- Procedimiento Nº: E/09587/2019

- 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: La reclamación interpuesta por ***A.A.A.*** (en adelante, el reclamante) tiene entrada con fecha 10/06/2019 en la Agencia Española de Protección de Datos. La reclamación se dirige contra ***SAROU S.L.,*** con NIF ***B65352643*** (en adelante, el reclamado). Los motivos en que basa la reclamación son en síntesis los siguientes: que el reclamado realiza la gestión de su comunidad de vecinos; que publicaron en portal web las escrituras de tres propietarios revelando información de DNI, profesiones, estados civiles, etc., que incluso en una copia puede verse el precio que pagaron por el piso; que el 17/04/2019 se solicitó por escrito retirar esa información y que la persona responsable ha reconocido la irregularidad comprometiéndose a rectificar pero a día de hoy todo sigue igual.

Y, entre otra, anexa la siguiente documentación:

 Copia de tres escrituras de compraventa de inmuebles donde consta:
o En uno de los ficheros consta el nombre, apellidos, profesión, nacionalidad, estado civil, domicilio y nº NIE de la parte compradora y de la parte vendedora. Asimismo constan los datos de dirección, datos descriptivos y catastrales del inmueble objeto de la compraventa así como su precio.
o En uno de los ficheros consta el nombre, apellidos, profesión, nacionalidad, estado civil, domicilio y en NIF/NIE de la parte compradora y de la parte vendedora.
o En uno de los ficheros consta el nombre, apellidos, profesión, nacionalidad, estado civil, domicilio y ni NIF/NIE de la parte compradora y de la parte vendedora.
Se aportan capturas de pantalla de la web https://www.ovetauki.com/index.php?route=login con los pasos a seguir hasta localizar 3 documentos con títulos *"Escriptura Europa 75"*, *"Escriptura Europa 75.1", "Escriptura Europa 75"* junto a 3 botones con el nombre *"Descargar"* a la derecha de cada documento. Consta en la columna *"Propietario"* correspondiente a cada documento, la palabra *"GENERAL".* Para acceder a la pantalla de los documentos consta la ruta *"Propmanager/Administración de Fincas /Normativa de la Comunidad/Escritura de obra nueva y división de propiedad horizontal"*

 Se aporta copia de correo electrónico de fecha 17/04/2019 remitido por ***A.A.A. mailto:***EMAIL.1*** dirigido a ***B.B.B. ***EMAIL.2***.

 Se aporta copia de correo electrónico de fecha 18/04/2019 remitido por ***B.B.B. ***EMAIL.2*** dirigido a ***EMAIL.1.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

Con fecha 24/07/2020, el administrador de TARINAS ASSOCIATS, S.L., remite a esta Agencia la siguiente información y manifestaciones:

1. Que no son quienes administran ni han administrado la comunidad de propietarios R.R.R..

2. Que tampoco gestionan el portal web indicado.

3. Que desconocen los hechos.

Con fecha 24/07/2020, el administrador de SAROU S.L. remite a esta Agencia la siguiente información y manifestaciones:

1. Que SAROU, S.L. desde el 18/10/2019 ya no es la empresa administradora de dicha comunidad de propietarios.

Se aporta copia de *"ACTA DE LA JUNTA EXTRAORDINARIA DE COMUNIDAD DE PROPIETARIOS R.R.R. 20.00 hores del día 18/10/2019"* en la que consta que *"PRIMER.- S'aprova per UNANIMITAT la Revocació del càrrec de l'Administrador de la Comunitat designat a Tarinas Propmanager (SAROU, S.L.)"*

2. Que SAROU, S.L. utiliza un portal web subcontratado con la empresa NICHDAY DF, S.L. servicio ofertado para intercambiar información y documentación entre los vecinos y la mercantil con la finalidad de gestionar la comunidad.

Aporta copia de contrato *"CONTRATO TERCEROS CON ACCESO A DATOS (ENCARGADO DE TRATAMIENTO"* firmado a 20/12/2018 donde consta:

a. SAROU, S.L. como responsable del tratamiento.
b. NICHDAY DF, S.L. como encargado del tratamiento.
c. *"CLÁUSULAS*
PRIMERA.- Objeto del contrato e identificación de la información afectada.
[…]
Concretamente, el Encargado de Tratamiento posa a disposición del Responsable un portal Web Documental llamado Ovet Auki. Se trata de una herramienta que funciona como canal de comunicación entre los usuarios y que permite poder visualizar en la nube documentación personal de interés del Usuario, ya sea empresa, colaborador o trabajador. El portal no supone en ningún caso una herramienta para la contratación directa de los productos o servicios que presta, sino que es un instrumento para poder controlar y tener acceso directo a la documentación diaria de una manera más práctica."
d. *"SEXTA. - Medidas de seguridad*
El Encargado de Tratamiento deberá aplicar en el tratamiento de los datos, las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuada al riesgo y evitar la alteración, pérdida, tratamiento o acceso no autorizado a los ficheros de datos.
Estas medidas incluyen, entre otras:

- La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanente del sistema y servicios de tratamiento.
- La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida y en caso de incidente físico o técnico.
- Un proceso de verificación, avaluación y valoración regular de la eficiencia de las medidas técnicas y organizativas para garantizar la seguridad de los datos."
e. *"OCTAVA. - Obligaciones del Responsable de Tratamiento*
Corresponde al responsable del tratamiento:
a) Entregar al Encargado de Tratamiento los datos necesarios para la prestación del servicio, así como para el cumplimiento de las obligaciones establecidas en la cláusula séptima.
b) Velar de forma previa y durante todo el tratamiento por el cumplimiento de la normativa de protección de datos."

3. Que SAROU, S.L. está en proceso de elaborar un protocolo de conservación de datos así como de auditoría de la documentación adjuntada al portal por parte de los empleados.

4. Que SAROU, S.L. ha llevado a cabo formaciones dirigidas a sus trabajadores con el fin de que tengan un nivel suficiente de conocimiento y sensibilidad en materia de protección de datos.

5. Que todas las personas trabajadoras a las que se les encomiendan tareas en relación
a la subida de documentación al portal Ovet Auki reciben una formación inicial.

6. Se aporta copia de correo electrónico remitido por ***C.C.C.*** en fecha 18/06/2019 enviado a ******EMAIL.1*** donde consta:

"Te informo de que la Escritura de Divisón de la Propiedad Horizontal ya ha sido retirada del Portal OvetAuki. Te envío "pantallazo" del único documento que está disponible ahora mismo en el portal.
Quedamos a tu disposición por si necesitaras algo más."

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

El artículo 32 del RGPD *"Seguridad del tratamiento*", establece que:

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

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

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

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

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

III

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

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad en su sistema permitiendo el acceso a datos personales, al ser exhibidos en la página web escrituras de tres propietarios revelando información de DNI, profesión, estado civil, etc., que el precio que pagaron por el piso, con vulneración de las medidas de carácter técnico y organizativas.

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 quiebra de seguridad puesta de manifiesto por el reclamante, 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.

En el caso examinado, de la documentación obrante en el expediente se ofrecen indicios evidentes de que los sistemas de la entidad sufrieron un incidente de seguridad vulnerando el artículo 32 del RGPD, *Seguridad del tratamiento,* permitiendo el acceso por parte de los usuarios de la web a datos de los propietarios al ser publicadas escrituras de tres propietarios donde constan todos sus datos de carácter personal.

Hay que indicar que la reclamación se dirigió en un primer momento a Tarinas Associats, S.L. cuyo administrador señalo que la citada entidad no era responsable del tratamiento y que no administraba la Comunidad de Propietarios a que se hace mención en la reclamación.

Posteriormente, el mismo administrador si bien esta vez de la mercantil SAROU, S.L. señalaba que desde el 18/10/2019 ya no era la que administraba la citada comunidad de propietarios, aportando copia del acta de la junta extraordinaria de la CP de 18/10/2019 en la que figura en catalán *"S'aprova per UNANIMITAT la Revocació del càrrec de l'Administrador de la Comunitat designat a Tarinas Propmanager (SAROU, S.L.)".*

El reclamado ha señalado que tras un análisis llevado a cabo de lo sucedido se adoptaron una serie de medidas a fin de minimizar el riesgo provocado y aporta copia de correo electrónico remitido el 18/06/2019 a la dirección ****EMAIL.1* donde comunica que la Escritura de División de la Propiedad Horizontal había sido retirada del Portal OvetAuki.

Asimismo ha comunicado que utiliza un portal web subcontratado con la empresa NICHDAY para intercambiar información y documentación entre los vecinos y la mercantil con la finalidad de gestionar la comunidad estando en proceso de elaborar un protocolo de conservación de datos y la auditoría de la documentación adjuntada al portal por parte de los empleados; ha llevado a cabo acciones formativas dirigidas a sus trabajadores con el fin de que obtengan conocimientos y sensibilidad en materia de protección de datos.

También aporta el documento brecha de seguridad donde consta cual fue el origen de la quiebra, las medidas aplicadas para solucionarlo, etc.

III

Por tanto, se ha acreditado que la actuación del reclamado como entidad responsable del tratamiento ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado,

Por la Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

1. PROCEDER al ARCHIVO de las presentes actuaciones.

2. NOTIFICAR la presente resolución a ***A.A.A.*** y a TARINAS VILADRICH ADVOCATS S.L.P., con NIF ***B62178231.***

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.

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