- **Procedimiento Nº: PS/00523/2021**

RESOLUCIÓN DEL PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante la COMUNIDAD DE PROPIETARIOS R.R.R., con ***CIF.: ***NIF.1*** (en adelante, "la parte reclamada"), en virtud de denuncia presentada por ***A.A.A.***, (en adelante, "la parte reclamante"), por la presunta vulneración de la normativa de protección de datos: Reglamento (UE) 2016/679, del Parlamento Europeo y del Consejo, de 27/04/16, relativo a la Protección de las Personas Físicas en lo que respecta al Tratamiento de Datos Personales y a la Libre Circulación de estos Datos (RGPD); la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD), y atendiendo a los siguientes:

ANTECEDENTES:

PRIMERO: Con fecha 27/08/20, tuvo entrada en esta Agencia el escrito presentado por la reclamante, en el que, en esencia, se reclamaba que, para acceder a la piscina de su comunidad, le exigía la identificación como propietaria mediante la presentación de su DNI y sus datos personales que eran registrados por el vigilante de seguridad de la instalación, en un folio en blanco a la vista de todos no existiendo ningún documento junto al vigilante en el cual indicase qué se iban a hacer con esos datos.

Junto al escrito de reclamación se adjunta la siguiente documentación:

a).- Copia de circular fechada a 03/07/20 donde consta que la Junta Directiva acordó la apertura de la piscina con condiciones como la que el guarda de seguridad controle el cumplimiento de las medidas sanitarias y de aforo. No consta la necesidad de identificarse con el DNI.

b).- Copia de atestado policial Nº 10113/20, que se levantó cuando la reclamante llamó a la policía al no dejarla entrar en la piscina de la comunidad si no enseñaba su DNI.

c).- Fotografía de cartel informativo existente en la comunidad de vecinos, fechado el 24/07/20, donde constaba la siguiente información: *"es necesario que muestre su documento nacional de identidad al controlador de la piscina puesto que el registro de acceso diario a tal recinto puede ser requerido en cualquier momento por la autoridad competente por motivos de sanidad pública".*

SEGUNDO: Con fecha 07/10/20, por parte de esta Agencia y en relación con lo estipulado en el artículo 65.4 de la Ley LOPDGDD, se envió escrito a la entidad reclamada solicitándola información sobre los aspectos reseñados en la reclamación.

Según certificado de la Sociedad Estatal Correos y Telégrafos, el requerimiento enviado a la parte reclamada, el día 07/10/20, a través del servicio de notificaciones postales de Correos fue entregado en destino el día 23/10/20, identificándose el receptor con el Nº de **DNI: ***NIF.2***

TERCERO: Con fecha 08/01/21 por parte de la Directora de la Agencia Española de Protección de Datos se dicta acuerdo de admisión de trámite de la reclamación

presentada, de conformidad con el artículo 65 de la Ley LPDGDD, al apreciar posibles indicios racionales de una vulneración de las normas en el ámbito de las competencias de la Agencia Española de Protección de Datos.

CUARTO: Con fecha 08/07/21 y 21/09/21, por parte de la Subdirección General de Inspección de Datos se dirigió sendos escritos de requerimiento informativo a la parte reclamada, al amparo de los poderes de investigación otorgados a las autoridades de control en el art 57.1 del RGPD, sin que hasta la fecha respuesta alguna se haya recibido en esta Agencia con respecto a dichos requerimientos.

QUINTO: Con fecha 10/11/21, a la vista de los hechos expuestos, la Directora de la Agencia Española de Protección de Datos, acordó iniciar procedimiento sancionador a la parte reclamada por infracción del artículo 5.1.c) del RGPD, al acceder a una cantidad excesiva de datos personales de la reclamante con respecto a los fines a los que estaban destinados, imponiéndola una sanción inicial de 3.000 euros y por la Infracción del artículo 13 del RGPD, al no informar convenientemente a los usuarios de la piscina de la comunidad del tratamiento que se iba a hacer de sus datos personales, cuando accedían a la piscina comunitaria, con una sanción inicial de 3.000 euros.

SEXTO: Notificada la incoación del expediente el 10/01/22 a la Comunidad de Vecinos, a fecha de hoy, no consta que la parte reclamada haya formulado alegaciones al acuerdo de inicio del procedimiento.

En este sentido, el artículo 64.2.f) de la LPACAP -disposición de la que se informó la reclamada en el acuerdo de apertura del procedimiento- establece que, *"si no se efectúan alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, cuando éste contenga un pronunciamiento preciso acerca de la responsabilidad imputada, podrá ser considerado propuesta de resolución"*.

En el presente caso, el acuerdo de inicio del expediente sancionador determinaba los hechos en los que se concretaba la imputación, la infracción a la normativa vigente atribuida a la reclamada y la sanción que podría imponerse. Por ello, tomando en consideración que la reclamada no ha formulado alegaciones al acuerdo de inicio del expediente y en atención a lo establecido en el artículo 64.2.f) LPACAP, el citado acuerdo de inicio es considerado en el presente caso propuesta de resolución.

HECHOS PROBADOS

1º.- La reclamante indica en su escrito que, siendo propietaria de la vivienda sita en ******DIRECCION.1*** desde hace 15 años, al intentar hacer uso de la piscina comunitaria, el vigilante de seguridad contratado por la comunidad de vecinos le solicitó que mostrase el DNI para acceder a la piscina, a lo que ella se negó al ser propietaria y estar correctamente identificada. Así las cosas, la reclamante le solicitó al vigilante de seguridad que le informase el propósito de recoger los datos personales y que le ensañara el escrito donde estaba esa norma.

2º.- La reclamante sigue indicando que, puesto en contacto con el presidente de la comunidad, éste la manifestó que era obligatorio para acceder al recinto presentar el DNI y que existía una ley del Ministerio de Sanidad que estaba muy por encima de la Ley de Protección de Datos, ya que existía la posibilidad de que se produjese un brote

del “COVID”, y el Ministerio le obligaba a pedir el DNI para poder después ponerse en contacto con los vecinos e informales de que habían estado en contacto, por lo que, si no enseñaba su DNI la prohibía acceder a la piscina de la comunidad.

3º.- Puesto en contacto con el administrador de la finca le manifestó que esta medida por el “COVID19”, fue tomada exclusivamente por decisión de la Junta directiva de la comunidad de vecinos, nunca por Junta de Vecinos, como obligatoriamente debía de haber ocurrido.

4º.- Unos días después intentó volver a acceder a la piscina de la comunidad, pero no la permitieron el acceso al negarse a mostrar el DNI, por lo que requirió la presencia de la policía, que levantó atestado de los hechos con número: Nº 45668/2020.

5º.- Además, la reclamante indica que, cuando los propietarios accedían a la piscina y presentaban su DNI al vigilante de seguridad, éste apuntaba los datos de la persona que accedía en un folio en blanco a la vista de todos y que no existía ningún documento junto al vigilante en el cual informase de la gestión que se iba a realizar con esos datos.

6º.- Por parte de esta Agencia, se ha enviado hasta tres escritos a la Comunidad de Propietarios solicitando información sobre los hechos indicados por la reclamante sin que en ninguno de ellos se haya recibido respuesta alguna en esta Agencia. Tampoco se ha recibió ningún escrito de alegaciones a la incoación del procedimiento sancionador.

FUNDAMENTOS DE DERECHO

I.- Competencia

Es competente para resolver este Procedimiento Sancionador, la Directora de la Agencia Española de Protección de Datos, en virtud de los poderes que el art 58.2 del RGPD y arts. 47, 64.2 y 68.1 de la Ley LOPDGDD.

II.- Sobre el tratamiento de datos personales resultantes de la situación derivada de la extensión del virus COVID-19,

Ante la situación de emergencia de salud pública derivada de la extensión del COVID19, la Agencia Española de Protección de Datos elaboró varios documentos en relación con ello para dar respuesta a las dudas que surgían con la situación que se vivía en el año 2020. Así, el informe del Gabinete Jurídico de la AEPD, con N/REF: 0017/2020 indicaba, al respecto, lo siguiente:

“En primer lugar, con carácter general, debe aclararse que la normativa de protección de datos personales, en tanto que, dirigida a salvaguardar un derecho fundamental, se aplica en su integridad a la situación actual, dado que no existe razón alguna que determine la suspensión de derechos fundamentales, ni dicha medida ha sido adoptada.

Sin perjuicio de lo anterior, el propio RGPD contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la epidemia, en que existe una emergencia sanitaria de alcance

general. Por ello, al aplicarse dichos preceptos previstos para estos casos en el RGPD, en consonancia con la normativa sectorial aplicable en el ámbito de la salud pública, las consideraciones relacionadas con la protección de datos -dentro de los límites previstos por las leyes- no deberían utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades, especialmente las sanitarias, en la lucha contra la epidemia, por cuanto ya la normativa de protección de datos personales contiene una regulación para dichos casos que compatibiliza y pondera los intereses y derechos en liza para el bien común.

El Considerando (46) del RGPD ya reconoce que, en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público, como en el interés vital del interesado u otra persona física. (46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente.

Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano.

Por lo tanto, como base jurídica para un tratamiento lícito de datos personales, sin perjuicio de que puedan existir otras bases, -como por ejemplo el cumplimiento de una obligación legal, art. 6.1.c) RGPD, el Reglamento reconoce explícitamente las dos citadas: misión realizada en interés público (art. 6.1.e) o intereses vitales del interesado u otras personas físicas, (art. 6.1.d).

El art. 6.1, letra d) RGPD considera no sólo que el interés vital es suficiente base jurídica del tratamiento para proteger al "interesado" (en cuanto que este es un término definido en el art. 4.1) RGPD como persona física identificada o identificable), sino que dicha base jurídica puede ser utilizada para proteger los intereses vitales "de otra persona física", lo que por extensión supone que dichas personas físicas pueden ser incluso no identificadas o identificables; es decir, dicha base jurídica del tratamiento (el interés vital) puede ser suficiente para los tratamientos de datos personales dirigidos a proteger a todas aquellas personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría, desde el punto de vista de tratamiento de datos personales, en la manera más amplia posible, las medidas adoptadas a dicho fin, incluso aunque se dirijan a proteger personas innominadas o en principio no identificadas o identificables, por cuanto los intereses vitales de dichas personas físicas habrán de ser salvaguardados, y ello es reconocido por la normativa de protección de datos personales.

El apartado 3 del artículo 6 RGPD no establece la necesidad de que la base del tratamiento por razón de interés vital haya de ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros aplicables al responsable del tratamiento, pues dicho apartado se refiere exclusivamente a los tratamientos establecidos para el cumplimiento de una obligación legal, o para el cumplimiento de

una misión realizada en interés público o en el ejercicio de poderes públicos, ambas referidas en las letras c) y e) de dicho artículo 6 RGPD, pero no para los tratamientos incluidos en la letra d). c. Sin embargo, para el tratamiento de datos de salud no basta con que exista una base jurídica del art. 6 RGPD, sino que de acuerdo con el art. 9.1 y 9.2 RGPD exista una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos (entre ellos, datos de salud).

(…) En una situación de emergencia sanitaria como a la que se refiere la solicitud de este informe, es preciso tener en cuenta que, en el exclusivo ámbito de la normativa de protección de datos personales, la aplicación de la normativa de protección de datos personales permitiría adoptar al responsable del tratamiento aquellas decisiones que sean necesarias para salvaguardar los intereses vitales de las personas físicas, el cumplimiento de obligaciones legales o la salvaguardia de intereses esenciales en el ámbito de la salud pública, dentro de lo establecido por la normativa material aplicable.

Cuáles sean dichas decisiones, (desde el punto de vista de la normativa de protección de datos personales, se reitera) serán aquellas que los responsables de los tratamientos de datos deban de adoptar conforme a la situación en que se encuentren, siempre dirigida a salvaguardar los intereses esenciales ya tan reiterados. Pero los responsables de tratamientos, al estar actuando para salvaguardar dichos intereses, deberán actuar conforme a lo que las autoridades establecidas en la normativa del Estado miembro correspondiente, en este caso España, establezcan.

Así, el legislador español se ha dotado de las medidas legales necesarias oportunas para enfrentarse a situaciones de riesgo sanitario, como la Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública (modificada mediante Real Decreto-ley 6/2020, de 10 de marzo, por el que se adoptan determinadas medidas urgentes en el ámbito económico y para la protección de la salud pública, publicado en el Boletín Oficial del Estado de 11 de marzo de 2020) o la Ley 33/2011, de 4 de octubre, General de Salud Pública.

El artículo 3 de la primera de dichas normas señala que: [c]on el fin de controlar las enfermedades transmisibles, la autoridad sanitaria, además de realizar las acciones preventivas generales, podrá adoptar las medidas oportunas para el control de los enfermos, de las personas que estén o hayan estado en contacto con los mismos y del medio ambiente inmediato, así como las que se consideren necesarias en caso de riesgo de carácter transmisible. Del mismo modo, los artículos 5 y 84 de la Ley 33/2011, de 4 de octubre, General de Salud Pública se refieren a la anterior Ley orgánica 3/1986, y a la posibilidad de adoptar medidas adicionales en caso de riesgo de transmisión de enfermedades.

Por lo tanto, en materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitarias etc., la normativa aplicable ha otorgado "a las autoridades sanitarias de las distintas Administraciones públicas" (art. 1 Ley Orgánica 3/1986, de 14 de abril) las competencias para adoptar las medidas necesarias previstas en dichas leyes cuando así lo exijan razones sanitarias de urgencia o necesidad. En consecuencia, desde un punto de vista de tratamiento de datos personales, la salvaguardia de intereses esenciales en el ámbito de la salud pública corresponde a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las

medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública.

Serán estas autoridades sanitarias competentes de las distintas administraciones públicas quienes deberán adoptar las decisiones necesarias, y los distintos responsables de los tratamientos de datos personales deberán seguir dichas instrucciones, incluso cuando ello suponga un tratamiento de datos personales de salud de personas físicas. Lo anterior hace referencia, expresamente, a la posibilidad de tratar los datos personales de salud de determinadas personas físicas por los responsable de tratamientos de datos personales, cuando, por indicación de las autoridades sanitarias competentes, es necesario comunicar a otras personas con las que dicha persona física ha estado en contacto la circunstancia del contagio de esta, para salvaguardar tanto a dichas personas físicas de la posibilidad de contagio (intereses vitales de las mismas) cuanto para evitar que dichas personas físicas, por desconocimiento de su contacto con un contagiado puedan expandir la enfermedad a otros terceros (intereses vitales de terceros e interés público esencial y/o cualificado en el ámbito de la salud pública).

Ahora bien, los tratamientos de datos personales en estas situaciones de emergencia sanitaria, como se ha mencionado al principio de este informe, siguen siendo tratados de conformidad con la normativa de protección de datos personales (RGPD y Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, LOPDGDD), por lo que se aplican todos sus principios, contenidos en el artículo 5 RGPD, y entre ellos el de tratamiento de los datos personales con licitud, lealtad y transparencia, de limitación de la finalidad (en este caso, salvaguardar los intereses vitales/esenciales de las personas físicas), principio de exactitud, y por supuesto, y hay que hacer especial hincapié en ello, el principio de minimización de datos.

Sobre este último aspecto hay que hacer referencia expresa a que los datos tratados habrán de ser exclusivamente los limitados a los necesarios para la finalidad pretendida, sin que se pueda extender dicho tratamiento a cualesquiera otros datos personales no estrictamente necesarios para dicha finalidad, sin que pueda confundirse conveniencia con necesidad, porque el derecho fundamental a la protección de datos sigue aplicándose con normalidad, sin perjuicio de que, como se ha dicho, la propia normativa de protección de datos personales establece que en situaciones de emergencia, para la protección de intereses esenciales de salud pública y/o vitales de las personas físicas, podrán tratarse los datos de salud necesarios para evitar la propagación de la enfermedad que ha causado la emergencia sanitaria.

Respecto del principio de limitación de la finalidad en relación con supuestos de tratamientos de datos de salud por razones de interés público, el Considerando (54) RGPD es claro, cuando establece que: El tratamiento de categorías especiales de datos personales, sin el consentimiento del interesado, puede ser necesario por razones de interés público en el ámbito de la salud pública. Ese tratamiento debe estar sujeto a medidas adecuadas y específicas a fin de proteger los derechos y libertades de las personas físicas. […] Este tratamiento de datos relativos a la salud por razones de interés público no debe dar lugar a que terceros, como empresarios, compañías de seguros o entidades bancarias, traten los datos personales con otros fines".

III.- Sobre la recogida excesiva de datos personales para poder acceder a la piscina de la comunidad de vecinos:

En el presente caso, la reclamante manifiesta que, tras negarse a presentar el DNI para acceder a la piscina de su comunidad pues consideraba que era excesivo presentar el DNI al vigilante, pues al ser propietaria, con una antigüedad de más de 15 años, estaba suficientemente identificada. Que se puso en contacto con el presidente de la comunidad para denunciar el caso a lo que éste le manifestó que era obligatorio, para acceder al recinto, presentar el DNI y que existía una ley del Ministerio de Sanidad que estaba muy por encima de la Ley de Protección de datos, ya que, si existiera un brote del covid19, el Ministerio le obliga a pedir el DNI para poder después localizar a los vecinos en caso de contagio.

Respecto al uso excesivo de datos personales, el considerando 39 del RGPD establece que: *"(…) Todos los tratamientos de datos personales deben ser adecuados, pertinentes y limitados a lo necesario para los fines para los que sean tratados. Ello requiere, en particular, garantizar que se limite a un mínimo estricto su plazo de conservación. Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios. Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica. Deben tomarse todas las medidas razonables para garantizar que se rectifiquen o supriman los datos personales que sean inexactos. Los datos personales deben tratarse de un modo que garantice una seguridad y confidencialidad adecuadas de los datos personales, inclusive para impedir el acceso o uso no autorizados de dichos datos y del equipo utilizado en el tratamiento".*

Por su parte, el artículo 5.1.c) del RGPD establece los Principios relativos al tratamiento, indicando respecto a esto que: *"Los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);*

Pues bien, aunque en la situación de pandemia que se vivió en el año 2020, las autoridades sanitarias competentes adoptaron las medidas necesarias para atajar la pandemia, y por tanto, los distintos responsables de los tratamientos de datos personales debieron seguir dichas instrucciones, incluso cuando ello supuso un tratamiento de datos personales de salud, en caso de que hubiera sido necesario comunicar a otras personas un posible brote en su entorno con el objetivo de salvaguardar la salud de todos, el hecho de pedir los datos personales incluidos en el DNI de la reclamante, resulta excesivo a los fines para los que estaban destinados, pues al ser propietaria de una vivienda en la comunidad con una antigüedad de más de 15 años, estaba suficientemente identificada incluso, solamente con la indicación del portal, piso y letra, por ejemplo.

Por tanto, los hechos expuestos son claramente constitutivos de una infracción, imputable a la parte reclamada, por vulneración del artículo 5.1.c) del RGPD, al solicitar a la reclamante más datos personales de los estrictamente necesarios para el fin que se perseguía.

En este sentido, el artículo 72.1.a) de la LOPDGDD tipifica, a efectos de prescripción, como “muy grave”, el: *“tratamiento de los datos personales vulnerando los principios y garantías establecido en el artículo 5 del RGPD”.*

Esta infracción puede ser sancionada según lo establecido en el artículo 83.5.b) del RGPD, donde se establece que: *“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 derechos de los interesados a tenor de los artículos 12 a 22”.*

De acuerdo con los preceptos indicados a efectos de fijar el importe de la sanción a imponer, se considera que procede graduar la sanción de acuerdo con el siguiente criterio agravante que establece el artículo 83.2 del RGPD:

a).- La duración de la infracción, pues se constata, según la reclamante y el acta policial que la comunidad de vecinos pedía los datos personales de todos aquellos que, durante la época estival del año 2020, hacían uso de las instalaciones de la piscina de la comunidad de vecinos (apartado a).

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en su artículo 5.1.c) del RGPD, permite fijar una sanción de 3.000 euros, (tres mil euros).

IV.- Sobre la falta de información facilitada a los usuarios de la piscina cuando se les pedía el DNI para acceder a la piscina de la comunidad:

Según la reclamante, cuando los propietarios accedían a la piscina de la comunidad y presentaban su DNI, el vigilante de seguridad apuntaba los datos personales de la persona que accedía en un folio en blanco a la vista de todos, no existiendo ningún documento junto al vigilante que informara sobre el tratamiento de los datos personales. Tampoco se informaba a los usuarios de la instalación sobre la gestión que posteriormente se realizaría con los datos personales obtenidos de los DNI.

Respecto a la información que el responsable del tratamiento de los datos personales debe proporcionales a los interesados cuando obtienen sus datos personales, el artículo 13 del RGPD, establece lo siguiente:

“1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará:

a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;

b) los datos de contacto del delegado de protección de datos, en su caso;

c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;

d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;

e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;

f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:

a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;

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

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

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

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

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

Por tanto, atendiendo a lo expuesto, los hechos conocidos son constitutivos de una infracción, imputable al reclamado, por vulneración del artículo 13 del RGPD, al no informar convenientemente de la gestión que se realizaba con los datos personales obtenidos cuando se accedía a la piscina comunitaria.

En este sentido, el artículo 72.1.h) de la LOPDGDD, considera muy grave, a efectos de prescripción, *"la omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del RGPD"*

Esta infracción puede ser sancionada según lo establecido en el artículo 83.5.b) del RGPD, donde se establece que: *"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 derechos de los interesados a tenor de los artículos 12 a 22".*

De acuerdo con los preceptos indicados a efectos de fijar el importe de la sanción a imponer, se considera que procede graduar la sanción de acuerdo con el siguiente criterio agravante que establece el artículo 83.2 del RGPD:

a).- La duración de la infracción, pues se constata, según la reclamante y el acta policial que la comunidad de vecinos pedía los datos personales de todos aquellos que, durante la época estival del año 2020, hacían uso de las instalaciones de la piscina de la comunidad de vecinos (apartado a).

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en su artículo 13 del RGPD, permite fijar una sanción de 3.000 euros, (tres mil euros).

V.- Sanción Total

El balance de las circunstancias contempladas en los puntos anteriores permite fijar una sanción total de 6.000 euros (seis mil euros): 3.000 euros por la infracción del artículo 5.1.c) del RGPD y 3.000 euros por la infracción del artículo 13 del RGPD.

A tenor de lo anteriormente expuesto, por la Directora de la Agencia Española de Protección de Datos,

RESUELVE:

PRIMERO: IMPONER a la COMUNIDAD DE PROPIETARIOS R.R.R.**,** con CIF.: ******NIF.1,*** las siguientes sanciones:

a).- Sanción de 3.000 euros (tres mil euros) por la infracción del artículo 5.1.c) del RGPD,

b).- Sanción de 3.000 euros (tres mil euros) por la Infracción del artículo 13 del RGPD,

SEGUNDO: NOTIFICAR la presente resolución a la COMUNIDAD DE PROPIETARIOS R.R.R.**.**

TERCERO: Advertir al sancionado que la sanción impuesta deberá hacerla efectiva una vez sea ejecutiva la presente resolución, de conformidad con lo dispuesto en el artículo 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en el plazo de pago voluntario que señala el

artículo 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 en la cuenta restringida ***Nº ES00 0000 0000 0000 0000 0000***, abierta a nombre de la Agencia Española de Protección de Datos en el Banco CAIXABANK, S.A. o en caso contrario, se procederá a su recaudación en período ejecutivo.

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

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

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.6 de la LOPDGDD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

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

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