millones de euros y cuya actividad es "*Gestión y administración de la propiedad inmobiliaria*".

SEUR GEOPOST SLU es una sociedad limitada española matriz del grupo. Según los datos obrantes en AXESOR tiene 2094 empleados y un volumen de ventas de más de 600 millones de euros y cuya actividad es "*Otras actividades postales y de correos*".

Se ha solicitado información y documentación a la entidad notificante y a ***SEUR***, y de las respuestas recibidas se desprende lo siguiente:

Respecto de la cronología de los hechos. Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

(…).

Respecto de las causas que hicieron posible la brecha

(…).

Respecto de los datos afectados

(…).

Respecto del contrato con SEUR

(…)

Respecto de las medidas de seguridad implantadas

AXA ha remitido la siguiente documentación de seguridad:

- ***(…)***

En relación con las medidas implantadas con posterioridad al incidente:

- ***(…)***

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo

No han tenido incidencias de seguridad previos

TERCERO: La entidad AXA REAL ESTATE INVESTMENT MANAGERS S.A. cuya actividad es "*Gestión y administración de la propiedad inmobiliaria*", tiene un volumen de ventas de más de 7 millones de euros (7.843.146 euros)

FUNDAMENTOS DE DERECHO

I
Competencia

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

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

II

Cuestiones previas

El RGPD en su artículo 4 establece que "se entenderá por:

1) «datos personales»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

2) «tratamiento»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;

(…)

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;"

AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A. como responsable del tratamiento, el 26 de mayo de 2023, notificó a la División de Innovación Tecnológica de

esta Agencia una brecha de seguridad de los datos detectada el 24 de mayo de 2023, pero producida el 11 de mayo de 2023, ***(…).***

III

Artículo 32 del RGPD

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

"1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

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

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

Hay que señalar que el RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la

naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

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

"(83) A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales".

La responsabilidad del reclamado viene determinada por la falta de medidas de seguridad adoptadas para este caso concreto, con las peculiaridades que presenta, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico.

Por lo tanto, esta Agencia considera que podría haberse vulnerado el artículo 32 del RGPD, al no haberse cumplido por parte de la entidad reclamada, con la obligación de implementar medidas técnicas y organizativas de seguridad apropiadas para garantizar en este caso concreto, con las especiales características que pueda presentar, un nivel de seguridad adecuado al incluir la clave de acceso al USB en el mismo sobre.

En el presente caso, AXA remitió por mensajería postal, en un sobre, un USB con datos de 143 personas, incluidos medios de pago. El USB estaba cifrado pero la contraseña iba dentro del sobre.

Se ha indicado que el sobre vino devuelto, pero sin el USB ni la contraseña dentro.

Estos hechos evidencian una falta de medidas por incluir la contraseña en el interior del sobre.

AXA ha indicado como medidas preexistentes y medidas correctoras adoptadas las siguientes:

"1) Procedimiento interno de Seguridad de la información AXA REIM cuenta con un procedimiento de seguridad de la información implementado a nivel compañía.

En el mismo, se incluye un apartado relativo a "Transferencia de soportes físicos", en el cual se recoge la siguiente obligación para los empleados: "Cuando se transfieran físicamente datos secretos o confidenciales, se evitará en la medida de lo posible el uso de soportes físicos.

La transferencia segura de archivos debe utilizarse como medio preferente. Si se envían soportes físicos, deben cifrarse o ser sometidos a estrictos controles físicos. Los soportes cifrados deben enviarse por separado de las claves de descifrado."

Por lo tanto, de forma previa al incidente, AXA REIM había adoptado medidas destinadas a mantener la confidencialidad de los datos personales almacenados en soportes físicos.

Por otro lado, cabe hacer hincapié en que el procedimiento habitual dentro de la compañía para la transferencia de información es vía electrónica, evitándose en la medida de lo posible el envío a través de soportes físicos.

Sin embargo, en este caso concreto, y por requerimiento de la aseguradora Acquinex, fue necesario realizar, de manera puntual y aislada, el envío de la información por esta vía.

2) Formación en seguridad de la información Todos los empleados de AXA REIM, reciben la formación y concienciación apropiadas sobre las políticas y procedimientos de la empresa, según corresponda a su puesto de trabajo, así como actualizaciones periódicas de dichas políticas y procedimientos.

Concretamente, todos los empleados (incluido el que procedió a introducir el USB en el sobre) recibieron una formación inicial sobre seguridad de la información al incorporarse a AXA REIM y anualmente a partir de entonces.

No obstante, y a raíz de los últimos acontecimientos, se está realizando una evaluación interna acerca de cómo lograr transmitir de una manera más efectiva estas obligaciones a los empleados, con la finalidad de evitar, en la medida de lo posible, este tipo de actuaciones y concienciar todavía más a todo el personal.

3) Análisis de riesgos del proveedor Como procedimiento habitual, dentro de AXA REIM antes de incorporar a un nuevo proveedor, se lleva a cabo un análisis de riesgos

con el objetivo de analizar la viabilidad de su contratación y si cumple los requisitos exigidos por la normativa en protección de datos personales.

Este análisis determina el nivel de riesgo que los tratamientos que realiza el proveedor supondrán para los derechos y libertades de los interesados, con el fin de que AXA REIM analice la suficiencia de las medidas de seguridad aplicadas.

Tras la realización del correspondiente análisis de riesgos de la comunicación de los datos a SEUR, como entidad de mensajería y transporte, el resultado fue que la comunicación suponía un riesgo bajo desde el punto de vista del tratamiento de datos personales.

Habida cuenta lo anterior, AXA REIM procedió a la contratación de este proveedor que contaba con unos mecanismos de seguridad adecuados para preservan la confidencialidad de la información y privacidad de los datos.

Nuevas medidas adoptadas para la mitigación de los efectos de una potencial incidencia:

1) Sensibilización del usuario implicado A raíz del incidente de seguridad, se ha contactado con el empleado encargado de introducir la información en el sobre, para recordarle y advertirle de la importancia de cumplir con estas directrices, a lo que la persona implicada reaccionó adecuadamente, comprometiéndose a seguir las instrucciones y colaborando en todo momento para evitar futuras incidencias.

2) Vigilancia de la dark web Desde AXA REIM se ha adoptado como medida mitigadora durante 2 meses realizar una monitorización cibernética, con la finalidad de sondear la dark web a los efectos de verificar que la información y datos personales sustraídos del USB no están siendo utilizados de manera fraudulenta (suplantación de identidad, pérdidas financieras, phishing etc).

En caso de que durante este plazo de monitorización se detecte alguna similitud con la información que contenía el dispositivo USB, saltará una alerta informando de una posible actuación ilícita por parte de algún tercero.

3) Comunicación a los afectados Se ha enviado comunicación a los afectados indicando las medidas que se están adoptando en respuesta a la brecha, así como las que los propios usuarios pueden adoptar para reducir riesgos.

4) Informes y seguimiento Se hace un seguimiento continuado de la incidencia por parte del DPO y se ha realizado el presente informe de valoración del incidente por parte del equipo de Seguridad Informática de AXA REIM para actualizar la información del estado de la incidencia.

El presente informe a su vez se complementa con el reporte adjuntado como Evidencia 15, que detalla el estado de situación en relación con la 6 monitorización web de cualquier potencial filtración, así como las herramientas utilizadas.

5) Cambio de proveedor

Ante la incidencia detectada en el transporte del dispositivo USB, se ha optado por la contratación de un nuevo proveedor para la realización del envío, siendo este realizado por Correos."

Por todo ello, de conformidad con las evidencias de las que se dispone en el presente momento de acuerdo de inicio del procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que existen evidencias suficientes respecto de la ausencia de medidas de seguridad adecuadas en el tratamiento por la parte reclamada de los datos que ha incluido en el USB encriptado al incluir la clave de acceso en el mismo sobre.

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

IV
Tipificación de la infracción del artículo 32 del RGPD

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

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

> *a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43; (…)"*

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

A efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

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

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

V

Propuesta de sanción

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan**:**

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

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

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

b) la intencionalidad o negligencia en la infracción;

c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;

d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;

e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;

f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;

g) las categorías de los datos de carácter personal afectados por la infracción;

h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;

i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42,

k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción."

Por su parte, el artículo 76 "*Sanciones y medidas correctivas" de la LOPDGDD* dispone:

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

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

a) El carácter continuado de la infracción.

b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.

c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.

d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.

e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.

f) La afectación a los derechos de los menores.

g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.

h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado."

Sanción por las infracciones del artículo 32 del RGPD.

De acuerdo con los preceptos transcritos, y sin perjuicio de lo que resulte de la instrucción del procedimiento, a efectos de fijar el importe de cada sanción por cada infracción, se procede a graduar cada multa teniendo en cuenta:

Como circunstancias para tener en cuenta:

Artículo 83.2.a) RGPD: "*la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate, así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido",* ya que de los hechos objeto del presente procedimiento sancionador se desprenden deficiencias en la gestión de la entidad reclamada.

En la notificación inicial realizada por ALLIANZ sobre la brecha de seguridad producida, dicha entidad informa a la AEPD que son 150 las personas afectadas, sin embargo, seguidamente indica que ha enviado 143 notificaciones de las 150 que debería haber enviado, y en la notificación adicional remitida por ALLIANZ indica que

el número de afectados es de 800 personas.

Artículo 83.2.b) RGPD: "*intencionalidad o negligencia en el tratamiento de los datos"* ya que, se ha constatado el extravío de un medio de almacenamiento con datos personales, junto con la clave que permitía el acceso a los datos obrantes en él.

Artículo 83.2 g) RGPD *"las categorías de los datos de carácter personal afectados por la infracción"*, ya que la actividad de la entidad reclamada exige un continuo tratamiento de datos de carácter personal, entre otros, el DNI, medios de pago y el domicilio arrendado. Asimismo, la entidad reclamada realiza para el desarrollo de su actividad un elevado volumen de tratamiento de datos personales.

Considerando los factores expuestos, la valoración inicial que alcanza la cuantía de la multa es de 100.000 € por infracción del artículo 32 del RGPD, respecto a la seguridad del tratamiento de los datos personales.

VI
Responsabilidad

Establece la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, en el Capítulo III relativo a los "*Principios de la Potestad sancionadora*", en el artículo 28 la bajo la rúbrica "*Responsabilidad*", lo siguiente:

"1. 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."

La falta de diligencia a la hora de implementar las medidas apropiadas de seguridad con la consecuencia del quebranto del principio de confidencialidad constituye el elemento de la culpabilidad.

VII
Medidas

De confirmarse ambas infracciones, podrían acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En concreto en este caso las medidas consistirían en notificar en el plazo de dos meses desde la recepción de la resolución dictada, que la entidad responsable del tratamiento de datos personales se ajusta a las disposiciones del presente Reglamento, para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, así como la capacidad para restaurar la disponibilidad y el acceso a los datos

personales tras un incidente como el que nos ocupa, así como contar con un adecuado proceso de verificación, evaluación y valoración de la eficacia de tales medidas, de conformidad con el artículo 32 del RGPD.

Se advierte que no atender a los requerimientos de este organismo puede ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

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

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A., con NIF A78465267, por la presunta infracción del artículo 32 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4 del RGPD, calificada como grave y a efectos de prescripción en los artículos 73 f) de la LOPDGDD.

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

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

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de 100.000 € (cien mil euros) por infracción del artículo 32 del citado RGPD, respecto a la seguridad del tratamiento de los datos personales.

QUINTO: NOTIFICAR el presente acuerdo a AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A., con NIF A78465267, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de expediente que figura en el encabezamiento de este documento.

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

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la

sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 80.000 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en [Introduzca el texto correspondiente a 80.000 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en [Introduzca el texto correspondiente a 60.000 euros.

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

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente 80.000 o 60.000 euros, deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

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

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

En cumplimiento de los artículos 14, 41 y 43 de LPACAP, se advierte que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica por comparecencia en la sede electrónica del Punto de Acceso General de la Administración o a través de la Dirección Electrónica Habilitada única y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

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

935-110422

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

>>

SEGUNDO**:** En fecha 17 de junio de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **80000 euros** haciendo uso de una de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente. Por tanto, no ha quedado acreditado el reconocimiento de responsabilidad.

TERCERO**:** El pago realizado conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción, en relación con los hechos a los que se refiere el Acuerdo de Inicio.

CUARTO: En el Acuerdo de inicio transcrito anteriormente se señalaba que podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá "ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…".

FUNDAMENTOS DE DERECHO

I
Competencia

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

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

II
Terminación del procedimiento

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

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

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

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

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

Habiéndose procedido al pago de la sanción de carácter pecuniario, de conformidad con el apartado 2 de este artículo, el pago voluntario implica la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada. Por tanto, procede la imposición de las medidas necesarias para que cese la conducta o se corrijan los efectos de la infracción.

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

PRIMERO: DECLARAR la terminación del procedimiento **EXP202309790**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: ORDENAR a ***AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A. y SEUR GEOPOST, S.L.*** para que en el plazo de 2 meses desde que la presente resolución sea firme y ejecutiva, notifique a la Agencia la adopción de las medidas que se describen en los fundamentos de derecho del Acuerdo de inicio transcrito en la presente resolución.

TERCERO: NOTIFICAR la presente resolución a ***AXA REAL ESTATE INVESTMENT MANAGERS IBERICA S.A. y SEUR GEOPOST, S.L.***.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo

Común de las Administraciones Públicas, los interesados podrán interponer recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

1309-16012024

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