

- **Expediente N°: E/08568/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: **A.A.A.** (en adelante, la parte reclamante) con fecha 19 de abril de 2021 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra GRUPO INMOBI DESARROLLOS INMOBILIARIOS, S. L. con CIF B73976771 (en adelante, GRUPO INMOBI). Los motivos en que basa la reclamación son los siguientes:

La parte reclamante adquirió una vivienda a GRUPO INMOBI el día 14 de septiembre de 2020. En el transcurso de la mudanza encontró dos carpetas en un mueble que había quedado en la vivienda con “diversas hojas de visita, modelo normalizado de dicha inmobiliaria, en los cuales aparecen los nombres y apellidos, número de identificación, dirección, teléfono de contacto, dirección de correo electrónico y firma de las personas que habían visitado el inmueble.

Junto a la notificación se aportan hojas de visita “en blanco” (formularios sin completar) y adjunta ocho formularios con datos personales.

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

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 24 de mayo de 2021 como consta en el acuse de recibo que obra en el expediente.

No se ha recibido respuesta a este escrito de traslado.

TERCERO: Con fecha 3 de agosto de 2021, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: 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 los poderes de investigación otorgados a las autoridades de control en el artículo 58 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:

Notificación a la AEPD y comunicación a los afectados

Adjunta la parte reclamada a su escrito el documento “(...)”.

(...).

Causas del incidente

Manifiesta la parte reclamada lo siguiente en relación con las causas del incidente: “(...)”.

Número de afectados y categorías de los datos personales expuestos y uso posterior

La información facilitada por la parte reclamante incluye (...).

En relación con la posible utilización posterior de los datos, la parte reclamada en su escrito expresa lo siguiente:

(...).

Medidas de seguridad implantadas antes del incidente

En relación con las medidas de seguridad, (...).

Medidas de seguridad implantadas tras el incidente

Manifiesta la parte reclamada en su escrito que (...).

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación 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 el GRUPO INMOBI realiza, entre otros tratamientos, la recogida, registro y acceso de los siguientes datos personales de personas físicas, tales como: nombre, número de identificación, datos de localización, dirección de correo electrónico..., etc.

El GRUPO INMOBI 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 citado 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 haber tenido acceso a los datos personas no autorizadas a ello.

Hay que señalar que la identificación de una brecha de seguridad no implica la imposición de una sanción de forma directa por esta Agencia, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Dentro de los principios del tratamiento previstos en el artículo 5 del RGPD, la integridad y confidencialidad de los datos personales se garantiza en el apartado 1.f) del artículo 5 del RGPD. Por su parte, la seguridad de los datos personales viene regulada en los artículos 32, 33 y 34 del RGPD, que reglamentan 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

Seguridad del tratamiento

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 pseudonimización 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”.

En el presente caso, de la documentación aportada por el GRUPO INMOBI en el curso de estas actuaciones de investigación no se desprende que, con anterioridad a la brecha de seguridad, el GRUPO INMOBI careciera de medidas de seguridad razonables en función de los posibles riesgos estimados.

El GRUPO INMOBI, manifiesta que se ha debido a un error humano puntual por parte de uno de sus empleados y no a una falta de medidas de seguridad. Esta persona olvidó de manera accidental recoger su carpeta corporativa para almacenarla en sus instalaciones de acuerdo con las instrucciones que facilitamos a todos nuestros empleados.

El GRUPO INMOBI informa de las medidas de seguridad técnicas y organizativas que tenía implantadas antes de producirse el incidente. Las medidas son las siguientes:

(...).

Asimismo, no existen evidencias de que no hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

El GRUPO INMOBI, facilita documentación que se refiere a las medidas de seguridad implantadas tras el incidente y entre las que se encuentra (...).

Además, tras el requerimiento de información llevado a cabo por la SGID, la parte reclamada ha informado de todas las actuaciones llevadas a cabo para paliar el incidente.

Cabe destacar la buena disposición de la parte reclamada en el sentido de que, en cuanto ha tenido conocimiento del incidente, ha puesto en marcha las medidas oportunas para evitar que se pueda repetir en el futuro.

IV

Principios relativos al tratamiento

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»).”

En el presente caso, consta que los datos personales de los afectados, obrantes en la base de datos del GRUPO INMOBI, fueron indebidamente expuestos a un tercero, al haber dejado por un descuido por parte de un empleado del GRUPO INMOBI que enseñaba la vivienda, las hojas de visita con los datos personales de las personas que también visitaron el mismo inmueble que la parte reclamante. Solo se tiene constancia del acceso no autorizado a los datos por parte del reclamante.

No obstante, cabe recordar que la mera identificación de una brecha de seguridad por parte de esta Agencia no implica la comisión de una infracción en materia de protección de datos, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

Tal como se ha expuesto anteriormente, de los hechos que se deducen del expediente administrativo, no se desprende que, con anterioridad a la brecha de seguridad, el GRUPO INMOBI, careciera de medidas de seguridad razonables en función de los posibles riesgos estimados ni que no se hubiera actuado de forma diligente una vez conocida la brecha de seguridad, ni que las medidas adoptadas con posterioridad al incidente aquí analizado no fueran adecuadas.

Al respecto, el artículo 28 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público dispone que: *“Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, (...) que resulten responsables de los mismos a título de dolo o culpa”*.

En el presente caso, no ha quedado acreditado que el GRUPO INMOBI hubiera actuado de forma negligente ni, mucho menos, con dolo por su parte, por tanto, no cabe entender que se hubiera producido una infracción del artículo 5.1.f) RGPD.

V

Notificación de una violación de la seguridad de los datos personales a la autoridad de control

El artículo 33 “Notificación de una violación de la seguridad de los datos personales a la autoridad de control” del RGPD dispone:

“1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 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.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

- a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;*
- b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;*
- c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;*
- d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.*

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo”.

En el presente supuesto, se ha comprobado que era improbable que la quiebra de seguridad constituyera un riesgo para los derechos y libertades de las personas físicas, por lo que el GRUPO INMOBI estaba exenta de notificar la brecha de seguridad a esta Agencia, según lo establecido en el artículo 33 del RGPD.

El GRUPO INMOBI, manifiesta que, tras valorar la brecha de seguridad mediante un análisis de riesgo asociado a la brecha, se concluyó que no existía riesgo para los derechos y libertades de los interesados, considerando no necesaria la notificación de la brecha de seguridad a la autoridad de control.

VI

Comunicación de una violación de la seguridad de los datos personales al interesado

El artículo 34 “Comunicación de una violación de la seguridad de los datos personales al interesado” del RGPD establece:

“1. 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.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

- a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;*
- b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concrete el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;*
- c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.*

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.”

En el presente caso, no resultaba probable que la brecha de seguridad entrañara un alto riesgo para los derechos y libertades de las personas físicas, el GRUPO INMOBI, manifiesta que, tras valorar la brecha de seguridad mediante un análisis de riesgo asociado a la brecha, concluyó que no existía riesgo para los derechos y libertades de los interesados, considerando no necesaria la comunicación de los hechos a los afectados.

Además, se han tomado medidas ulteriores que garantizan que ya no existe la probabilidad de que se concretara un alto riesgo para los derechos y libertades de los interesados, por lo que el GRUPO INMOBI no estaba obligada a realizar la comunicación a los interesados de que se había producido una brecha de seguridad, en los términos del artículo 34 del RGPD.

Cabe destacar que no constan ante esta Agencia otras reclamaciones de posibles afectados, a excepción de la que ha dado origen al presente expediente.

VII Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Así pues, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **A.A.A.** y GRUPO INMOBI DESARROLLOS INMOBILIARIOS, 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, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

1245-120122

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