

- **Expediente N.º: PS/00413/2022**

### RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

#### ANTECEDENTES

PRIMERO: Doña **A.A.A.**, (en adelante, la parte reclamante), con fecha 14/05/2021, interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **METROPOLITAN SPAIN, S.L.**, con NIF **B62936737** (en adelante, la parte reclamada).

Los motivos en que basa la reclamación son los siguientes:

La parte reclamante es socia del gimnasio METROPOLITAN CLUB, en c/ Cisneros 67 de Santander. Se incorporó a ese centro en septiembre de 2020, y hasta el día 6/05/2021, se accedía mediante una pulsera y una tarjeta identificativa en el ordenador de recepción. Desde la citada fecha, se ha impuesto como requisito a los usuarios o el acceso a sus instalaciones mediante huella dactilar. Se ha negado a ceder los datos de su huella, al entender que se trata de una petición excesiva de datos biométricos y le han comunicado que van a dar de baja como socia, sin más alternativa.

Aporta copia de hoja de reclamación ante Consumo de 6 de mayo del 2021, ejemplar para enviar por el reclamante en 10 días a la D. Gral. que señala el formulario, sin que conste su presentación.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5/12, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a la parte reclamada, 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 1/10, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 7/06/2021, 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 14/08/2021, de conformidad y a efectos del artículo 65.5 de la LOPDGDD, la reclamación se consideró admitida a trámite.

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 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:

Como consecuencia del requerimiento de información efectuado por la inspección a **METROPOLITAN SPAIN, S.L.**, con fecha **21/03/2022**, **METROPOLITAN SPAIN, S.L.** remite a esta Agencia la siguiente información y manifestaciones:

1. Indican que aportan información de METROPOLITAN al haber sido requerida, pero que acompañan otra información de LLEFISA SL, que es al titular del CLUB AQUA FLORANES donde la reclamada fue socia de 2/09/2020 a 1/06/2021. Indica que *“la biometría se instaló en dicho Club en febrero 2021 como único modo de acceso unido a la pulsera”* (punto 23 de su respuesta).

2. Precisa METROPOLITAN que, si bien el tratamiento de datos de salud está en principio prohibido, que el artículo 9.2.a) del RGPD señala la excepción, limitándose a citarlo. Añade que: *“la base de legitimación (artículo 6 del RGPD) en que se amparan estos tratamientos de datos personales, en este caso es el consentimiento del interesado al facilitar su huella para establecer el patrón biométrico y al firmar la normativa de socios donde se informa de dicho tratamiento.”*

3. Aporta COPIA DE ESCRITO DE “METROPOLITAN SPORT CLUB & SPA”, (en lo sucesivo, el contrato) figurando la referencia en margen derecho a LLEFISA SL. Se contienen los datos personales de la reclamante. Así, en la parte “objeto del contrato” “fecha de alta” 2/09/2020”.

Consta que la titular de la cuenta bancaria que figura autoriza a LLEFISA a realizar el cargo del pago de la cuota contratada.

También consta:

- “*PROTECCIÓN DE DATOS: De acuerdo con la normativa vigente en protección de datos, podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, así como revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a LLEFISA, SL., en C/ Cisneros nº 67, 39007 Santander o al mail dpo@clubmetropolitan.net. “Podrá presentar reclamación ante la AEPD”.*

-Informa de la “NORMATIVA METROPOLITAN AQUA”, que inicia con:

*“1. Por mediación del presente documento, LLEFISA, S.L. (METROPOLITAN AQUA-FLORANES) prestará los servicios de utilización de sus instalaciones y maquinaria deportiva con acceso al centro sito en C/ Cisneros nº 67, 39007 Santander”*

-En su punto 5, de “información y funcionamiento del Club”: “Todos los socios disponen de una pulsera personal e intransferible. Para poder acceder a las instalaciones es necesario el uso de un sistema biométrico junto con la pulsera de acceso.

-Se alude a la condición de socio de METROPOLITAN, y se mencionan otros centros e instalaciones de METROPOLITAN en otras ciudades pudiendo tener acceso en los mismos.

4. Aporta también, un documento firmado por reclamante sobre: “AUTORIZACIÓN AL TRATAMIENTO DE DATOS PERSONALES” (en lo sucesivo, cláusula protección de datos) donde consta que:

*“Le informamos que LLEFISA, SL cumple todos los requisitos establecidos en la normativa de Protección de Datos de carácter personal, RGPD 2016/679 (UE) y que todos los datos bajo nuestra responsabilidad vienen siendo tratados de acuerdo con las exigencias legales, guardándose las debidas medidas de seguridad que garanticen la confidencialidad de los mismos.*

*Los datos personales que ha facilitado de nombre y apellidos, DNI, dirección postal y/o electrónica, así como el número de su tarjeta de crédito, serán tratados por LLEFISA SL, SL, con CIF B60422417 en c/ Cisneros nº 67, 39007-SANTANDER con la finalidad de gestionar su solicitud de incorporación como socio del gimnasio y finalidades inherentes como la gestión y cobro de recibos, la entrada en las instalaciones, la participación en eventos y máster class, etc.*

*Con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones, METROPOLITAN opta por un sistema de acceso mediante el registro biométrico (código hash encriptado) y una pulsera personal que complementará el uso biométrico... Dichos datos biométricos no serán objeto de tratamiento en ningún caso por parte de METROPOLITAN.*

*La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro, y que en caso de no aceptarse nos impide prestar el servicio al socio. De acuerdo con la normativa vigente en protección de datos, podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, así como revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a LLEFISA SL, c/ Cisneros nº 67, 39007-Santander.”*

5. Manifiesta METROPOLITAN que “La finalidad del tratamiento es el acceso inequívoco e intransferible del usuario a las instalaciones del gimnasio.”

6. En relación con el funcionamiento del sistema y al proceso de acceso, manifiesta METROPOLITAN:

- La ficha del usuario se almacena en el software PROVIS, el patrón se genera a través del algoritmo de encriptación, conocido solo por el fabricante NITGEN, imposibilitando que se pueda recuperar externamente para cálculo o reconstrucción de la huella.
- “Cuando el usuario accede al gimnasio, se valida primero con una pulsera RFID. Una vez pasada la pulsera e identificado el usuario, si este tiene registrado en el sistema la necesidad de comprobar su patrón de huella construye

*en tiempo real un nuevo patrón-que no se guarda- y que se compara 1 a 1 con el patrón almacenado."*

A partir de la baja de un socio, ya no se conserva su patrón de huella.

*"Actualmente los usuarios no tienen otro sistema de acceso a las instalaciones del gimnasio."*

7. Aporta la siguiente documentación:

7.1- REGISTRO DE ACTIVIDADES DEL TRATAMIENTO (RAT) DE LA ACTIVIDAD "GESTIÓN ACCESO SOCIOS A CLUB", donde consta, entre otros, que:

- a. El responsable del tratamiento es LLEFISA S.L.
- b. El ejercicio de derechos se realiza frente a METROPOLITAN SPAIN S.L., difiriendo del contenido que figura en la información proporcionada a la reclamante.
- c. El encargado del tratamiento es PROYECTOS VISUALES ZARAGOZA S.L.
- d. La base jurídica es el contrato mercantil y el consentimiento.
- e. Que la finalidad del tratamiento es la gestión de los datos personales de los abonados para permitirles el acceso a la instalación.
- f. Que entre los datos tratados consta la huella dactilar.
- g. Que en el apartado de "*Periodo de conservación de los datos*" consta: "*Durante la vigencia de la condición de socio. Cuando se cause baja por cualquier motivo el socio entregará la pulsera de acceso y se eliminarán.*"

En el apartado de "*categorías de destinatarios*", figura que "*no se prevén*", igual que respecto a "*transferencia internacional de datos*".

7.2- ANÁLISIS DE RIESGOS, fechado a 30 de enero de 2020, figura referencia a que el análisis "realizado por METROPOLITAN SPAIN SL", y en el margen figura el nombre de la Compañía que lo realiza. En el apartado de "RIESGOS DE CUMPLIMIENTO NORMATIVO" y en el apartado "*asociados al cumplimiento normativo*" indica que se trata del uso de la huella digital, y, además:

- "*RIESGO: No facilitar toda la información requerida por los apartados 1 y 2 del art. 13 en el momento de recoger los datos, cuando se obtengan del interesado*

*¿Por qué? La cláusula informativa facilitada por la empresa para el tratamiento de datos biométricos es completa, pero en algunos casos se deberá explicar personalmente.*

*Medidas correctoras: Facilitar información completa. Tener en cuenta que la información debe facilitarse también a los socios ya existentes".*

7.3- EVALUACIÓN DE IMPACTO, fechada a 5/02/2021, "*Metropolitan Spain SL*", "*AQUA FLORANES. Santander, perteneciente a LLEFISA SA. Sistema de apertura mediante control biométrico*" (pág. 48 punto 6) realizado por la misma empresa que el análisis de riesgos visto en el punto 7.2, firmado por DPD de METROPOLITAN. Consta que:

*“la EIPD se realiza sobre el tratamiento de los datos de los socios del responsable del tratamiento con la finalidad de controlar el acceso al gimnasio. Los datos tratados son la huella dactilar o aquellos datos identificativos necesarios a incluir en la pulsera de identificación del socio, con la finalidad de que el sistema reconozca al interesado y permita, mediante esta identificación, acceder al gimnasio. Asimismo, se identifica fecha y hora del acceso”*

*“2.- Procedimiento de comparación de los datos captados con los datos almacenados El usuario (socio) cuando accede al gimnasio se valida primero con una pulsera RFID. Una vez pasada la pulsera e identificado el usuario, si éste tiene registrado en el sistema la necesidad de comprobar su patrón de huella construye en tiempo real un nuevo patrón que se compara uno a uno con el patrón almacenado a través de los algoritmos internos de NitGen. Este patrón es generado en tiempo real y no se guarda”*

*“3.- Criterios para la codificación y el almacenamiento de la información captada Se almacena en el perfil del usuario un patrón generado a través del algoritmo de encriptación en posesión del fabricante NitGen. No se almacenan datos en bruto.”*

Según indica el informe, LLEFISA es responsable del tratamiento en el gimnasio al que pertenecía la reclamada y en el de “Palacio Santa Ana Madrid”. También alude a otros gimnasios en los que el responsable es METROPOLITAN.

a. Existe un riesgo residual para los derechos y libertades que no excede de un nivel medio.

b. Que, con relación a la necesidad y proporcionalidad del tratamiento, manifiesta que:

*“Partiendo del cumplimiento de una de las condiciones de licitud del tratamiento tasadas en el artículo 6, numeral 1º letra b), dado que el mismo se produce como actividad encuadrada dentro de la ejecución del contrato de socio, que el socio lee y firma en el momento de darse de alta como socio y que regula la relación entre el interesado, el socio, y el responsable del tratamiento, el Club METROPOLITAN AQUA FLORANES, debemos analizar la necesidad y la proporcionalidad de este tratamiento.*

*A lo anterior, hay que añadir que los datos son recogidos para el acceso y uso del gimnasio y los socios no pueden ser identificados para otros fines distintos a dicho acceso, permaneciendo en tanto que socios del gimnasio; en el contrato se informa del procedimiento de huella digital y si el cliente está conforme firma el contrato y accede al Club, y si no está conforme, no pasa a ser socio. “*

7.4- Aporta copia de contrato de encargo del tratamiento, firmado y fechado a 30 de diciembre de 2018, siendo el responsable del tratamiento LLEFISA. S.L., (Metropolitan Aqua Floranes) y encargado del tratamiento PROYECTOS VISUALES ZARAGOZA S.L. En el mismo constan, entre otros apartados:

a. El objeto del encargo es el servicio de instalación y mantenimiento de la aplicación de gestión y control de acceso a las instalaciones deportivas.

b. Que el encargado deberá tratar los datos existentes en la aplicación PROVISPORT cuyo contenido habitual son datos de socios y usuarios del Club de “las siguientes tipologías: datos de identificación y contacto, accesos biométricos al club deportivo (có-

*digos hash) ...”*

7.5.- Informe de “octubre 2019” firmado por la DPD de METROPOLITAN, sobre “viabilidad de la implantación de un sistema biométrico para acceder a las instalaciones de los centros Metropolitan”. Entre otras indicaciones señala que a los datos relativos a huellas dactilares se les debe aplicar el régimen previsto para las categorías especiales de datos previsto tanto en el artículo 9 como en otros artículos del RGPD. De acuerdo con estas consideraciones, el tratamiento de datos biométricos requerirá no solo la concurrencia de una de las bases jurídicas establecidas en el art. 6 del RGPD, sino que, también deberán concurrir alguna de las excepciones previstas en el art. 9.2 del RGPD.

7.6- Escrito de *NITGEN Biometrics Solutions*, de NITGEN Co, Ltd., con sede en Corea del Sur, sobre los datos de la huella extraídos por sus lectores. Indica que “no pueden ser descifrados ni desmontados por ninguna entidad no autorizada”, y que “las únicas claves para el algoritmo están en posesión de NITGEN y no están disponibles para el personal que distribuyen o compara el equipo” “Una vez escaneado y convertido al patrón de huella de NITGEN, la imagen escaneada se destruye. Todo lo que queda es un modelo matemático que no puede ser decodificado para obtener la imagen de la huella original”.

- “Que el número total de personas con huellas dactilares almacenadas actualmente son 1356.”, que coincide con el número total de usuarios dados de alta.

QUINTO: Como consecuencia del requerimiento de información efectuado a METROPOLITAN SPAIN, S.L., por la inspección, con fecha 10/05/2022, la citada entidad, remite a esta Agencia la siguiente información y manifestaciones:

1.Aporta copia de “contrato de corresponsabilidad” entre LLEFISA S.L. (METROPOLITAN AQUA FLORANES), y METROPOLITAN SPAIN, S.L., firmado y fechado a 25 de mayo de 2018.

En el EXPONEN, figura:

*“Ambas empresas han determinado conjuntamente los objetivos y los medios del tratamiento, por lo que son consideradas corresponsales del tratamiento de los socios del Club deportivo AQUA FLORANES”*

En cláusulas, primera, figuran marcadas cruces en:

*“Objetivo común con respecto al procesamiento”*

*“Procesamiento de datos personales para el mismo propósito”*

*“Utilización del mismo conjunto de datos personales - base de datos de socios-para el procesamiento entre ambos responsables”*

*“Diseño del proceso conjunto”*

*“Reglas comunes de manejo de información entre ambos responsables”*



En la segunda, se indica que son corresponsables respecto del tratamiento de datos personales relativos a la gestión de socios del “CLUB AQUA FLORANES.” “los tratamientos a realizar son”: alta y baja socio, control acceso a instalaciones y gestión cuotas.

En la cláusula tercera: “Obligaciones de los corresponsables del tratamiento”, se indica.

- Los corresponsables se obligan a responder a los interesados ante el ejercicio de sus derechos ante cualquiera.

- “Los corresponsales en el momento de la recogida de los datos, deben facilitar la información relativa a los tratamientos de datos que se van a realizar, incluyendo la identidad de los diversos responsables del tratamiento, para ello se hace mención en las altas de socios a LLEFISA SA, titular de la instalación de Santander y a METROPOLITAN SPAIN SL titular de la marca METROPOLITAN y de la gestión de centros deportivos”

- “Los corresponsables notificarán al resto de los responsables del tratamiento, las violaciones de seguridad de datos...” sin precisar quienes son esos otros “responsables del tratamiento”

En el 6, se indica: “realizar conjuntamente las evaluaciones de impacto relativas a la protección de datos, cuando proceda”

2. Aporta copia de facturas y pedidos y contratos a nombre de METROPOLITAN SPAIN SL DE 19/01/2017, “DOS SERVIDOR sql”, SERVICIO CONTRATADO “CLOUD”, según METROPOLITAN, “servidores donde está ubicado el software de PROVIS”.

3. Que “la ficha de usuario” en el software PROVIS son una serie de registros relacionados entre sí en una base de datos, siendo el software PROVIS un “ERP de gestión, facturación y control de accesos especializados para centros deportivos”.

-En la base de datos del software PROVIS se almacena un patrón generado a través del algoritmo privado del fabricante NitGen.

En la pulsera RFID que portan los socios solo se almacena un UID (identificador único), no se almacena ningún patrón. Añade que “El lector RFID activa el lector de huella, este no da un acceso directo”.

4. Manifiesta que la opción de configuración, “Permite búsqueda en frío”, que significa búsqueda de huellas de tipo 1: N, no está seleccionada.

Aporta captura de pantalla de sus sistemas donde consta la opción “Permite búsqueda en frío” sin seleccionar.

5. Aporta extracto de base de datos con las 100 últimas bajas de usuarios donde constan los campos “ID Persona” y “Última fecha de baja”. Aportan extracto de base de datos con los 100 últimos borrados de huella con los campos, entre otros, “Fecha” e “ID Persona”. Que, en el extracto de borrado de huellas, el campo “Fecha” toma valores entre “25/05/2021” y “25/04/2022”. Se comprueba en dichos extractos que constan usuarios dados de baja de los cuales no consta borrado de su huella.

6. Se aportan tres extractos de base de datos solicitados con relación al “*número total de personas de las cuales tienen huellas dactilares almacenadas*”, “*número total de personas dadas de alta en el sistema de acceso por huella*”, y “*número total de personas dadas de alta como usuarios del gimnasio*” siendo dichos extractos aportados idénticos y con un número total de personas en cada caso de 1387.

Que los tres extractos anteriores constan obtenidos con los mismos parámetros de búsqueda y consta en cada uno de los tres listados el siguiente texto; “*Generado el jueves, 05 de mayo de 2022 a las 12:38:00*”.

7. Con fecha 13/07/2022, se comprueba que en la url <https://provis.es/wp-content/uploads/2019/05/MANUAL-Completo.pdf> consta el manual del software PROVISPORT para “*gestión y control de accesos en instalaciones deportivas*” donde consta una pantalla del software similar a la aportada por el denunciado y consta asimismo en este manual que “*Si permite búsqueda en frío el lector de huella, permitiendo de esta manera, la posibilidad de poder autenticar clientes utilizando únicamente su huella dactilar sin introducir previamente ningún número PIN*”.

SEXTO: Con fecha 3/08/2022, la Directora de la AEPD acordó:

“*INICIAR PROCEDIMIENTO SANCIONADOR a LLEFISA, S.L., con NIF **B60422417**, por la presunta infracción:*

- *Del artículo 13 del RGPD, tipificada en el artículo 83.5.b) del mismo RGPD, y a efectos de prescripción, calificada como leve en el artículo 74.a) de la LOPDGDD.*
- *Del artículo 7 del RGPD, tipificada en el artículo 83.5.a) del RGPD, y a efectos de prescripción, calificada como muy grave en el artículo 72.1.c) de la LOPDGDD.*

“*a los efectos previstos en el art. 64.2 b) de la LPCAP, las sanciones que pudiera corresponder serían de multas de 2.000 €, y de 15.000 €, según lo especificado, sin perjuicio de lo que resulte de la instrucción.*”

SÉPTIMO: De acuerdo con el certificado de notificación telemática, figura, con el siguiente resultado:

Fecha de puesta a disposición: 05/08/2022 11:54:03

Fecha de rechazo automático: 16/08/2022 00:00:00.

Con el fin de garantizar la recepción del acuerdo, en aplicación del artículo 41.6 del RGPD, y al no existir dirección de correo electrónico del reclamado, ni dispositivo electrónico para ser informado de la puesta a disposición de la notificación en sede electrónica, se remitió vía postal el acuerdo de inicio, siendo recibido por la reclamada.

OCTAVO: Con fecha 31/03/2021, se recibe escrito de LLEFISA. La persona que realiza las alegaciones, además de delegada de protección de datos, es la misma que presentó las respuestas en nombre de METROPOLITAN durante el traslado de la



reclamación, figurando también con esta categoría en dicha entidad, y la que presentó toda la documentación. Indica que METROPOLITAN estuvo vinculada con LLEFISA hasta agosto 2022. Solicita el sobreseimiento del expediente, y se archiven las actuaciones. Manifiesta:

1.No puede considerarse reclamada a LLEFISA porque la reclamante señala como tal a METROPOLITAN SPAIN SL y el traslado de la reclamación se le hizo a dicha entidad, no siendo LLEFISA responsable de las gestiones de METROPOLITAN.

2.La lectura que figura en el contrato que firma la reclamante sobre: *“La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro, y que en caso de no aceptarse nos impide prestar el servicio al socio.”*, mantenemos que en la frase *“nos impide prestar el servicio al socio. LLEFISA, SL, no se refiere a impedir que una persona sea socia como ha querido reflejar la denunciante pretendiendo que esta AEPD considere como un defecto de consentimiento por no ser libre.”*

Sobre la manifestación: *“Que el sistema de biometría se instaló en este Club Aqua Flo- ranes en febrero de 2021 como único modo de acceso unido a la pulsera”*, no se corresponde con la realidad: no era el único modo de acceso. En ningún momento se obtuvieron los datos biométricos de la reclamante, y, sin embargo, durante el tiempo que continuó siendo socia del club, hasta el mes de junio de 2021, hizo uso de las instalaciones entrando por el control de accesos sin usar en ningún momento la biometría, dado que se respetó su negativa a darla y así mismo sucede con otros socios. Esta afirmación, se corrobora con el registro de los accesos de la reclamante a las instalaciones sin acceso biométrico hasta la fecha de su baja y con la copia de su ficha donde consta que no existe ninguna biometría grabada (aporta Documentos núm.1). En el mismo figura listado Excel, nombre y apellidos, por fecha, desde 1/02 a 6/05/2021 (búsqueda hasta 31/07/2021), hora entrada y salida y el cómputo del tiempo consumido como *“permanencia”*. En ese listado, no figura relación alguna de tarjeta ni sistema de acceso. También acompaña la ficha PROVISPORT de la reclamante que contiene sus datos y fotografía, y de la que se extrae o se ve el listado Excel anteriormente señalado y un número de tarjeta.

También se aporta un registro de accesos a la instalación de otros socios, *“fichas PROVISPORT”* sin biometría grabada, así como imágenes de sus fichas (aporta documento núm.2). En el mismo, según indica, se corrobora la no obligatoriedad de tener la biometría registrada para acceder a las instalaciones.

En cuanto a que se indica en el punto 6, que *“actualmente los usuarios no tienen otro sistema de acceso a las instalaciones, “se debe matizar, pues “existen sistemas alternativos para acceder a las instalaciones, como el “control manual de acceso por entrega de DNI para su comprobación en la recepción, mediante el cotejo de la fotografía que consta en la ficha de PROVIS versus el DNI. Sin embargo, se prioriza el sistema de control con pulsera y código hash para agilizar los accesos y dar total autonomía al socio para entrar y salir del establecimiento sin esperar que recepción abra el turno o puerta de acceso.”*

3.El tipo de datos que se tratan para acceder a las instalaciones mediante huella dactilar son biométricos, pero no de carácter especial, contando que existe diferenciación

entre los procesos que implican identificación biométrica y los que implican verificación/autenticación biométrica. En la primera, se comparan los datos adquiridos en el momento de la identificación con una serie de plantillas almacenadas en una base de datos, el proceso de búsqueda es uno a varios. Considera que estos serían los considerados de especial protección, encuadrados en la prohibición general y excepciones del artículo 9 del RGPD.

En el segundo tipo de procesos, se comparan los datos adquiridos en el momento de la verificación con una única plantilla biométrica almacenada en un dispositivo, el proceso de búsqueda es de uno a uno. Estima que el sistema empleado para el control de acceso de los usuarios a las instalaciones del gimnasio en Santander al que acudía la reclamante, *“autentifica que la persona que porta la pulsera y que pone el dedo en el sistema es la misma”*. Considera que estos, que son los que utiliza para su control de acceso, no serían de especial protección y no entrarían en la prohibición que establece el artículo 9.1 del RGPD. Junto a esta consideración, decaería la circunstancia agravante de la infracción del artículo 83.2.g) por no ser datos especialmente protegidos y sus implicaciones.

4. Sobre el carácter incompleto de la imputación del artículo 13 del RGPD, indica:

a) *“La normativa firmada por la reclamante se produjo antes de la implementación del acceso biométrico”, “y por ello la información del nuevo sistema de acceso se informaba mediante la cartelería colocada en la recepción, la publicidad del sistema NITGEN y una persona en los accesos del torno”. Adjunta documento 11 que consiste en una hoja titulada: “METROPOLITAN Sport Club & Spa Tratamiento de datos personales” sin fecha. Inicia con “METROPOLITAN cumple todos los requisitos establecidos en el RGPD...”, destacando que los datos facilitados, se incluyen los biométricos, son tratados por METROPOLITAN con la finalidad de gestionar su solicitud de incorporación como socio del gimnasio y finalidades inherentes, como la gestión y cobro de recibos, el acceso a las instalaciones.*

El plazo de conservación de los datos biométricos consta en el registro de actividades, es hasta que se deja de ser socio del Club o hasta que se ejercía el derecho de limitación o supresión. *“En relación con la posible comunicación de datos a terceros”, la inexistencia de tal comunicación y por un aspecto de minimizar el texto en el redactado de la normativa en aquel momento por la plantilla existente, no se hizo mención de que “los datos biométricos no se comunicarían a terceros”, mención para la responsable obvia a partir del Análisis de Riesgos y la EIPD. Al no producirse ni realizarse elaboración de perfiles, no se había mencionado este, considerando que “si no se hace un determinado tratamiento de datos no era necesario mencionarlo”.*

En la *“normativa de socios”* de AQUA FLORANES *“actual”*, ya se menciona los tres apartados referidos. Aporta documento 12 que, según manifiesta, contiene una normativa de socios actual, que permite constatar que no existe infracción continuada del derecho de información, y que no ha habido beneficio como consecuencia de no haber informado del plazo de conservación de datos. Se visiona el documento 12 que trata de un modelo, no se contiene fecha de implantación, que contiene las Cláusulas del contrato de uso de las instalaciones del Club, *“normativa socio”* en el que se integra ahora el apartado: *“autorización al tratamiento de datos personales por la entidad”*. Se contiene:

*“Le informamos que LLEFISA, SL cumple todos los requisitos establecidos en el RGPD 2016/679 (UE) y que todos los datos bajo nuestra responsabilidad vienen siendo tratados de acuerdo con las exigencias legales, guardándose las debidas medidas de seguridad que garantizan la confidencialidad de estos. Los datos personales que ha facilitado de nombre y apellidos, DNI, dirección postal y/o electrónica, así como el número de su tarjeta de crédito o su cuenta bancaria, serán tratados por LLEFISA SL, con CIF B60422417 en c/ Cisneros nº 67, 39007-Santander con la finalidad de gestionar su solicitud de incorporación como socio del gimnasio y finalidades inherentes como la gestión y cobro de recibos, la entrada en las instalaciones”*

*“Con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones, se opta por un sistema de acceso mediante el registro biométrico (código hash encriptado) y una pulsera personal que complementará el uso biométrico. Dichos datos biométricos no serán objeto de otro tratamiento por parte de LLEFISA, SL ni por el proveedor de servicios informáticos, a excepción de los servicios de mantenimiento. El plazo de conservación de dichos datos personales no excederá del momento en que cause baja el socio por cualquier circunstancia o de su solicitud de supresión. No se adoptarán decisiones automatizadas ni se elaborarán perfiles con dichos datos. La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro y el control de acceso para solamente los socios. Podrán utilizarse medios alternativos de acceso.”*

*Finalmente, se informa entre otros ejercicios de derechos, que puede ejercer la revocación del consentimiento prestado para el tratamiento de estos, dirigiendo su petición a LLEFISA.*

5. Sobre la falta de consentimiento del socio al momento de firmar la normativa, “son condiciones del servicio necesarias para el buen funcionamiento del centro, y que en caso de no aceptarse, nos impide prestar el servicio al socio”, considerando que se trata de la seguridad de las personas y enseres (máquinas, aparatos, instalaciones, etc.), “no al acceso al gimnasio”, para lo cual, no hay nada mejor que acreditar que las personas que entran son realmente socios del centro, quienes por su propio interés, cuidarán de sus pertenencias y de los equipos y máquinas con las que practican deporte. El consentimiento al tratamiento de los datos biométricos o no, en ningún caso condicionaba la condición de socio, aceptación y firma de la normativa, puesto que existía otra posibilidad de acceder. Con tales finalidades, LLEFISA, SL ha introducido el control de acceso biométrico, para asegurarse del buen funcionamiento del centro y de la seguridad de las pertenencias de los socios, siendo que casi la totalidad de socios lo han tomado como una mejora de la calidad y seguridad del centro, y algunos (poquísimos) no les ha parecido bien por las causas que sean y no han querido dar el patrón de huella para que, junto con la pulsera, accedan a las instalaciones, a los que se sumarian que en “algunas personas de edad avanzada”, no ha sido posible obtener su patrón, y han seguido entrando sin hacer uso de la biometría.

A efectos de acreditar que cuenta con el consentimiento para levantar la prohibición del tratamiento de datos biométricos, conforme señala el artículo 9.1.a) del RGPD,

LLEFISA acredita el consentimiento del interesado con la firma de la normativa de socios. “También es un acto afirmativo claro el de proceder técnicamente a la captura del patrón de huella en el dispositivo (pulsera)”. El consentimiento del socio se da en el contexto de la normativa de socios, especificándose los diferentes tratamientos de datos personales de los mismos. A esto, se suma que AQUA FLORANES tiene colocada en 2021 una cartelería informativa en la recepción del centro. Adjunta documento 11, que consiste en una hoja “Tratamiento de datos personales”, con información, no sobre LLEFISA, sino sobre METROPOLITAN como la entidad que trata los datos. Se indica, además del registro biométrico y la pulsera que *“Otra de las formas de identificación para el acceso podrá ser con la imagen del socio visualizada momentáneamente en una pantalla en la recepción. En caso de no aceptarse los sistemas de identificación de acceso, el Club no podrá prestar servicios al socio ni permitir su acceso a las instalaciones.”*

*Indica que de ese cartel también se desprende la otra posibilidad existente para acceder al centro, solicitud de DNI en el acceso y comparativa con la imagen que se muestra en la pantalla del ordenador de recepción. Solo la no aceptación de alguna de las dos posibilidades condicionaba que no pudiera ser socio del gimnasio, pero en ningún momento se condicionaba la posibilidad de ser socio a la aceptación de la huella biométrica, como se ha pretendido por la denunciante. El consentimiento no debe considerarse libremente prestado, cuando el interesado no goza de verdadera o libre elección, o “no puede denegar o retirar su consentimiento sin sufrir perjuicio alguno.”*

En este caso, no se ha producido perjuicio alguno a la denunciante ni al resto de los socios, al existir conjuntamente otra posibilidad de acceso al centro sin huella dactilar, la de la imagen del socio visualizada momentáneamente en una pantalla de recepción, “y prueba de ello son los Excel aportados de todos los accesos entre 1/02 a 31/07/2021, fecha de su baja por la circunstancia que fuera”.

Estima que “el consentimiento se ha dado libremente pues LLEFISA no está en desequilibrio claro con el denunciante o socios en general, puesto que ni AQUA FLORANES es el único centro deportivo al que pueden acudir los ciudadanos de Santander, ni obliga a ser socio exigiendo la huella dactilar del mismo”

A fecha de la denuncia, LLEFISA está solicitando un consentimiento para el tratamiento de datos biométricos que no se consideraban a tenor del criterio de la AEPD como categoría especial de dato, y que el socio presta “válidamente y de forma expresa”, y ofreciendo “medios alternativos para acceder a las instalaciones”, “sin imponer el tratamiento de datos biométricos de forma obligatoria para poder acceder a las instalaciones”.

“Cuando se puso en marcha el control de acceso biométrico junto con la pulsera, una persona del equipo de recepción se encargaba de informar personalmente a los socios en su acceso al club, siendo que el consentimiento más evidente se manifestó con la acción personal y física de cada socio en proceder técnicamente la obtención de la huella”

6.Con referencia al ANÁLISIS DE RIESGOS de fecha 30/01/2020, indica que correspondía al sistema de tratamiento de METROPOLITAN AQUA FLORANES por lo que

algunos de los riesgos en el mismo, puestos de manifiesto no se corresponden con la situación real en relación con el responsable LLEFISA, SA, que tiene objeto de este Procedimiento Sancionador.

Un mes antes de la implementación del sistema de control de accesos con pulsera y código hash, se firma la EIPD para LLEFISA, en 31/12/2020. El documento de EIPD de 5/02/2021 se refería a METROPOLITAN. Adjunta documento 4 en el que se ve, “AQUA FLORANES SANTANDER- sistema de apertura mediante control biométrico”. A destacar:

- “(7) “La EIPD se realiza sobre el tratamiento de los datos de los socios del responsable del tratamiento con la finalidad del controlar el acceso al gimnasio. Los datos tratados son la huella dactilar o aquellos datos identificativos necesarios a incluir en la pulsera de identificación del socio, con la finalidad de que el sistema reconozca al interesado y permita, mediante esta identificación, acceder al gimnasio. Asimismo, se identifica fecha y hora de acceso.”

- “(7.1) 2.- Procedimiento de comparación de los datos captados con los datos almacenados

*El usuario (socio) cuando accede al gimnasio se válida primero con una pulsera RFID. Una vez pasada la pulsera e identificado el usuario, si éste tiene registrado en el sistema la necesidad de comprobar su patrón de huella construye en tiempo real un nuevo patrón que se compara uno a uno con el patrón almacenado a través de los algoritmos internos de NitGen. Este patrón es generado en tiempo real y no se guarda.” “d. Tecnología: identificación o verificación mediante plantilla almacenada durante el proceso de registro (código único para cada huella y el patrón se obtiene con los algoritmos matemáticos de NitGen).”*

*“3.- Criterios para la codificación y el almacenamiento de la información captada. Se almacena en el perfil del usuario un patrón generado a través del algoritmo de encriptación en posesión del fabricante NitGen. No se almacenan datos en bruto. a. Actividad del proceso: almacenamiento de datos en la pulsera del socio.”*

7.No existen riesgos evidentes con la tecnología utilizada, para garantizar de manera suficiente al interesado, que la plantilla obtenida a partir de los datos biométricos (código hash 1:1) no coincidirá con ninguna otra plantilla o huella dactilar utilizada en otros sistemas similares y tal como la propia AEPD indica, “es innegable que la utilización de sistemas basados en la recogida de la huella dactilar para llevar a cabo el control de entrada en el gimnasio evita el riesgo de suplantación que se pudiera producir”.

8.En cuanto a la agravación de las infracciones:

-por aplicación del artículo 83.2 a) del RGPD, considera que el consentimiento ha sido libre y no se puede considerar que afecta a todos los clientes de la entidad, ni siquiera la reclamante se vio afectada, nunca facilitó su huella, y siguió acudiendo al gimnasio tantas veces como quiso con medios alternativos, como figuraba en la captura de pantalla del programa de gestión PROVISPORT, donde se aprecia su entrada y salida de forma reiterada sin dato biométrico registrado.



-por aplicación del artículo 83.2.b), en cuanto a la obtención del consentimiento para un tratamiento lícito, actúa con diligencia al ser escrupulosa en la obtención del libre consentimiento de sus socios y en la información facilitada sobre el nuevo tratamiento de datos biométricos para el control de accesos.

Han mejorado la redacción para que se entienda perfectamente por el socio la “autorización al tratamiento de datos”, para caso “de no considerar conveniente el acceso mediante el control de acceso con biometría”, siga teniendo otra opción para acceder al gimnasio que no obligue al tratamiento de datos biométricos. Adjunta la nueva redacción en la que se indica que en los datos que proporciona: nombre y apellidos, DNI, dirección postal-electrónica, número de tarjeta de crédito o su cuenta bancaria... serán tratados con la finalidad de gestionar su solicitud de incorporación como socio del gimnasio y finalidades inherentes como la gestión y el cobro de recibos, la entrada en las instalaciones. Continúa:

*“Con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones, se opta por un sistema de acceso mediante el registro biométrico (código hash encriptado) y una pulsera personal que complementará el uso biométrico. Dichos datos biométricos no serán objeto de otro tratamiento por parte de LLEFISA, SL ni por el proveedor de servicios informáticos, a excepción de los servicios de mantenimiento. El plazo de conservación de dichos datos personales no excederá del momento en que cause baja el socio por cualquier circunstancia o de su solicitud de supresión. No se adoptarán decisiones automatizadas ni se elaborarán perfiles con dichos datos. La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro y el control de acceso para solamente los socios. Podrán utilizarse medios alternativos de acceso.” Finalmente, se le informa del ejercicio de los derechos, entre los que figura “la oposición al tratamiento y la revocación del consentimiento prestado para el tratamiento de los mismos.”*

#### 9. Aporta:

a) Certificado de la empresa desarrolladora de la aplicación PROVISPORT (Proyectos Visuales Zaragoza SL) de 28/03/2023 indicando que “Se ha verificado que se está utilizando un sistema de validación biométrica de los clientes o búsqueda 1:1.

*Utilizándose un sistema combinado de acreditaciones RFID para localizar al cliente en la base de datos y verificar a través del patrón del cliente, almacenado y generado por el algoritmo del fabricante en el momento del alta, con el patrón capturado en el momento del acceso.*

b) Registro de actividades de tratamiento, “gestión de acceso socios al club”, responsable del tratamiento LLEFISA SL, ejercicio de los derechos de acceso rectificación limitación supresión portabilidad y oposición: calle Cisneros 67, Santander, base jurídica: normativa de socios, contrato, consentimiento al facilitar sus datos biométricos, tipología de datos: nombre, apellidos, fotografía, huella dactilar, código hash, frecuencias de acceso, firma e imagen, finalidad del tratamiento: gestión de los datos personales de los abonados para permitirles el acceso a la instalación.



Periodo de conservación de datos: mientras sea socio. Categorías de destinatarios: No se prevén

NOVENO: Con fecha 13/04/2021, se emite propuesta de resolución del literal:

*“1-Que por la Directora de la Agencia Española de Protección de Datos se sancione a **LLEFISA, S.L.**, con NIF **B60422417** por una infracción del:*

*-artículo 13 del RGPD, de conformidad con el artículo 83.5.b) del RGPD, tipificada a efectos de prescripción en el artículo de la LOPDGDD, con una multa administrativa de 2.000 euros.*

*-artículo 9.1 del RGPD, de conformidad con el artículo 83.5.a) del RGPD, tipificada a efectos de prescripción en el artículo 72.1.e) de la LOPDGDD, con una multa administrativa de 15.000 euros.*

*--artículo 6.1 del RGPD, de conformidad con el artículo 83.5.a) del RGPD, tipificada a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, con una multa administrativa de 10.000 euros.*

*2-Que por la Directora de la Agencia Española de Protección de Datos se ordene a **LLEFISA, S.L** en virtud del artículo 58.2 del RGPD, que acredite una correcta y adecuada implantación del sistema de huella atendiendo a la base legitimadora para el tratamiento de los datos del registro de la huella dactilar, a los que ya disponen de ese dato, y a la información del tratamiento asociada a la misma.*

Figura aceptada la entrega el 14/04/2013.

DÉCIMO: Con fecha 28/04/2023 ahora tienen alegaciones en las que manifiestan:

1) Reitera su alegación de que su tratamiento biométrico es de verificación 1 versus 1 y no de identificación y no serían datos especiales, aunque el tratamiento vaya dirigido a identificar a una persona. “En el mismo sentido que la comprobación del DNI con la ficha del socio también va dirigida a identificar a una persona de forma unívoca” y no sería calificable como de categoría especial.

El instructor no ha entrado a rebatir ninguno de los argumentos técnicos de alegaciones que demuestran que la técnica empleada es segura. Hasta el presente, no hay prueba de que se haya producido ninguna brecha de seguridad. Se confirmaría que el sistema garantiza que no existen riesgos evidentes con la plantilla código hash 1:1, “ya que no coincidiría con ninguna otra plantilla ni huella dactilar utilizada en otros sistemas similares” “En el sistema NitGen, la reversión del algoritmo utilizado es imposible.” “No podemos suscribir que frente a una vulnerabilidad se vean afectados todos los sistemas de acceso con datos biométricos al mismo tiempo; cada sistema tiene su código de encriptación.”

La prohibición del tratamiento de los datos biométricos, si puede ser este el caso, en este supuesto consideran que se da la circunstancia que vence su prohibición dado de que el socio ha dado su consentimiento explícito para el tratamiento de dichos datos personales con uno o más fines especificados. Ello lo relaciona con que la captura de unos datos biométricos como es la huella se ha de dar de forma consciente con la

acción positiva para iniciar el tratamiento como es este caso, a diferencia de otros sistemas en que la persona no es consciente de que se está tomando la información biométrica o de cuando se está tomando.

Para el sistema y control de accesos al Club, da igual como se llame el usuario, lo único que le interesa y necesita es que el usuario sea un individuo registrado en el sistema y que esté autorizado a acceder a las instalaciones como socio, con dos finalidades, una que sea un socio activo y por tanto al corriente de sus cuotas de pago y otra, que no sea un sujeto usurpador no autorizado que pueda comprometer la seguridad de las instalaciones y de las personas. El sistema no trata de identificar inequívocamente al usuario, sino de verificar que sus datos se corresponden con el código hash y autenticarlo como un usuario autorizado para el acceso al club.

Es en el proceso de verificación y autenticación que se establece la correspondencia con el parámetro registrado y por tanto se valida al socio, en el procedimiento 1:1, distinto del de identificación, 1: varios, de identificación real del usuario que la reclamada no realiza en ningún momento.

2) En cuanto a la reclamación ante Consumo manifiesta que la reclamante solamente pidió la hoja y que no la llegó a presentar.

3) Se dan *“en distintos puntos de su escrito”* como *“hecho probado”* que *“Actualmente los usuarios no tienen otro sistema de acceso a las instalaciones del gimnasio”*, siendo una manifestación de la reclamante que no es cierta y debe rechazarse habiendo acreditado que había cartelera informativa en la recepción del centro, documento 11 de alegaciones, y que se aportó un listado de usuarios desde 1/02 a 6/05/2021 que accedían sin datos biométricos.

Manifiesta que *“En ningún momento se condicionaba la posibilidad de ser socio a la aceptación de la huella biométrica, como se ha pretendido por la denunciante”*. El hecho de que los socios no den sus datos biométricos de forma voluntaria no tiene ninguna consecuencia negativa o perjuicio para el socio.

Reitera que existían sistemas alternativos de acceso, como la exhibición del DNI en -comparativa de imagen mostrada en la pantalla del ordenador de recepción, que se desprende del cartel. Solo la no aceptación de alguna de las dos posibilidades condicionaba que no pudiera ser socio del gimnasio, pero en ningún momento se condicionaba la posibilidad de ser socio a la aceptación de la huella biométrica, como se ha pretendido por la denunciante.

4) La normativa de socios actual es la de 2023 de la que se aportó el modelo en alegaciones que se extrae del sistema informático (para que no se contengan datos de personas), si bien habían aportado 3 páginas, ahora aportan la que faltaba, (documento núm. 2) *“la de la autorización al tratamiento de datos biométricos”*. El documento porta pie de firma para el usuario y no indica desde cuando entra en vigor. Además, figura: *“condición de socio:*

*“Los datos personales que ha facilitado de nombre y apellidos, DNI, dirección postal y/o electrónica, así como el número de su tarjeta de crédito o su cuenta bancaria, serán tratados por LLEFISA SL. con la finalidad de gestionar su solicitud de incorporación*

como socio del gimnasio y finalidades inherentes como la gestión y cobro de recibos, la entrada en las instalaciones, la participación en eventos y master class, etc. Los datos no se cederán a terceros, no se adoptarán decisiones automatizadas ni se elaborarán perfiles con dichos datos. No se realizan transferencias internacionales de datos.

El plazo de conservación de los datos personales será de 5 años a contar del momento en que cause baja el socio por cualquier circunstancia o de su solicitud de supresión, en cuyo caso se mantendrán bloqueados hasta el cumplimiento de los plazos exigidos por la normativa fiscal.

#### Registro de accesos

“Tal y como se especifica en la normativa de socios, con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones y equipos, LLEFISA, SL ha optado por una gestión de accesos mediante un sistema con la biometría del socio (registro biométrico con código hash encriptado) y una pulsera personal que complementa el uso biométrico. La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro y el control de acceso para los socios. La finalidad de este registro de accesos con biometría es facilitar la verificación y acreditación de la condición de socio para evitar el acceso de personas no autorizadas. El plazo de conservación de los datos personales no excederá del momento en que cause baja el socio por cualquier circunstancia o de su solicitud de supresión.

No se adoptarán decisiones automatizadas ni se elaborarán perfiles con dichos datos.

No se realizan transferencias internacionales de datos. Las características del sistema NetGin las encontrará en la Recepción del centro. Se entenderá que autoriza el tratamiento de datos biométricos si se presta a la obtención de su huella digital con el mecanismo de NetGin en la recepción. En otro caso, podrá utilizar como medio alternativo de acceso la presentación de su DNI o el pasaporte al personal de recepción del club en cada uno de sus accesos, quienes validarán su condición de socio activo en el programa de gestión del centro y procederán a una apertura manual del torno, sin que ello comprometa su condición de socio. De acuerdo con la normativa vigente en protección de datos, podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, así como revocar el consentimiento prestado para el tratamiento de los mismos, indicando del derecho de que se trata, dirigiendo su petición a LLEFISA, SL, c/ Cisneros nº 67, 39007-Santander o al mail dpo@wemet.es adjuntando documento acreditativo de su identidad. Puede presentar reclamación ante a la AEPD. FIRMA EL SOCIO CONFORME”

Manifiesta que adjuntan una autorización de muestra de consentimientos firmado en los que figuran datos personales de socios (documento 3 a 10) con la cautela de que no se harán públicos en ningún momento, tratándose de la firma del citado documento “autorización al tratamiento de datos personales”, en los que figura mecanizado el nombre y DNI y fechas de alta que van a título de ejemplo de fechas: que van entre los rangos de 19/02/2021, a 25/04/2023, (siendo la número documento 10 un posible error, alta: 3/09/2013), sin saber si la fecha de alta coincide con la de esta autorización al no constar en el pie de firma fecha alguna.

5) Añade que en relación al punto 2 de la Propuesta de Resolución, la reclamada, LLEFISA, SL ya acredita una correcta y adecuada implantación del sistema de huella atendiendo a la base legitimadora del consentimiento para el tratamiento de los datos del registro de la huella dactilar mediante una Tablet que genera el documento aportado como Documento núm. 2 (Autorización tratamiento de datos biométricos) de los que ya eran socios antes de la obtención de dicho dato y de los que se incorporan al Club como socios (siempre que lo faciliten), en el que se detalla la información del tratamiento asociada a dicha huella dactilar.

-En relación con el punto 1 de la Propuesta de Resolución, la reclamada, LLEFISA, SL ya facilita la información requerida en el art. 13 del RGPD, aun con la salvedad de que se refiere a revocación del consentimiento y no retirada del mismo, entendiéndolo como acciones sinónimas a los efectos de su ejercicio, o que en todo caso se minore el importe de la sanción de 2.000 euros, atendiendo la mínima infracción por no mencionar “*retirada*” en vez de revocación del consentimiento, o en no duplicar los términos.

6) Aporta un repaso cronológico:

Octubre 2019: Informe sobre viabilidad del uso de datos biométricos. Previo a la diferenciación por la AEPD de la identificación-autenticación 1:1 versus 1: N.

2/09/2020: alta de **A.A.A.** como socia AQUA FLORANES cuando el control de accesos no era biométrico.

2/09/2020. Firma de normativa de socios. Por ello la firma de la Normativa no contiene mención a dicho tratamiento de datos, no siendo un incumplimiento porque en dicho momento no existía el registro de accesos con biometría.

2/09/2020. Firma de la autorización al tratamiento de datos para la gestión como socio (acceso al club, recibos bancarios, master class, etc.) más información sobre (1) AQUA FLORANES optará por el control de accesos biométrico y (2) uso de las plataformas accesorias (Technogym, Trainigym, etc.) para lo que no se solicita ningún tipo de autorización por que la biometría no existe y el uso de las plataformas es una decisión personal de cada socio.

30/12/2020: EIPD sobre el tratamiento de control de acceso con datos biométricos.

30/01/2021: Análisis de riesgos antes de la instalación del sistema de control con biometría.

1/02/ 2021: instalación del sistema de control de accesos biométricos en AQUA FLORANES, no en fecha 6/05/2021 como dice la reclamante.

1/02/2021: cartelería informativa del nuevo sistema de accesos y persona en el Torno (control de accesos) informando del sistema.

6/05/2021: solicitud de hoja de reclamación por **A.A.A.**

1/06/2021: baja de la socia, sin manifestación de motivo.

Del relato concluye que el contrato de septiembre de 2020, no se podía hacer referencia a los datos biométricos porque no existían, el control era por DNI+ficha de socio en el ordenador. Con ello rebate también la falta de información sobre el periodo de conservación de los datos biométricos en el contrato, la información sobre destinatarios o existencia de decisiones automatizadas:

La falta de referencia en la evaluación de impacto a otras modalidades de acceso nada más que a la biometría era porque se centraba en ese exclusivo tratamiento biométrico por lo que no se volvieron a analizar los sistemas existentes hasta el momento.

El nuevo contrato de “*normativa de socios*” en el que se ampliaba el derecho de información, del que aportó el modelo según sale del programa informático, por ello no llevaba fecha, ya se había puesto a disposición de los socios en enero 2023 y el modelo de “*autorización específica*” se había distribuido también para todos los socios (aquellos anteriores a la puesta en marcha de los nuevos dispositivos de registro de accesos de febrero de 2021). Adjunta como Documentos nim 3 a 10, autorizaciones al tratamiento de datos biométricos correspondientes a una muestra de socios del periodo febrero 2021 a septiembre 2022 (bajo la marca METROPOLITAN), documentos del periodo diciembre 2022 a abril 23, así como de socios previos a febrero 2021.

La reclamante es informada cuando se da de alta como socia del uso de un “*sistema biométrico*”, o “*registro biométrico*” a pesar de no estar en uso todavía para el acceso a las instalaciones, pero no se le recogió dato alguno de dicho tipo en aquel momento porque el sistema no estaba en funcionamiento; diferenciando los párrafos sobre lo que era tratamiento de los datos facilitados con la finalidad de gestionar su incorporación al club, cobro de recibos y acceso a las instalaciones en aquel momento, de los párrafos siguientes informativos: “*optar por un sistema de control de accesos mediante huella y pulsera*”; y el uso de las plataformas accesorias. Tal diferenciación con total transparencia puesto que *no hay mención alguna a ningún tipo de tratamiento de datos biométricos en aquel momento puesto que no existen en aquel momento en el Club*.

Acreditándose que en aquel momento no se trataban datos biométricos por LLEFISA, SL, no puede deducirse ni concluirse que el contrato firmado por la reclamante carezca de información sobre:

- a) la base jurídica del tratamiento de datos biométricos (no existían);
- b) finalidad del uso del sistema biométrico (no existía). En el momento de hacerse socia solamente se proporcionaban datos de nombre y apellidos, DNI, dirección postal y/o electrónica, número tarjeta de crédito.
- c) la posible comunicación de datos a terceros, no se producía.
- d) el plazo de conservación de los datos. Es cierto que no se indicaba, pero no existían datos biométricos.
- e) si se van a adoptar decisiones automatizadas a las que se refiere el artículo 22, apartados 1 y 4 del RGPD, incluida la elaboración de perfiles, y, si fuera así, sobre la lógica aplicada y sobre la importancia y consecuencias previstas de dicho tratamiento para el interesado. No se adoptan decisiones automatizadas ni existen los datos objeto de controversia.

En relación con el hecho de que en el contrato y en la autorización no se indica nada de acceso o uso alternativo al registro biométrico, ni si la comunicación de datos



personales es un requisito legal o contractual, o un requisito necesario para suscribir el contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos, es irrelevante porque en aquel momento no se trataban ni recogían datos biométricos, por lo que no puede deducirse un incumplimiento de la legislación a dicha fecha.

Indica que *“las autorizaciones al tratamiento de datos biométricos se empezaron a obtener con la puesta en práctica del registro de acceso con biometría-a partir de febrero de 2021-, según se puede deducir del documento 2, y que a su vez “modificaron las cláusulas de información en la normativa, que consta de tres páginas y es la última la que lleva la “autorización al tratamiento de datos por la tipología de datos biométricos”* Así, *“la información de la recogida de datos en el momento en que se recogen y se van a tratar se consiguió mediante el cartel enmarcado en recepción y una persona que respondía a las preguntas y dudas sobre lo que implicaba la recogida de la huella, cómo se utilizaría, la ficha técnica del sistema NitGen; la captación (acción física positiva del socio) de la huella y la autorización expresa de los socios a medida que iban accediendo al club (solamente de los socios que autorizaron el tratamiento de la huella digital, por lo que es obvio que AQUA FLORANES no dispuso en ningún momento de la autorización firmada por la reclamante).*

*“Aunque se informara previamente a los socios (autorización) de un sistema que se instauraría en un futuro, ello no puede considerarse incumplimiento ni inseguridad porque se cubrió la posible confusión del interesado que interpreta esta AEPD con la efectiva información y consentimiento (por acción física de dar la huella) en el momento de puesta en marcha del sistema en febrero de 2021 y autorización firmada.”*

*“Estamos de acuerdo con esta AEPD en que en el tratamiento ulterior que se materializa cuando se pretendieron recoger los datos de la reclamante, es cuando se debe completar la información sobre dicho tratamiento, adecuándose a las operaciones de tratamiento que se dan con la implantación del control de acceso con biometría y la toma y uso de huellas dactilares para acceso a las instalaciones del club. De hecho, la reclamante nunca manifiesta que no se la hubiera informado del tratamiento, estaba perfectamente informada, ni de que se vulneraran derechos, ni ejerció ningún tipo de derecho ante el Club o METROPOLITAN SPAIN, SL o LLEFISA, SL”*

Considera que sí que informó a través de un cartel informativo en la recepción y una persona que *“paulatinamente fue obteniendo el consentimiento con la firma de la autorización “.*

*“No entendemos que sea información fundamental informar de aspectos que no se producen ni condicionan los hechos. Debemos contradecir las manifestaciones de esta AEPD en el sentido de que, aunque la reclamante no diera la huella, LLEFISA, SL se considere eximida de la obligación de dar dicha información, puesto que DICHA INFORMACION SE FACILITÓ MEDIANTE EL CARTEL Y LA FICHA TECNICA DEL SISTEMA.”*

*“LLEFISA, SL no puede aportar la autorización de esta socia al tratamiento de sus datos biométricos porque no existió dicha autorización a la vez que nunca se trataron datos biométricos de la socia en cuestión.”*

7) No se halla conforme con la estimación de la AEPD de que no figura referencia al consentimiento como base legitimadora del tratamiento del registro biométrico para el



acceso al gimnasio de la reclamada, ya que en la fecha de su incorporación “no se trataban dichos datos biométricos” El párrafo referente a “METROPOLITAN opta por el sistema ...” es meramente informativo por el mismo argumento (no era necesario pedir autorización porque no se obtenían datos biométricos en septiembre de 2020).

Para el resto de los socios que autorizaron la captación y tratamiento de la huella tenemos la acción positiva de dar la huella para que se recoja en el sistema y la autorización firmada en la Tablet como prueba evidente de consentimiento de los socios para el tratamiento de dichos datos. Ello comporta que el consentimiento es la base jurídica del tratamiento de datos biométricos por lo que el resto de las bases jurídicas contempladas en el 6.1 del RGPD y que implican la “necesidad” del tratamiento, no se aplica a este supuesto.

En relación con la afirmación de la propuesta que señala que “*aunque existiera (el consentimiento), como habría de prever la opción de no otorgarlo sin consecuencia alguna negativa, no se estima el mismo una base jurídica del tratamiento adecuada para el tratamiento de datos en esa modalidad con la prestación de este servicio, a menos que se diera una alternativa distinta real y efectiva al uso de la huella.*” Se ha demostrado que los socios tenían otras modalidades de acceso al club (DNI contrastado con la ficha de socio), que la socia en cuestión accedió desde la implantación de la huella en febrero de 2021 hasta que se dio de baja en junio de 2021 sin facilitar la huella, pero en vez de considerar que LLEFISA, SL facilitaba medios alternativos y por tanto el consentimiento era libre y no tenía represalias para con los socios, manifiestan que ahora se ha convertido en INNECESARIO.

*“Reiteremos que, para la prestación del servicio, entendiendo como servicio, no el acceso al club, sino el servicio deportivo de máquinas, entrenadores, equipos, etc. es necesario un buen control de accesos a las instalaciones. Es por ello por lo que hemos de ser especialmente atentos y no hacer confluir bajo un mismo concepto “servicio” la actividad del club (prestación de servicios de carácter deportivo) con el acceso al mismo que no es ningún tipo de servicio sino un medio para disfrutar del servicio (del buen servicio) con seguridad, discreción y corrección.*”

El control de accesos, lo más riguroso posible, es lo que hace que el club preste un buen servicio para con sus socios. Es por ello por lo que, en ningún momento se pretende acreditar que para la prestación del servicio(s) deportivos “fuera o sea necesario el uso de la huella dactilar” porque en ningún momento es la cuestión objeto de la reclamación y la apertura del procedimiento sancionador.

*Hemos de reiterar que no se ha visto vulnerada en ningún momento la opción voluntaria de facilitar la huella o rechazar el procedimiento de captación, y que ningún socio ha sufrido repercusión negativa alguna. “*

*“Nadie puede acreditar que hubiera ningún tipo de represalia por no dar la huella dactilar. Ni tan solo la denunciante puede acreditar una represalia del tipo de echarla del club porque no había dado su huella. Se quedó hasta que quiso, es decir, hasta que llegó el verano y se dio de baja en el club porque ya no le interesaba (por suponer). A todos los socios se facilitó (con el cartel y la información técnica del sistema) tanto la información de su uso, como una alternativa libre de no uso para los que no deseaban otorgar dicho consentimiento explícito (autorización firmada en la Tablet) y por tanto no facilitar el procedimiento de recogida de datos biométricos.”*

No puede afirmar esta AEPD que en el caso de LLEFISA, SL *“la instauración del consentimiento como base jurídica del tratamiento en el uso de la huella dactilar incida en la prestación del servicio que se contrata, condicionándolo a la aceptación de esas modalidades de tratamiento, por la posición jurídica del responsable”*. Es una afirmación falsa. Se permite el acceso bajo otras modalidades y se ha demostrado que no se condiciona la obtención de datos biométricos a la prestación de servicios deportivos y condición de socio.

8) Sobre los motivos explicitados de porque procede un procedimiento de imposición de multas administrativas, señalando la AEPD *“por la importancia que tiene que, ante la prestación de un servicio oneroso, se cumpla completamente con los requisitos del tratamiento de datos, ...”* considera que ese aspecto no es relevante para diferenciarlo de lo que serían entidades públicas o en función del tipo de servicios como aspecto a tener en cuenta para exigir mayor cumplimiento de la normativa en cuestión.

9) Se acredita a efectos de ausencia de culpabilidad que la reclamada realizó un análisis de riesgos como recoge el artículo 32.2 del RGPD. *“Que, del citado análisis de riesgos, donde se evaluó la posibilidad o probabilidad que distintas amenazas se pudiesen materializar, surgió un plan de tratamiento del riesgo a través del cual, mediante la implantación de determinadas medidas (código hash irreversible) minorar el riesgo inherente del tratamiento, dando por tanto cumplimiento a las exigencias del art. 32.2 del RGPD.”*

Además de que *“la sanción es desproporcionada por considerar que en la infracción del artículo 9.2.b) en relación con el 6.1 del RGPD, no se pueden producir las agravantes del 83.2.a) del RGPD, pues la infracción es ya de carácter muy grave, no puede utilizarse esa misma gravedad intrínseca en la propia infracción para añadir a la misma un agravante”, “dado que comportaría que se estuviera sancionando dos veces por la misma conducta”*.

Sobre la aplicación del artículo 83.2. b) del RGPD por el mismo motivo, la intencionalidad o negligencia en la infracción ya va incorporada en el tipo que se sanciona, suponiendo una ficticia suma de agravamientos que no procede.

Además en relación con el artículo 83.2.a) manifiesta que de los 1000 socios, solamente ha reclamado uno, no estando de acuerdo en que los afectados son todos porque son personas que no se han visto afectadas en ningún momento ni lo han manifestado sino que cuando fueron informadas del nuevo sistema de registro aceptaron dando su huella y firmaron la autorización o no la firmaron, sin afectación y sin consecuencias negativas por parte del Club existiendo socios que siguen accediendo con otros medios alternativos a los biométricos.

Considera no serían de aplicación las circunstancias agravantes del art. 83.2.g) en los comportamientos sancionados, por no incurrir LLEFISA, SL en dicho comportamiento en relación con el art. 9.1 del RGPD. Si el tratamiento de un dato de especial protección necesita del consentimiento del interesado, libre, la acción positiva (poner el dedo en un dispositivo la primera vez para captar la huella) y la autorización con la firma en una Tablet, implican y demuestran que no hay circunstancias que agraven la conducta ya que se ha obtenido el consentimiento para la obtención y tratamiento de datos de especial protección.

Un patrón no reversible no puede ser utilizado fuera del sistema NitGen ni con otro dedo que no sea del interesado por lo que no hay ningún tipo de daño ni presente ni futuro, ni para la reputación, ni para la confidencialidad, ni que pueda suponer perjuicios sociales o económicos.

Tampoco se muestra de acuerdo con la consideración de la circunstancia agravante del 83.2.k) del RGPD en relación con el art. 76.2.b) LOPDGDD, es decir la vinculación entre la actividad empresarial de la reclamada (actividad deportiva) y el tratamiento de datos personales implicando la exigibilidad de un cumplimiento diligente de los principios que presiden el tratamiento de datos de carácter personal y en la calidad y efectividad de las medidas técnicas y organizativas que debe tener implementadas para garantizar el respeto de este derecho fundamental tanto de sus clientes como de terceros. Estiman que su actividad es de puesta a disposición de los clientes de máquinas, equipos, entrenadores, para lo cual no necesita tratar, ni trata de forma habitual datos de carácter personal.

*" Tener datos de socios en los sistemas informáticos para acreditarlos como socios y girarles sus recibos-cuotas no debe confundirse con la actividad propia de la compañía. La actividad, según el objeto social de la compañía es la PRESTACION DE SERVICIOS DE GESTION Y ASESORAMIENTO TECNICO. INCLUYENDO CONSERVACION, MANTENIMIENTO, EQUIPAMIENTO, PUBLICIDAD, DIRECCION TECNICA, COMERCIAL Y ADMINISTRATIVA DE EXPLOTACIONES DEPORTIVAS, ETC. "No estamos hablando de una compañía de seguros, de un centro sanitario, de una empresa informática o de videovigilancia, ni de una empresa de prevención de riesgos laborales, no estamos hablando de ninguna de las actividades del elenco del art 37 del RGPD ni del art 34 de la LOPDGDD cuya tipología de datos y categoría de interesados se supone más sensible"*

-Como elementos que considera deberán ser atenuantes:

- o Tiene designado un DPD desde el momento en que dejó de pertenecer a la marca METROPOLITAN, a finales del año 2022 y desde 2020 estaba bajo el paraguas de la figura del DPO de METROPOLITAN SPAIN, SL. El artículo 76.2 g de la LOPDGDD debe tenerse en consideración como elemento atenuante de graduación de la sanción, cuando no fuera obligatorio disponer del mismo

- o El gimnasio estuvo cerrado desde el 14/03 al 20/06/2020 decisión gubernamental, presentó un ERE por las citadas circunstancias, congeló las cuotas de los socios durante dicho periodo, tuvo que invertir en medidas de seguridad sanitarias a efectos de la post pandemia, limitar el aforo de socios en las instalaciones por motivos sanitarios y con ello, sufrir consecuencias económicas de las que todavía no se ha recuperado, cuyos datos aportan en un Excel (ingresos y gastos periodo 2020-2022) como Documento 13, que ha sufrido una escisión de la marca METROPOLITAN en octubre de 2022. *"La autoridad de control puede considerar reducir la multa sobre la base del principio de incapacidad de pago en estos momentos, así como por el peligro de que la imposición de la multa pondrá en peligro la viabilidad económica y continuidad."* El documento 13 es una hoja excel, fecha abr 2023, constando datos de los ejercicios 20 a 22, viéndose la evolución de las cantidades de ingresos por cuotas socios de cada uno, de los sueldos y salarios, de seg social empresa y gastos de explotación, con un sumatorio de

rendimientos que es en los tres ejercicios en negativo, más importante en 2020, casi el triple que en 2022 (-134 mil frente a -51 mil) y unos ingresos en 2022 de 782.724 euros frente a 479.943 en 2020, con evolución en 2021 de 643.608.

- o Falta de período de pruebas.

### HECHOS PROBADOS

- 1) La reclamación de la reclamante se dirige contra METROPOLITAN SPAIN, S.L.

La reclamante manifiesta que desde septiembre de 2020 era socia del gimnasio de c/ Cisneros 67 bajo, en Santander, y que, desde el día 6/05/2021, se impuso como requisito a los usuarios el acceso a sus instalaciones mediante huella dactilar. Añade que anteriormente, accedía mediante una pulsera y una tarjeta identificativa que pasaba “*en el ordenador de recepción*”. Declara que se ha negado a dar sus datos de la huella dactilar.

2) METROPOLITAN, manifestó en actuaciones previas que la empresa titular del gimnasio CLUB AQUA FLORANES, en la dirección señalada por la reclamante, es LLEFISA SL, figurando la reclamante de alta desde 2/09/2020 hasta el 1/06/2021 (se aporta ficha con fotografía de la reclamante con página de control de asistencia de accesos de 14/04 a 6/05/2021, último día de asistencia, sin biometría). Figura anotada: 11/03/2021 “*Se niega a dar la biometría...*”. METROPOLITAN y LLEFISA mantienen relaciones por la gestión y explotación de gimnasios, contando según se deduce por ejemplo del análisis de riesgos de 30/01/2020, cada uno con la titularidad de varios centros. El centro al que pertenecía la reclamada es denominado en la evaluación de impacto de 5/02/2021 como METROPOLITAN AQUA FLORANES -Santander, titularidad de LLEFISA SL, figurando esta como responsable del citado centro en la citada EIPD firmada por la misma persona que efectúa alegaciones en nombre de LLEFISA, y DPD de esta, EIPD, que fue aportada por METROPOLITAN. En alegaciones al acuerdo, LLEFISA aporta otra evaluación de impacto de fecha 31/12/2020, figurando en ambas los gimnasios titularidad de LLEFISA y con el mismo objeto, realizados por la misma empresa, y firmados por la misma persona.

METROPOLITAN además aportó:

a) COPIA DE CONTRATO entre LLEFISA S.L. (“*normativa METROPOLITAN AQUA*”) y la reclamante, de 2/09/2020, conteniéndose datos de la reclamante y donde consta la información de que para acceder al gimnasio los socios disponen de una pulsera personal-intransferible y que para poder acceder a instalaciones es necesario el uso de un sistema biométrico junto con la pulsera de acceso. También se informa de la posibilidad de ejercer los derechos, entre los que se menciona la “*revocación del consentimiento prestado para el tratamiento de los mismos*”, dirigiendo su petición a LLEFISA, SL. En el contrato figura que la reclamante autoriza a LLEFISA a realizar el cargo del pago de la cuota y que prestará los servicios de uso de instalaciones y maquinaria deportiva con acceso al centro.

b) Documento de la misma fecha, denominado “*AUTORIZACION AL TRATAMIENTO DE DATOS*”, en el que se informa que los datos “*personales que ha facilitado de nom-*

*bre y apellidos, DNI, dirección postal y/o electrónica, así como el número de su tarjeta de crédito, serán tratados por LLEFISA SL, SL... con la finalidad de gestionar su solicitud de incorporación como socio del gimnasio y finalidades inherentes como la gestión y cobro de recibos, la entrada en las instalaciones, la participación en eventos y master class, etc. Con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones, METROPOLITAN opta por un sistema de acceso mediante el registro biométrico (código hash encriptado) y una pulsera personal que complementará el uso biométrico. Dichos datos biométricos no serán objeto de tratamiento en ningún caso por parte de Metropolitan. La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro, y que en caso de no aceptarse nos impide prestar el servicio al socio".*

En ninguna parte del contrato o de la llamada autorización, se alude al consentimiento para el tratamiento de los datos del registro biométrico (concretado en la huella dactilar), a su obtención y a la posibilidad de retirarlo en cualquier momento relacionado con el mismo, ni se insta su obtención para la utilización de la huella, imponiéndose como forma de adquirir la condición de socio, uso de los servicios y acceso con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones. La autorización es la opción que selecciona la reclamante según el contrato y la "autorización". No se indica otro modo de acceso a la instalación. Por otro lado, la huella dactilar no estaba instaurada en dicho gimnasio al momento de dicho contrato, y según la reclamante se instauró el 6/05/2021, según la reclamada a partir de 1/02/2021.

Ni en el contrato ni en la autorización, se informa de las bases jurídicas legitimadoras del tratamiento, tampoco sobre la específica del registro biométrico para acceso al gimnasio.

La reclamante no llegó a proporcionar la huella para el acceso al gimnasio, y consta que acudió hasta el 6/05/2021, siendo baja en LLEFISA el 1/06/2021, manifestando que se ha negado a proporcionar la huella y aportando impreso de reclamación ante Consumo rellenado con fecha 6/05/2021, sin que conste acreditada presentación de ese mismo ejemplar ante la D.G. de Comercio y Consumo según figura en el mismo impreso.

1) En el registro de actividad del tratamiento (RAT) de LLEFISA "actividad gestión acceso socios al club", del que LLEFISA SL es responsable, se indica que la base jurídica es "normativa de socios, contrato, consentimiento al facilitar sus datos biométricos", mientras que en el contrato y la autorización de 2/09/2020, se constata que no se alude a la base jurídica del tratamiento de la huella dactilar. En el RAT, figura que la finalidad del tratamiento es la gestión de los datos personales de los abonados para permitir el acceso a la instalación, figurando entre los datos tratados, la huella dactilar. Este fin que consta en el RAT "para permitir el acceso a la instalación" se contradice con la finalidad que figura en el contrato y en la autorización de tratamiento de datos en la que consta: "proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones, siendo un requisito o condición de servicio necesaria para el buen funcionamiento del centro", mientras que la EIPD que aportó LLEFISA efectuada el 31/12/2020 por la misma persona DPD de METROPOLITAN, y la que firmó la nota sobre "viabilidad" del tratamiento de la huella, en octubre de 2019, se indica que



obedece a la necesidad de controlar el acceso a las instalaciones. Destaca en el punto 7.2 de la EIPD en cuanto a la necesidad y proporcionalidad de la instauración del tratamiento, la necesidad de controlar el adecuado acceso a las instalaciones y para la seguridad de sus equipos y otros, evitando que accedan personas ajenas al mismo, se evita llevar tarjetas que pueden ser intercambiadas con otros usuarios, sin proporcionar datos o índices sobre la incidencia y habitualidad de este tipo de accesos, o afectación a la seguridad de las personas, o pertenencias. Sobre la proporcionalidad detalla que “los datos son recogidos para el acceso y uso del gimnasio y los socios no podrán ser identificados para otros fines distintos al control de acceso en las instalaciones y los datos se eliminarán cuando cause baja como socio del gimnasio; en el contrato (normativa de socios) se informará del procedimiento de huella digital y si el cliente está conforme firmará la normativa y accederá al Club, y si no está conforme, no podrá acceder.”

También figura:

- “*periodo de conservación de los datos*” consta que, durante la vigencia de la condición de socio, y cuando se cause baja por cualquier motivo, el socio entregará la pulsera de acceso y se eliminarán. Sin embargo, en el contrato o en la autorización no se indica nada de la conservación de datos de la huella, ni de los destinatarios o las categorías de destinatarios de los datos personales, en su caso de la existencia de decisiones automatizadas.

4) En otra EIPD que aporta LLEFISA sobre “*el sistema de apertura mediante el control biométrico*” de 31/12/2020, se indica entre otras circunstancias, que se efectúa en base a que se cumplen los criterios de que los tratamientos pueden implicar toma de decisiones automatizadas, e implican uso de datos biométricos con propósito de identificar de manera única a una persona física y que el proceso de uso se iniciará. para el primer trimestre 2021. El apartado 7 señala que “*Los datos tratados son la huella dactilar o aquellos datos identificativos necesarios a incluir en la pulsera de identificación del socio, con la finalidad de que el sistema reconozca al interesado y permita, mediante esta identificación, acceder al gimnasio. Asimismo, se identifica fecha y hora del acceso.*”

Tras indicar que se capta y registra la huella y se guarda en la base de datos de la aplicación (PROVIS) a través de una transformación en patrón con un algoritmo, se almacena en el perfil del usuario un patrón generado a través del algoritmo de encriptación en posesión del fabricante NitGen. No se almacenan datos en bruto.

El usuario cuando accede al gimnasio se valida primero con una pulsera RFID, una vez pasada la pulsera e identificado el usuario, si éste tiene registrado en el sistema la necesidad de comprobar su patrón de huella construye en tiempo real un nuevo patrón que se compara uno a uno con el patrón almacenado a través de los algoritmos internos de NitGen. Este patrón es generado en tiempo real y no se guarda.

Indica la EIPD que la base jurídica para el tratamiento derivada del artículo 6.1.b), por tener el usuario la condición de parte del contrato como socio con LLEFISA y sobre la especificidad de la prohibición del tratamiento de datos biométricos no señala aspecto alguno, a pesar de que, en el informe, la misma DPD sobre “viabilidad” acentuaba la prohibición de este tipo de datos.



5) En actuaciones previas, METROPOLITAN manifestó que todos los usuarios dados de alta en el gimnasio tienen sus huellas dactilares almacenadas, en total 1356 usuarios, sin especificar a que centro/s corresponden. LLEFISA en sus alegaciones indica que el registro alcanza a unos mil usuarios

6) El proceso de uso y registro de la huella dactilar para el acceso al gimnasio, parte de la obtención de la huella del usuario de un patrón. El patrón se genera con un algoritmo de encriptación (conocido solo por el fabricante, NITGEN). En la ficha del usuario-socio-en el software "PROVISPORT", se almacena el patrón generado a través de algoritmo de encriptación del fabricante NitGen. En PROVISPORT, LLEFISA almacena los datos de socios y usuarios del club. LLEFISA dispone de contrato de encargo de tratamiento para el sistema de huella dactilar de acceso al gimnasio contratado el 30/12/2018 con PROYECTOS VISUALES DE ZARAGOZA, también titular de la aplicación PROVISPORT utilizada para el almacenamiento y gestión del patrón de la huella.

En este caso concreto, al alternarse el uso de una pulsera RFID, primero el usuario se valida con dicha pulsera que porta un identificador único.

*"una vez pasada la pulsera e identificado el usuario, "si este tiene registrado en el sistema la necesidad de comprobar su patrón de huella" construye en tiempo real un nuevo patrón que se compara uno a uno con el patrón almacenado a través de los algoritmos internos de NitGEN. Este patrón es generado en tiempo real y no se guarda. "d. Tecnología: identificación o verificación mediante plantilla almacenada durante el proceso de registro (código único para cada huella y el patrón se obtiene con los algoritmos matemáticos de NitGen).*

El patrón de huella se conserva mientras el usuario es socio del Club y utiliza la pulsera de acceso hasta que la persona usuaria ha dejado de ser socio. A través del citado software se ejecuta el borrado y supresión.

*"3.- Criterios para la codificación y el almacenamiento de la información captada  
Se almacena en el perfil del usuario un patrón generado a través del algoritmo de encriptación en posesión del fabricante NitGen. No se almacenan datos en bruto."*

En el apartado de evaluación de necesidad y proporcionalidad del tratamiento, se indica que se parte del cumplimiento de unas condiciones de licitud de tratamiento basadas en el artículo 6.1.b), dado que el mismo se produce como actividad encuadrada dentro de la ejecución del contrato de socio, que el socio lee y firma en el momento de darse de alta como socio y que regula la relación entre LLEFISA y el socio. Sobre la necesidad de controlar adecuadamente el acceso al Club, restringido únicamente para los socios y empleados del Club, *"queda manifiestamente claro que cualquier organización requiere de sistemas de control, ya sea mediante control personal o mediante control automatizado, para el adecuado acceso a las instalaciones y para la seguridad de sus equipos y otros bienes"*. Como proporcionalidad alude a la sentencia de asunto FITNESS MURCIA, SAN 1066/2020, fallada antes de la entrada en vigor del RGPD. Añade que los datos son recogidos para el acceso y uso del gimnasio y los socios no podrán ser identificados para otros fines distintos al control de acceso en las instalaciones, y los datos se eliminarán cuando cause baja como socio del gimnasio; en el contrato (normativa de socios) se informará del procedimiento de huella digital y si el cliente está conforme firma-

rá la normativa y accederá al Club, y “si no está conforme, no podrá acceder.” La EIPD no alude a otras modalidades de acceso más que la biométrica, aunque añade que “*Es cierto que la entidad manifiesta la prioridad de este sistema de acceso para evitar que otras personas puedan utilizar las instalaciones, y se decanta por querer limitar el acceso sin este dispositivo. No obstante, para casos puntuales facilitará un acceso mediante entrega de documento acreditativo de identidad, visualización en pantalla de ordenador de ficha de socio, etc., aunque no hará publicidad de ello.*”

En una de las conclusiones, figura que “*En la normativa de socios (equivalente al contrato) LLEFISA, SL, informará del nuevo tratamiento de datos a partir de su puesta en marcha y será atento al nivel de sensibilización de los mismos.*”

7) LLEFISA ha variado la redacción del contrato “normativa de socios” y la “autorización al tratamiento de datos personales”, aportando en alegaciones y en propuesta su nueva redacción.

Consiste la “autorización al tratamiento de datos personales”, en información de la recogida de datos, se remite a la “normativa de socios” especificando que aparte de los datos para la gestión y cobro de recibos y entrada en las instalaciones (con el nombre y apellidos, dni, dirección postal y electrónica y número de tarjeta o cuenta bancaria) y su tiempo de conservación que precisa, hay un apartado a continuación concreto de “registro de accesos”, en el que se explica la OPCION que toma la reclamada, y a la que antes se alude en el contrato “normativa de socios” de implantar la modalidad de “accesos mediante sistema con la biometría del socio-registro biométrico con código hash encriptado- y una pulsera personal” que complementa el uso biométrico (no señala el contenido o referencia de datos que contiene la pulsera ni el sistema en que se basa el citado registro biométrico, ya que pueden ser varios), continua informando que se usará:

- Con finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como instalaciones- equipos
- Siendo condición del servicio necesarias para el buen funcionamiento del centro (no detalla en qué sentido o conveniencia o interés y repercusión positiva que le da dicho uso o de que le viene dicho buen funcionamiento al centro), y
- Sirve también de “*control de acceso para los socios*”.
- “*La verificación de este registro de accesos con biometría es facilitar la verificación y acreditación de la condición de socio para evitar el acceso de personas no autorizadas.*”
- “*Se entenderá que autoriza el tratamiento de datos biométricos se si presta la obtención de su huella digital con el mecanismo NETGIN en la recepción.*”
- “*En otro caso podrá utilizar como medio alternativo de acceso a la presentación de su DNI o el pasaporte al personal de recepción del club en cada uno de sus accesos quienes validarán su condición de socio activo en el programa de gestión del centro y procederán a una apertura manual del torno sin que ello comprometa su condición de socio*”
- Firma del socio conforme.

Se considera que este documento no recaba el consentimiento para el tratamiento de datos pues no informa en concreto de que tipo de datos biométricos se tratarán, se ha de firmar en bloque el documento de “*firma conforme*”, cuando al mismo tiempo ofrece otra opción que no se puede seleccionar en ese momento y que es más gravosa, con la obligación de presentar en cada ocasión que se accede a la instalación un documento

como es el DNI. Se estima que dicha “*firma conforme*” resulta una mera información, sin posibilidad concreta en dicho instante de consentir el uso o no uso del sistema biométrico, o el sistema alternativo.

Además, sigue sin informar de la base legitimadora del tratamiento al significar: “*Se entenderá que autoriza el tratamiento de datos biométricos si se presta la obtención de su huella digital con el mecanismo de NETGIN en la recepción*” que por otro lado se opone a la definición de consentimiento:

*“toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen”*

## FUNDAMENTOS DE DERECHO

### I

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 5/12, 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 registrarán 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

El artículo 70 de la LOPDGDD establece los sujetos responsables señalando:

*“1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:*

*a) Los responsables de los tratamientos.  
(...)”*

En el presente supuesto, la parte reclamante firmó el contrato de socio del gimnasio con la entidad LLEFISA, S.L., siendo el responsable del tratamiento de sus datos, de acuerdo con la información relativa al tratamiento de sus datos.

El traslado de la reclamación o la entidad contra la que reclama la reclamante no son determinantes cuando se ha podido acreditar que la reclamante era usuaria del citado gimnasio cuya dirección describe y localiza, y que se acredita mantuvo la relación con LLEFISA.

### III

La reclamante firmó un contrato y una *AUTORIZACIÓN AL TRATAMIENTO DE DATOS PERSONALES* con LLEFISA el 2/09/2020. En los mismos se indicaba que los datos personales “*que ha facilitado*” serán *tratados por LLEFISA SL, SL, con la finalidad de gestionar su solicitud de incorporación como socio del gimnasio y finalidades inherentes como la gestión y cobro de recibos, la entrada en las instalaciones...*”. Si bien aparecía informada sobre el uso del “*sistema biométrico*” junto con la pulsera de acceso, calificándola de necesaria, y que “*en caso de no aceptarse nos impide prestar el servicio al socio*”. Se acredita que, a la firma de dicho contrato, no funcionaban los registros de la huella para dichos accesos en la instalación objeto de la reclamación. Se acredita que en la “*autorización*”, no consta que en aquellos momentos se le recogiera el dato de la huella a tal fin, ya que todavía no se estaba utilizando. De hecho, la información no especificaba, sino aludía a un “*sistema biométrico y la pulsera*”. De acuerdo con lo declarado por la reclamante, la concreta y efectiva petición del registro de la huella se produjo el 6/05/2021, fecha que coincide con su última asistencia al gimnasio registrada en la aplicación informática, así como la nota de la aplicación informática de 11/03/2021, conforme se negó a dar la huella para el registro.

Se deduce según las EIPD, dos, en las que aparece LLEFISA, que tenía programada su implantación para el primer trimestre de 2021. Se puede deducir que, la reclamante accediera de hecho, según declara, con la pulsera y una tarjeta (figura en su ficha de la aplicación que disponía de tarjeta).

Las finalidades que figuraban en la información del registro biométrico y la pulsera contenidas en el contrato y la autorización son contradictorias con las que se contienen en las EIPD y en el RAT de LLEFISA. En el contrato y la autorización, de 2/09/2020, fecha en que aún no se usaba la huella, se indica que sus datos: nombre y apellidos, DNI se tratan entre otros fines, para la entrada en las instalaciones. *A continuación, explica que “Con la finalidad de proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones, opta por un sistema de acceso mediante el registro biométrico (código hash encriptado) y una pulsera personal que complementará el uso biométrico.”*, cuando se acredita que ese no fue de inicio el modo de acceder de la reclamante al gimnasio

Continúa: “*La biometría y la pulsera deben actuar conjuntamente para poder acceder al centro, no siendo operativos de manera independiente. Son condiciones del servicio necesarias para el buen funcionamiento del centro, y que en caso de no aceptarse nos impide prestar el servicio al socio. De acuerdo con la normativa vigente en protección de datos, podrá ejercer los derechos de acceso, rectificación, limitación, supresión, portabilidad y oposición al tratamiento de sus datos de carácter personal, así como revocación del consentimiento prestado para el tratamiento de los mismos, dirigiendo su petición a LLEFISA SL, c/ Cisneros nº 67, 39007-Santander.*” Información que no se adecua al momento en que se dan los datos y al desarrollo de los hechos, dado que la reclamante usó la pulsera y tarjeta para su acceso, no siendo preciso el registro de la huella, que resultaría exigible más tarde. Además, no se alude en ningún punto a la prestación/obtención del consentimiento.

El artículo 5 del RGPD, relativo a los principios que han de regir el tratamiento de datos personales menciona entre ellos el de transparencia. El apartado 1 del precepto, dispone: “*Los datos personales serán:*

*a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»)*

Manifestación del principio de transparencia es la obligación que incumbe a los responsables del tratamiento de informar, en los términos del artículo 13 del RGPD, al titular de los datos personales, cuando éstos se obtengan directamente del interesado:

*“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 toda la información indicada a continuación:*

*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 finés 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 consen-*



miento 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 no facilitar tales datos;

f) la existencia de decisiones automatizadas, 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.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información."

En ese sentido, el Considerando 60 del RGPD dice que "Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe, además, informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran."

La reclamación que examinamos versa, entre otras cuestiones, sobre la adecuación a la normativa de protección de datos de la información que se proporciona por LLEFISA al recoger los datos personales de una persona que venía haciendo uso del sistema con acceso por otros medios distintos a la huella desde su inicio, 2/09/2020. Específicamente, respecto del dato del uso de la huella para el acceso al gimnasio, objeto de la reclamación.

Es informada la reclamante cuando se da de alta, del uso de sus datos, nombre y apellidos, dni, cuenta bancaria, para la gestión y cobro de cuotas y acceso a instalaciones, añadiéndose que la reclamada opta además por un "sistema biométrico", o "registro biométrico" a pesar de no estar en uso todavía, sin más especificación de entre los múltiples tipos de datos biométricos que se pueden emplear, para accesos a instalaciones. Si bien no se le recogió dato alguno de dicho tipo en aquel momento, hay que deducir que no se trató mientras tanto dicho dato, hasta el momento en que se le solicita el registro concreto de la huella a la reclamante.

No obstante, la información que consta en el contrato y en la cláusula de protección de



datos firmados por la parte reclamante y reclamada, cuando se hace usuaria carece de información sobre:

- base jurídica del tratamiento, no se expresa extremo alguno sobre la misma, tampoco en el apartado denominado “*protección de datos*”, ni en su número 18 del contrato “*normativa Metropolitana AQUA*” en que expresamente se identifica a LLEFISA como responsable del tratamiento.

- falta de información sobre finalidad del uso del sistema biométrico, y en todo caso, no se hace en el momento en que se le tratan de recoger a la afectada. Lo firmado por la usuaria se ha de considerar sobre los datos que en ese momento facilita y entonces, todavía no se había instaurado la huella. Mencionan el nombre y apellidos, o la tarjeta de crédito, no se especifica nada más. A continuación, introduce la referencia a la exigencia por necesidades del buen funcionamiento del centro, para proteger *la seguridad de las personas que acceden y sus pertenencias, así como las propias instalaciones*, de la opción del centro, del uso, exigencia, de que para acceder se precisa del registro biométrico y una pulsera, pero no funcionaba todavía en aquel momento. Por otro lado, esta finalidad el registro biométrico dada entonces para el futuro, no coincide con la que figura en la EIPD ni en el RAT.

- falta de información referida a la posible comunicación de datos a terceros.

- El plazo de conservación de los datos o, no siendo posible establecer un plazo, sobre los criterios utilizados para determinarlo.

- Tampoco informa de si se van a adoptar decisiones automatizadas a las que se refiere el artículo 22, apartados 1 y 4 del RGPD, incluida la elaboración de perfiles, y, si fuera así, sobre la lógica aplicada y sobre la importancia y consecuencias previstas de dicho tratamiento para el interesado.

- En el contrato y en la autorización, no se indica nada de acceso o uso alternativo al registro biométrico, ni 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 no facilitar tales datos;

- No se refiere a la retirada del consentimiento, sino a la revocación u oposición de este, teniendo en cuenta que la oposición al tratamiento se produce cuando la base de legitimación de los datos son el artículo 6.1.e) y f) del RGPD (art 21 del RGPD. Tampoco aludir a la revocación es técnicamente aceptable, puesto que el RGPD se refiere al derecho a la “*retirada del consentimiento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada*” (art 13.2.c RGPD) o el artículo 7, apartado 3), del RGPD, que establece que el responsable del tratamiento debe garantizar que el interesado pueda retirar su consentimiento en cualquier momento y que será tan fácil retirarlo como lo fue darlo, refiriéndose más que a un derecho, a una acción. Retirada del consentimiento, que no ha de llevar a sufrir perjuicio alguno ni disminuir el nivel en la prestación del servicio,

Carencia de información que no consta se hubiera variado a lo largo de la relación de

la usuaria con la reclamada, específicamente en el momento en que de modo efectivo se le fuera a recoger la huella.

La aportación en alegaciones de la modificación de las cláusulas de información en el contrato o en la autorización no acredita la fecha en que se implantan y no contemplan todos los aspectos referidos que constituyen el principio básico de transparencia en la recogida de los datos que se tratan. La manifestación de que estuvo expuesto como cartelera a título informativo tampoco queda acreditada y sigue sin contener todos los extremos de información, habiéndose aportado por la reclamada información a distintos usuarios con distintas fechas.

El artículo 13 del RGPD dispone que cuando los datos personales se recaben de un interesado -lo que acontece a través del contrato y la “autorización” objeto de la reclamación- el responsable del tratamiento está obligado, en ese preciso momento, esto es, cuando los obtiene, a informar al titular de los datos, y en relación con los datos que va a tratar, no los que en el medio o largo plazo va a tratar. Estos, en su caso han de ser objeto de cuando se recojan y se inicie el tratamiento.

Debe tenerse en cuenta que la información de la recogida de datos debe ajustarse a los que efectivamente se recogen, y efectivamente se van a tratar a continuación y ese es el motivo de que se le tenga que informar. No puede servir una información en diferido de unos datos que se recogerán o cuyo sistema está previsto instaurar en un futuro, a medio plazo, 6 meses, o a largo plazo por ejemplo un año, pues además de no ajustarse al principio de lealtad, ofrece inseguridad en el tratamiento, debiendo tenerse por no puesta dicha información al no ajustarse a los hechos. En este caso, la información de unos datos que se van a recoger en un futuro podría carecer de efectos, al no darse el supuesto de hecho mismo sobre el objeto en que recae (recogida y uso de la huella para el acceso). Obsérvese que se refiere la información a un tratamiento “sistema biométrico” para acceso y la información parcial que se le asocia, cuando, además, ni los datos se recogieron (la huella en este caso concreto para el acceso, en mayo 2021) ni se almacenaron ni se usaron.

El tratamiento ulterior que se materializa cuando se pretendían recoger los datos de la reclamante, es cuando tenía que haber completado la información sobre dicho tratamiento, pues esta obligación, de acuerdo con las Directrices sobre la transparencia en virtud del RGPD, dictadas por el Grupo de trabajo del artículo 29 adoptadas el 29/11/2017, y revisadas el 11/04/2018, (punto 5), no es en modo alguno estática, sino que se ha de adecuar a los ciclos y operaciones de tratamiento y las eventuales modificaciones que puedan darse, especialmente si suponen un cambio esencial con respecto a la operación de tratamiento como es la toma y uso de huellas dactilares para acceso a una instalación, deportiva en este caso.

La reclamada, en su condición de responsable del tratamiento, conforme al artículo 13 RGPD estaba obligada a informar en el documento mediante el que recaban los datos de los usuarios, incluyendo como señala el artículo, las repercusiones de no darlos, en el momento en que se recaban. Por ello, el hecho de que la reclamante no diera la huella no se considera que exima de dar dicha información, máxime siendo ya usuaria del gimnasio como en este caso. Además, consta expresamente entre dicha obligación, los efectos que han de surtir en caso de no proporcionar los citados datos. Se observa pues y así se declara que, se ha prescindido parcialmente de diversa

información fundamental para el tipo de tratamiento que se lleva a cabo, considerando que se ha vulnerado el citado artículo 13 del RGPD por la reclamada.

#### IV

Como tipos específicos, los datos biométricos quedan definidos en el artículo 4.14 del RGPD:

*«datos biométricos»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos;*

Para considerarse datos biométricos en el sentido del RGPD, el tratamiento de datos sin procesar, como las características físicas, fisiológicas o conductuales de una persona física deben implicar una medición de dichas características. Así pues, del concepto, no hay que perder de vista:

-La naturaleza de los datos: datos relativos a las características físicas, fisiológicas o conductuales de una persona física;

- Los medios y las formas de tratamiento: datos *«obtenidos a partir de un tratamiento técnico específico»*; lo que diferencia por ejemplo de las imágenes de una persona que figuran en un sistema de videovigilancia, que no pueden considerarse datos biométricos si no se han tratado técnicamente de una forma específica con el fin de contribuir a la identificación única de esa persona. El considerando 51 del RGPD también se refiere a la no consideración sistemáticamente como un tratamiento de categoría especial de datos, a las fotografías, a menos que se les aplique un medio de tratamiento técnico específico que *“permita la identificación o la autenticación unívocas de una persona física”*.

- La finalidad del tratamiento: los datos se deben utilizar para la finalidad de identificar de manera unívoca a una persona física.

Los datos biométricos presentan la particularidad de ser producidos por el propio cuerpo y lo caracterizan definitivamente, son datos no sobre esa persona, sino que los datos refieren a la misma persona, en principio no modificables por voluntad del individuo, ni la persona puede ser liberada de ellos, no se pueden cambiar en caso de compromiso-pérdida o intrusión en el sistema. Además, debido a que los datos biométricos son propios de una persona y perpetuos, el usuario utiliza los mismos datos en diferentes sistemas. Por lo tanto, un robo de identidad no solo es perpetuo en el tiempo, sino que afecta a todos los sistemas en que un usuario tenga almacenados sus datos biométricos. El titular, por lo tanto, no tiene la posibilidad de utilizar un dato biométrico para el banco, y uno diferente para su sistema de salud, sino que utiliza la misma información para verificar su identidad en ambos, y frente a una vulnerabilidad se ven afectados todos ellos al mismo tiempo.

Todo ello, sin perder de vista que se trata de un sistema de identificación muy intrusivo para los derechos y libertades fundamentales de las personas físicas, entre otras circunstancias por el funcionamiento a través de sistemas de inteligencia artificial que im-

plementan algoritmos para diseñar y leer la plantilla biométrica, puesto en relación con la deficiencia en las normas de fabricación de sistemas homologados y certificados del software de uso, añadido a la extensión e interoperabilidad de uso de estos sistemas.

También de partida, hay que destacar la nota del carácter restrictivo, pues su tratamiento está prohibido, determinando el artículo 9.1 del RGPD:

*“Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o la orientación sexual de una persona física.”*

2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

Solo se pueden tratar con carácter excepcional, en determinados supuestos que se contemplan en el RGPD, que prevé unos estrictos requisitos para posibilitar finalmente la puesta en funcionamiento de tales sistemas, debido a la afectación a los derechos y libertades fundamentales, por los riesgos que puede entrañar el contexto de su tratamiento, y que como señala el Considerando 51 del RGPD: *“Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.”*

La definición de dato biométrico alude a “tratamiento técnico”, sin especificar, excepto para reseñar que el propósito de dicho tratamiento debe ser identificar a una persona. Las características biométricas se someten a un tratamiento técnico mediante un proceso que se contiene en todos los tratamientos de datos biométricos: captura o registro de datos, almacenamiento o procesamiento y última fase de comparación.

Se reduce la imagen bruta de las características biométricas, transformándose, conservándose información discriminada destacada que es esencial para el reconocimiento de la persona. Estas características extraídas se mantienen en una plantilla biométrica, que es una forma de representación matemática reducida de la característica original. La plantilla de referencia se almacena para su comparación. En la última fase, se comparará una muestra biométrica-como el dedo presentado al sensor con una plantilla previamente grabada. Las fases se avienen con la enumeración de lo que podría ser una operación de tratamiento de datos (recogida, almacenamiento, uso).

Por un lado, la definición de datos biométricos incluye que a través del tratamiento técnico específico, “*permitan o confirmen*” “*la identificación única*” de dicha persona. Las menciones a “*permitan*” pueden entenderse a la identificación, la de “*confirmen*” a la verificación. Por tanto, ambas, identificación o autenticación han de ser únicas, referidas a la identificación que se produzca de la persona. La identificación única por otro lado va más allá de que el dato sea de una persona física identificada o identificable. Dato de persona física identificada es que esa persona se la distingue o aísla de un grupo de personas. Único, puede referirse a que los datos biométricos tienen tales particularidades que pueden identificar sin ambigüedades a un individuo.

Las diferencias entre los términos identificación- autenticación se refieren al modo de búsqueda en los registros almacenados y al ingreso previo del registro, según se desprende del Dictamen 3/2012, del GT 29, de 27/04/2012, sobre la evolución de las tecnologías biométricas, momento en que los datos biométricos no gozaban de la categoría de “*especiales*” que introduce el RGPD y no se aludía por tanto al termino “*dirigidos a la identificación unívoca*”.

El considerando 51 señala que “*El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento*”.

Técnicamente, la plantilla biométrica contra la que se coteja la muestra es el producto de una medición que identifica unívoca y únicamente al individuo. Esto es lo que por ejemplo diferencia las imágenes visionadas de una videocámara que no pueden ser consideradas dato biométrico bajo la definición del artículo 9 si no son específicamente tratadas con un medio técnico para contribuir a la identificación de una persona.

Los datos biométricos de cada usuario, adquiridos en el momento de su captación y registrados, para someterlos al procedimiento técnico que convierte la imagen, el formato, en muestra biométrica y el algoritmo en plantilla biométrica, almacenándose, para que, con las muestras introducidas al colocar el dedo en los accesos, identifique a través del modelo guardado, de entre todas las plantillas, sin lugar a duda a su titular, lo que sería de forma única a dicha persona.

El uso de la huella no solo es capaz de validar la identidad de forma precisa, sino que tiene información única sobre personas físicas. El algoritmo del software, sobre la muestra biométrica, extrae las características biométricas, reduce y transforma en



etiqueta o números esa muestra, constituyendo una representación matemática de la característica biométrica original, que es la plantilla biométrica. La plantilla se almacena para su comparación en la última fase en la cual con la muestra biométrica-huella en el lector-y con la plantilla previamente grabada, está identificando unívocamente al empleado, en cada ocasión que entra o sale poniendo su huella en el lector, por lo que se considera que los datos entran dentro del ámbito de los datos especiales.

En el presente caso, desde luego, no puede hablarse de que no se trata información ligada a datos personales de una persona identificada en cada registro de accesos, aunque los datos se guarden en el dispositivo cifrados/encryptados. Cada vez que un usuario utiliza el sistema, permite o confirma su identificación única a través del tratamiento que lleva a cabo la reclamada con el dispositivo adquirido. La muestra presentada se compara y el sistema tiene la función de identificación con una función biométrica, identificando únicamente al usuario que dice ser y registrando sus datos, ya que se debe señalar que si no permitieran la identificación inequívoca del usuario no se produciría el libre acceso del socio a la instalación

## V

Acreditado así, que se trata de datos de carácter especial, para tratar categorías especiales de datos, debe encontrarse cobertura en el artículo 9.2 del RGPD y una vez excepcionada la prohibición general, hay que acudir a los supuestos del artículo 6.1 del RGPD para dar licitud al tratamiento en cuestión.

Los responsables del tratamiento solo pueden tratar datos personales de categoría especial si se cumplen una de las condiciones previstas en el artículo 9, apartado 2, así como una condición del artículo 6, por lo que procede reproducir el precepto:

*“1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:*

*a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;*

*b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;*

*c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;*

*d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;*

*e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;*

*f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos*

*por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*

*Lo dispuesto en la letra f) del párrafo primero no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones.”*

No figura referencia alguna como base jurídica del tratamiento del registro biométrico para acceso al gimnasio de la reclamada referida al consentimiento en la información del tratamiento proporcionada a la reclamante.

Es más, aunque existiera, como habría de prever la opción de no otorgarlo sin consecuencia alguna negativa, no se estima el mismo una base jurídica del tratamiento adecuada para el tratamiento de datos en esa modalidad con la prestación de este servicio, a menos que se diera una alternativa distinta real y efectiva al uso de la huella. En este caso, además, no queda acreditado que para la prestación del servicio fuera o sea necesario el uso de la huella dactilar (la reclamante estuvo desde 2/09/2020 sin usarla, acreditándose la innecesariedad)

Sobre la pretensión de la reclamada de que el hecho de someterse a la captación de la huella supone consentimiento al tratamiento, se ha de entender que dada la especificidad del consentimiento, y la información que ha de ir asociada al mismo, así como la opción voluntaria de no someterse al mismo sin sufrir repercusión negativa, no constituye per se una base jurídica del tratamiento legitimadora adecuada, al menos que se desarrolle convenientemente, tanto la información de su uso, como una alternativa libre de no uso para los que no deseen otorgar dicho consentimiento explícito por tratarse de dato biométrico especial.

Usualmente esta base jurídica del tratamiento ha de ir precedida de un adecuado análisis de la necesidad y proporcionalidad de las circunstancias de implantación y uso de la huella, las alternativas a su empleo y la afectación a los derechos de sus titulares, riesgos, garantías y las medidas de seguridad que con el desarrollo de la tecnología.

La instauración del consentimiento como base jurídica del tratamiento, en el uso de la huella dactilar puede incidir en la prestación de un servicio que se contrata, condicionándolo a la aceptación de esas modalidades de tratamiento, por la posición jurídica del responsable.

LLEFISA además cuenta en su RAT que la base jurídica del tratamiento es el consentimiento y el contrato mercantil. Acreditado que no hay tal consentimiento, se ha de analizar la relación contractual como legitimación para el registro de huellas para acceder a las instalaciones, que se incurriría en el artículo 6.1.b del RGPD, como:

*“el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;”*

Relacionando los fines que pretendía la reclamada con el uso de la huella:

-gestión de los datos personales de los abonados para permitirles el acceso a la instalación. (RAT).

- que el sistema reconozca al interesado y permita, mediante esta identificación, acceder al gimnasio. (EIPD).

- proteger la seguridad de las personas que acceden al centro y sus pertenencias, así como las propias instalaciones (contrato y autorización), *condiciones del servicio necesarias para el buen funcionamiento del centro y el control de acceso para solamente los socios*

En cualquier caso, no resulta necesario para la ejecución del contrato el registro de las huellas para el acceso, cuando puede haber otros medios para acceder como se acredita con la reclamante que estuvo usando desde su alta, tiempo en que no estaba instaurada la huella, utilizando las instalaciones.

Por otro lado, la reclamada no acredita tampoco en la EIPD la necesidad y la proporcionalidad de la instauración de la huella para dichos fines.

De este modo, se aprecia que la inicial infracción del artículo 7.4 del RGPD- condiciones del consentimiento- imputado a LLEFISA, deba ser modificada.

El precepto que fía al consentimiento del interesado al tratamiento no concurre, al no constar la base del consentimiento, no solo porque no se contiene extremo alguno que refiera los elementos propios de dicha figura para decidir sobre el mismo, ni siquiera se menciona, y ni se refiere ni tan siquiera como base jurídica del tratamiento, a efectos informativos. Además, como se ha insistido podría no ser una base jurídica de legitimación para el tratamiento de la huella dactilar en la prestación de un servicio sin alternativa a su no uso. Ello supone que la imputación del citado artículo deba variarse.

Aparte del consentimiento como base jurídica del tratamiento, del resto de las contempladas en el 6.1 del RGPD, todas suponen la “*necesidad*” del tratamiento, término que se contiene expresamente. En este sentido, el Comité Europeo de Protección de Datos (antiguo Grupo de Trabajo del artículo 29) en su dictamen sobre “*Directrices sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del Reglamento 2016/679*” indica que para tratar categorías especiales de datos debe encontrarse cobertura en el artículo 9.2 RGPD y una vez excepcionada la prohibición general, hay que acudir a los supuestos del artículo 6 RGPD para dar licitud al tratamiento en cuestión. (...) Los responsables del tratamiento solo pueden tratar datos personales de categoría especial si se cumplen una de las condiciones previstas en el artículo 9, apartado 2, así como una condición del artículo 6. (...)”

Sobre la alegación de que se da por probado que los usuarios solo tienen el medio de uso de huella y pulsera para los accesos al gimnasio, se indica que no figura así en hechos probados.

Considerando que se contienen datos incluidos en el artículo 9.1, con las excepciones al tratamiento que se prevén en el 9.2 del RGPD, que se acredita no concurren en la reclamada, y que, además, se precisa de una base legitimadora dentro del artículo 6.1 del RGPD, no siendo válida la alegada para el supuesto, la del artículo 6.1.b) del RGPD, se considera que LLEFISA, ha infringido los siguientes dos artículos:

-artículo 9.1 del RGPD, y

-artículo 6.1 del RGPD.

## VI

Los poderes correctivos de los que dispone la Agencia Española de protección de Datos, como autoridad de control, se establecen en el artículo 58.2 del RGPD. Entre ellos se encuentran la potestad de imponer una multa administrativa con arreglo al artículo 83 del RGPD -artículo 58.2 i)-.

En el presente caso, atendiendo a los hechos expuestos, se considera que las sanciones que correspondería imponer son de multas administrativas por tratarse de la prestación de un servicio oneroso, que en este caso afecta a consumidores y en un número, si no masivo, si elevado, en este caso más de mil potenciales usuarios que responden a una oferta de dicho tipo de servicios y dados los estrictos requisitos del tratamiento de este tipo de datos, siendo el de información sobre el tratamiento un contenido esencial del derecho dentro del tratamiento de datos y por la tipología y especificidad del dato huella dactilar cuyo tratamiento prohibido reúne diversos requisitos en supuestos en que su uso sea necesario.

En respuesta a la alegación de la reclamada de que se discrimina con por ejemplo el ámbito público, se ha de señalar que en estos supuestos no procedería sanción económica por señalarlo expresamente el artículo 77 de la LOPDGDD que puede dar lugar a toma de otras medidas indicadas en su punto 3.

## VII

Las infracciones que se le atribuyen a la reclamada se encuentran tipificadas en el artículo 83.5 del RGPD, que considera que la infracción de

- *“a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9” y*

- *“b) los derechos de los interesados a tenor de los artículos 12 a 22;*

*que,” son sancionables, de acuerdo con el apartado 5 del mencionado artículo 83 del citado Reglamento, “con multas administrativas de 20.000.000€ 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”.*

La LOPDGDD en su artículo 72.1, considera, a efectos de prescripción, que son: *“Infracciones consideradas muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

*“b) El tratamiento de datos personales sin que concurra alguna de las condiciones de licitud del tratamiento establecidas en el artículo 6 del Reglamento (UE) 2016/679.”*

*“e) El tratamiento de datos personales de las categorías a las que se refiere el artículo 9 del Reglamento (UE) 2016/679, sin que concurra alguna de las circunstancias previstas en dicho precepto y en el artículo 9 de esta ley orgánica.”*

También dentro de la LOPDGDD, el artículo 74 considera *“leves y prescribirán al año las restantes infracciones de carácter meramente formal de los artículos mencionados en los apartados 4 y 5 del artículo 83 del Reglamento (UE) 2016/679 y, en particular, las siguientes:*

*(...)*

*“a) El incumplimiento del principio de transparencia de la información o el derecho de información del afectado por no facilitar toda la información exigida por los artículos 13 y 14 del Reglamento (UE) 2016/679.”*

## VIII

Las multas que se impongan deberán ser, en cada caso individual, efectiva, proporcionada y disuasoria, de acuerdo con el artículo 83.1 del RGPD. A fin de determinar la multa administrativa a imponer se han de observar las previsiones del artículo 83.2 del RGPD, que indica:

*“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, en relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, “Sanciones y medidas correctivas”, 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 a 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 incluir 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”.*

*En relación con la alegación de que las agravantes constituirían una doble computación de factores, al ser la infracción ya muy grave se ha de señalar que el artículo 83.2 del RGPD ya previene que tanto para la imposición de la sanción como*

*para su cuantía se han de prevenir las circunstancias que concurren en los hechos valorados*

*Por otro lado, dicha valoración conjunta y sistemática puede dar como resultado que se concluya de variados elementos un aumento o reducción de la antijuridicidad o la culpabilidad que han de concurrir en los hechos, por lo que la alegación de la reclamada no puede ser estimada*

Para la infracción del artículo 13 del RGPD, se impone una multa de 2000€ (dos mil euros).

Para la infracción del artículo 9.1 del RGPD, a efectos de fijar el importe de la sanción a imponer en el presente caso, se considera que procede graduar la sanción de acuerdo con las siguientes circunstancias incluidas en el artículo 83.2 del RGPD:

Como circunstancias agravantes:

- artículo 83.2.g) del “*las categorías de los datos de carácter personal afectados por la infracción*”.

El diccionario de la RAE define el término “categoría” como “*cada una de las clases o divisiones establecidas al clasificar algo*”. La lectura del artículo 83.2.g) del RGPD nos remite, inicialmente, -haciendo una interpretación literal y estricta de la norma- a la rúbrica del artículo 9 del RGPD, “*Tratamiento de categorías especiales de datos personales*”, concluyendo así que el RGPD clasifica los datos personales, únicamente, en especialmente protegidos y el resto.

Sin embargo, una interpretación sistemática y teleológica del artículo 83.2.g) del RGPD conecta este precepto con otras clasificaciones que ofrece el texto del RGPD que, además, responden mejor a la finalidad que persigue la norma: graduar en el caso individual la multa administrativa que deba imponerse respetando en todo caso los principios de proporcionalidad y efectividad.

En ese sentido los considerandos 51 y 75 del RGPD distinguen un grupo de datos personales que, por su naturaleza, son *particularmente sensibles* por razón del importante riesgo que pueden entrañar, en el contexto de su tratamiento, para los derechos y libertades fundamentales. El común denominador de todos ellos es que su tratamiento comporta un *riesgo importante* para los derechos y las libertades fundamentales ya que puede llegar a provocar daños y perjuicios físicos, materiales o inmateriales. En este grupo o categoría de datos *particularmente sensibles* se incluyen las categorías de datos especialmente protegidos que regula el artículo 9 del RGPD -considerando 51 del RGPD- y, además, otros muchos datos no regulados en ese precepto. El considerando 75 menciona con detalle los datos personales cuyo tratamiento puede entrañar un *riesgo, de gravedad y probabilidad variables*, para los derechos y libertades de las personas físicas como consecuencia de que pueden provocar daños y perjuicios físicos, materiales o inmateriales. Entre ellos menciona aquellos cuyo tratamiento “*pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo*”.

En el presente caso, se estima que el hecho de que el consentimiento para el tratamiento de los datos de la reclamante que la reclamada efectuó hubiera recaído sobre un dato particularmente sensible, huella dactilar, incide en la gravedad de la conducta debiendo apreciar la concurrencia en calidad de agravante de la circunstancia del apartado g) del artículo 83.2. RGPD.

-Circunstancia del artículo 83.2.k) RGPD en relación con el artículo 76.2.b) LOPDGDD: La vinculación entre la actividad empresarial de la reclamada y el tratamiento de datos personales.

La reclamada, en el desarrollo de la actividad que le es propia, necesita tratar de forma habitual datos de carácter personal y este hecho incide en la diligencia que resulta exigible en el cumplimiento de los principios que presiden el tratamiento de datos de carácter personal y en la calidad y efectividad de las medidas técnicas y organizativas que debe tener implementadas para garantizar el respeto de este derecho fundamental tanto de sus clientes como de terceros.

Respecto a la alegación de la reclamada de que no existe tal vinculación entre su actividad empresarial deportiva y el tratamiento de datos personales y que su actividad es de puesta a disposición de los clientes de máquinas, equipos, entrenadores, para lo cual no necesita tratar, ni trata de forma habitual datos de carácter personal, los hechos son que es una actividad lucrativa que presta una serie de servicios variados y precisa datos para la gestión ordinaria de la misma, utilizando desde hace tiempo diversas tecnologías que enlazan los datos de los usuarios para la gestión del mismo, tanto a nivel de tecnologías: pulsera, huella, como afectando a su implantación interna de software de gestión, contrato de encargo de tratamiento, por poner solo un ejemplo

- Del artículo 83.2.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”*.

El número de personas afectadas pues, aunque se trate de un único reclamante es evidente que se han visto afectados todos los clientes de la entidad.

Del artículo 83.2.b) *“la intencionalidad o negligencia en la infracción”*. En el cumplimiento de sus obligaciones legales -por lo que aquí interesa del principio de obtención del consentimiento para un tratamiento lícito de datos- la reclamada debe de actuar con la diligencia que las circunstancias del caso exigen. A propósito del grado de diligencia que el responsable del tratamiento está obligado a desplegar puede traerse a colación la sentencia de la Audiencia Nacional, Sala de lo Contencioso Administrativo, de 17 de octubre de 2007 (rec. 63/2006), que, aunque dictada bajo la vigencia de la normativa precedente resulta extrapolable al asunto que nos ocupa. La SAN, después de indicar que las entidades en las que el desarrollo de su actividad conlleva un continuo tratamiento de datos de clientes y terceros han de observar un adecuado nivel de diligencia, precisa que *“...el Tribunal Supremo viene entendiendo que existe imprudencia siempre que se desatiende un deber legal de cuidado, es decir, cuando el infractor no se comporta con la diligencia exigible. Y en la valoración del grado de diligencia ha de ponderarse especialmente la profesionalidad o no del sujeto, y no cabe duda de*

*que, en el caso ahora examinado, cuando la actividad de la recurrente es de constante y abundante manejo de datos de carácter personal ha de insistirse en el rigor y el exquisito cuidado por ajustarse a las prevenciones legales al respecto*". (El subrayado es de la AEPD).

En este supuesto la falta de diligencia de la reclamada debe calificarse de "grave". La entidad debería haber sido particularmente escrupulosa en la verificación de la obtención de alguna excepción para el tratamiento de los datos inicialmente prohibidos y que el estudio de "viabilidad", realizado por la DPD afirmaba que necesitaba para su tratamiento de una doble habilitación.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD y 76.2 de la LOPDGDD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 9.1 del RGPD, conduce a la imposición de una sanción de 15.000 euros.

En cuanto a la infracción del artículo 6.1 del RGPD, se han de atender las siguientes circunstancias para la graduación de la infracción:

*-Del artículo 83.2.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"*. Ni la relación contractual puede coadyuvar a una necesaria implantación de un sistema de tratamiento al margen de un profundo análisis de necesidad y proporcionalidad, ni el supuesto consentimiento, por lo que dada la naturaleza del tratamiento y desde la fecha en que aparece implantado, mayo 2021, y que alcanza a todos los usuarios, se estiman elementos agravantes.

En función de este contexto, la infracción que se impone es de 10.000 euros.

Sobre la ausencia de culpabilidad por haberse analizado los riesgos y no haberse vulnerado las medidas de seguridad, no se valoran esos elementos en este procedimiento, y la culpabilidad como capacidad que tiene el sujeto obligado para obrar de modo distinto y, por tanto, de acuerdo con el ordenamiento jurídico, es claro que concurre, recordando que el Tribunal Supremo (Sentencias de 16 y 22/04/1991) considera que del elemento de la culpabilidad se desprende *"que la acción u omisión, calificada de infracción sancionable administrativamente, ha de ser, en todo caso, imputable a su autor, por dolo o imprudencia, negligencia o ignorancia inexcusable."*

Sobre la alegación de la situación económica de la reclamada, analizadas las cifras se estima que las cuantías de las tres sanciones son difíciles que comprometan la estructura económica o futuro de la misma, dadas las cifras de ingresos, considerándose los puntos de los que en el propio 83.5 del RGPD se parten, y se pueden considerar proporcionales y disuasorias por la vulneración de los preceptos examinados que se han infringido a los más de mil usuarios de sus servicios.

Sobre la existencia de DPD como atenuante, el precepto señala que *"podrá, tenerse en cuenta"* con lo cual no se puede aceptar automáticamente. En este caso la realización de las infracciones, que no tienen carácter episódico sino estructural, su permanencia tal existencia no ha servido para lo contrario, sin que por otro lado se haya analizado su papel en los tratamientos.

En cuanto a que no se han practicado pruebas y ello ha de servir como atenuante, se debe indicar que no especifica sobre qué hecho se debía practicar, o como sería el hecho caso de haberse practicado si se hubiera solicitado, siendo lo cierto que no fue propuesta en alegaciones al acuerdo de inicio. Por otra parte, tal y como señala el artículo 77 de la LPCAP no es un trámite preceptivo, considerando que no existía en el marco del procedimiento sancionador disconformidad sobre los hechos.

Finalmente, sobre que las infracciones declaradas no afectarían a todos los socios, señalado en este caso que la acción de someterse a la recogida de la huella per se no cumple los requisitos del consentimiento, ni se considera explícito con respecto a la normativa de protección de datos, no es incorrecta la mencionada afectación a todos, lo mismo que la cláusula informativa.

## IX

El artículo 58.2 del RGPD dispone lo siguiente: *“Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

*d) 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;”*

*f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición; [...]”*

*i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;”*

*“La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.”*

No se acredita que la reclamada haya dejado de utilizar la huella, como medio de acceso a la instalación deportiva utilizando una modalidad que incurre en la misma ausencia de base legitimadora y habilitación del tratamiento prohibido de la huella que se ha señalado en esta resolución para todo el colectivo sobre el que se han recogido los datos de la huella basados en el mismo clausulado. Las medidas de readaptación del tratamiento no se acreditan que hayan tenido lugar de modo efectivo durante la tramitación del expediente para todos los titulares sobre los que en su momento y con tales premisas se les recogieron sus datos, siendo una de las más importantes el reflejo expreso de una medida alternativa al uso de huella dactilar como consta que disponía.

Se considera pues que, con el fin de garantizar los derechos y libertades de los titulares de los datos, que concurre la necesidad y justificación de adoptar poderes correctivos que se determinan en la parte dispositiva.

El artículo 90.3 de la LPCAP indica que *“la resolución que ponga fin al procedimiento será ejecutiva cuando no quepa contra ella ningún recurso ordinario en vía administrativa,*



*pudiendo adoptarse en la misma las disposiciones cautelares precisas para garantizar su eficacia en tanto no sea ejecutiva”*

En el texto de la resolución se establecen cuáles han sido los hechos que determinan la necesidad de adecuación a la normativa de protección de datos, de lo que se infiere con claridad cuáles son las medidas a adoptar, sin perjuicio de que el tipo de procedimientos, mecanismos o instrumentos concretos para implementarlas corresponda a la parte sancionada, pues es el responsable del tratamiento quien conoce plenamente su organización y ha de decidir, en base a la responsabilidad proactiva y en enfoque de riesgos, cómo cumplir con el RGPD y la LOPDGDD.

Se le informa de que, según el artículo 83.6 del RGPD, el incumplimiento de las resoluciones de la autoridad de control adoptadas de acuerdo con el artículo 58.2 del RGPD constituye en sí misma una infracción autónoma, que dará lugar a la apertura del correspondiente expediente sancionador por dicha infracción, para la que se prevé una sanción de multa de hasta 20 000 000 de euros como máximo o, tratándose de una empresa, de una cuantía equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: IMPONER a **LLEFISA, S.L** con NIF **B60422417** por las siguientes infracciones del RGPD:

-artículo 13 del RGPD, de conformidad con el artículo 83.5.b) del RGPD, tipificada a efectos de prescripción en el artículo de la LOPDGDD, una multa administrativa de 2.000 euros.

-artículo 9.1 del RGPD, de conformidad con el artículo 83.5.a) del RGPD, tipificada a efectos de prescripción en el artículo 72.1.e) de la LOPDGDD, una multa administrativa de 15.000 euros.

--artículo 6.1 del RGPD, de conformidad con el artículo 83.5.a) del RGPD, tipificada a efectos de prescripción en el artículo 72.1.b) de la LOPDGDD, una multa administrativa de 10.000 euros.

SEGUNDO: Requerir a **LLEFISA SL**, en aplicación de los artículos 90.3 de la LPCAP, y 58. 2.d) y f), del RGPD, para que:

-Acredite en el plazo de 30 días, una correcta y adecuada implantación del sistema de uso de huella dactilar para acceso a instalaciones, considerando y acreditando su necesidad y proporcionalidad atendiendo a instauración de una base de tratamiento lícita para el tratamiento de los datos, también respecto a los que ya se disponen de ese dato, y a su correlativa información del tratamiento asociada a la misma.

-Proceda a: “*limitar temporal o definitivamente el tratamiento*” en el plazo de diez días sobre el uso del sistema de acceso al gimnasio con huella dactilar, en tanto no acomode la base legitimadora del tratamiento y su correcta información a los usuarios.

Transcurrido el tiempo otorgado, deberá informar a esta AEPD.

La falta de atención al requerimiento puede dar lugar a la comisión de una infracción del artículo 83.6 del RGPD,

TERCERO: NOTIFICAR la presente resolución a **LLEFISA, S.L.**

CUARTO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la LPACAP, en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29/07, en relación con el art. 62 de la Ley 58/2003, de 17/12, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **IBAN: ES00-0000-0000-0000-0000-0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

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

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13/07, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [<https://sedeagpd.gob.es/sede-electronica-web/>], o a través de alguno de los restantes registros previstos en el art. 16.4 de la

citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-181022

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