- **Expediente N.º: EXP202405327**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

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

HECHOS

PRIMERO: Con fecha 19 de marzo de 2024 se interpuso reclamación ante la Agencia Española de Protección de Datos por una posible infracción imputable a **LUDE GESTIONES Y SERVICIOS, S.L.** con NIF **B35787811** (en adelante, LUDE) y **MACROFIT CANARIAS, S.L.** con NIF **B76175355** (en adelante, MACROFIT)

Los hechos que se pone en conocimiento de esta autoridad son:

La reclamante pone de manifiesto que para acceder a las instalaciones de MACRO FIT ******CENTRO.1***, se establece como requisito obligatorio la recogida de la huella digital de los usuarios, lo que entiende como un tratamiento de datos no proporcional y que pudiera contravenir la normativa de protección de datos. Señala asimismo que se conservan datos de los usuarios, pese a haberse tramitado su baja.

Junto al escrito, se aporta:

- Copia de contrato de alta de abono de fecha 16 de diciembre de 2023, donde aparece el nombre y apellidos (***A.A.A.),*** dirección de correo (******EMAIL.1***), DNI, teléfono, datos bancarios y firma. Contiene, entre otras, las siguientes cláusulas:

  "ACCESO: El acceso a la instalación se hará por medio de un sistema de doble seguridad, en la que se verifica la identidad del cliente mediante la huella digital y tarjeta, pulsera o llavero. La huella del cliente quedará guardada, exclusivamente, en su tarjeta (llavero o pulsera), no quedando archivada en ningún dispositivo ni base de datos de MACRO FIT. En caso de olvido y de forma excepcional, se permitirá el acceso a la instalación previa identificación en la recepción. En todo caso, la pérdida, el deterioro o el olvido de la tarjeta u otro medio de acceso, en tres ocasiones durante un mes, obligará a solicitar un duplicado sin el cual no se le permitirá el acceso. El coste del duplicado, será de 4,00€ (tarjetas), o el precio estipulado si es otro medio (pulsera, llavero).

  NORMATIVA DE USO: El que suscribe, conoce y acepta las condiciones aquí indicadas, así como la NORMATIVA, la cual se puede solicitar en recepción en cualquier momento o visualizar en la web de Macro Fit (www.macrofit.es/normativa).

*TRATAMIENTO DE DATOS. Las diversas sociedades que gestionan gimnasios de la marca MACRO FIT (Lude Gestiones y Servicios, S.L., Macrofit Canarias**,** S.L, *****EMPRESA.1 y ***EMPRESA.2**) son los Responsables del tratamiento de los datos personales del Interesado y le informa que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril (GDPR) y la Ley Orgánica 3/2018 de 5 de diciembre (LOPDGDD), por lo que se le facilita la siguiente información del tratamiento. Fin del tratamiento: mantener una relación comercial en base a un interés legítimo por parte del responsable y/o la celebración de un contrato con el usuario. Criterios de conservación de los datos: se conservarán durante no más tiempo del necesario para mantener el fin del tratamiento y cuando y cuando ya no sea necesario para tal fin, se suprimirán con medidas de seguridad adecuadas para garantizar la seudonimización de los datos o la destrucción total de los mismos. Comunicación de los datos: No se comunicarán datos a terceros salvo obligación legal (salvo aquellas cesiones necesarias entre las empresas del grupo mencionadas en la presente cláusula). Derechos que asisten al Interesado: Derecho a retirar el consentimiento en cualquier momento. Derecho de acceso, rectificación, portabilidad y supresión de sus datos y a la limitación u oposición a su tratamiento. Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente. Datos de contacto para ejercer sus derechos: Lude Gestiones y Servicios, S.L. Macro Fit […]".*

- Copia del documento de baja de abono "*Macrofit*" con fecha de solicitud 2 de marzo de 2024 y fecha de baja 15 de marzo de 2024, donde aparece el número de cliente, nombre y apellidos (***A.A.A.)***, dirección de correo (******EMAIL.1***) y firma.

- Orden de domiciliación de pagos de fecha 16 de diciembre de 2023, con *MACRO FIT ***CENTRO.1*, (…), y donde figura como nombre del deudor: ***A.A.A.***, los datos bancarios del mismo, la fecha, y la firma del cliente.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a LUDE, 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.

La notificación del traslado de la reclamación, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue realizada en fecha 13 de abril de 2024 como consta en el acuse de recibo que obra en el expediente.

Con fecha 16 de abril de 2024 se recibe en esta Agencia escrito de respuesta indicando lo siguiente:

"*El 2 de marzo, solicitó la baja, con fecha de efecto del 14 de marzo por motivos de traslado de trabajo. (...).*

Nuestro personal le indica que la huella no va a ser almacenado ni objeto de tratamiento alguno por nuestra parte y que, por tanto, es imposible que ningún hacker robe algo que no existe.

Le indicamos que la huella será introducida en una tarjeta que llevará consigo el propio usuario, con el único fin de que se realice una doble verificación en el acceso, comprobando que el/la usuario/a que accede a las instalaciones es quien se encuentra matriculado/a, con el fin de garantizar que la tarjeta sea intransferible.

No obstante, (...), el reclamante no acabó de comprender la diferencia entre almacenar el dato biométrico en nuestros sistemas y hacerlo en una tarjeta que estaría en su posesión en todo momento.

*El sistema implantado por nuestra empresa con el fin de garantizar la seguridad de las instalaciones y de sus usuarios/as, evitando que pueda producirse un acceso incontrolado a la misma, creemos que cumple con la idoneidad necesaria, garantizando la finalidad de identificación/seguridad que se persigue al cruzar los datos de la huella dactilar leída al ponerse el dedo sobre el lector, con los portados en la tarjeta por el/la propio/a usuario/a. De hecho, dicho sistema es el que la propia Agencia Española de Protección de Datos sugiere en su Procedimiento Nº ***REFERENCIA.1 al recomendar a una empresa con idéntica actividad a la desarrollada por la nuestra, que los datos biométricos sean guardados en una tarjeta que portara el/la socio/a consiguiendo así que el tratamiento resulte menos excesivo, figurando en poder del propio socio o socia el sistema de autenticación completo*".

TERCERO: Con fecha 19 de junio de 2024, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada.

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 VIII, de la LOPDGDD.

Como consecuencia de las actuaciones realizadas, se ha tenido conocimiento de los siguientes extremos:

PUNTO 1. Con fecha 1 de octubre de 2024, **MACROFIT CANARIAS, S.L.** facilitó a esta Agencia la siguiente información en relación con las técnicas empleadas y la descripción del sistema utilizado:

a) Descripción del sistema utilizado, incluyendo detalle sobre los datos personales que se tratan (tales como, código identificativo del usuario, fecha y hora de entrada/salida, plantilla biométrica de la huella, imagen, etc.):

Manifestaban utilizar un software concreto de gestión de instalaciones deportivas, de una empresa española que da servicios a muchos centros deportivos. Se trata de una

base de datos que crea fichas de los clientes en las que se registran datos por pestañas, entre ella la de los accesos:
1. Persona. - Se indican los datos del cliente anotándose nombre y apellidos, fecha de nacimiento y DNI. - Igualmente, se refleja en esta pestaña, la fecha del alta.
2. Dirección. - Indicación del municipio, calle y número, además de número de teléfono y correo electrónico.
3. Económico. - Se registra la cuenta bancaria para la realización de los pagos.
4. Perfiles. - Pestaña para anotación del tipo de perfil de cliente al que pertenece (en algunas instalaciones hay que diferenciar si es familiar, trabajador o cualquier otro perfil que tenga alguna diferenciación especial).
5. Datos. - Solo se indica el ID de la persona, esto es, el número interno que el programa asigna a cada cliente.
6. Abono. - Datos del abono que tiene contratado, si corresponde y pantalla para asignar abonos a los clientes.
7. Cursillo. - Pantalla que indica el cursillo al que está inscrito el cliente y pestaña en el que gestionar altas y bajas de cursillos.
8. Servicios. - Si se requiere, indicación de otros servicios que ha contratado el cliente y zona donde gestionarlo (alquiler de taquilla, entrenamiento personal).
9. Reservas. - Sin uso en las instalaciones de MACRO FIT, sirve para gestionar alquileres de espacios.
10. Pagos. - Se refleja el histórico de pagos y desde donde se emiten facturas.
11. Accesos. - Pestaña que registra los accesos de los clientes y desde la que, si procede, se limita entradas.
12. Notas. - Espacio destinado a anotar cualquier aspecto que se quiera comunicar al cliente.
Indican que además de estos datos personales, el software permite definir los parámetros para gestionar los accesos a través de los tornos (horarios de entrada y salida, bien general o específicos en el caso de los cursillos).

b) Debido a que en el procedimiento de admisión a trámite indicaron que el sistema utiliza una tarjeta de usuario (entendiendo que el sistema la lee a la vez que reconoce la huella en el momento del acceso), se requirió información sobre si la autenticación/identificación del usuario se realiza 1 a 1, o bien 1 a N:

Manifestaron que 1 a 1 es la opción correcta (comparando las características de la huella capturada en el momento del fichaje, solo con la propia del usuario previamente almacenada en la tarjeta del usuario), ya que la huella es únicamente portada por el propio usuario en la tarjeta, llevando el usuario, en el dispositivo de acceso (tarjeta, pulsera o llavero), el sistema completo de autenticación.

c) Sobre los lugares de almacenamiento de las imágenes y las plantillas biométricas generadas a partir de las imágenes (servidor, lector, tarjeta, etc.).

Manifestaron que, como ya indicaron en el escrito de abril, la huella o algoritmo únicamente se graba en la tarjeta que se entrega al usuario en el momento del alta, no quedando almacenada en lector, servidor ni en ningún otro dispositivo ni base de datos en la nube.

d) Sobre los plazos de conservación de las imágenes y las plantillas biométricas (tanto de los obtenidos del proceso de registro de un nuevo usuario, como los recogidos en

el momento de los accesos a los centros, tanto si la autenticación resulta positiva como negativa).

No se almacenan ni en el proceso de registro ni en el de acceso. El sistema simplemente comprueba que los datos contenidos en la tarjeta coinciden con la huella real del usuario con el fin de asegurar el acceso en exclusiva, al propietario del dispositivo.

e) Sobre la baja de los datos del sistema, y cómo se produce el borrado del sistema de los datos personales cuando un usuario que se da de baja, incluidos los biométricos. Se ha requerido aportar acreditación documental del borrado de datos del reclamante.

Manifestaron que cuando un usuario se da de baja, se eliminan los datos almacenados en su ficha y que como el sistema no permite borrar el código identificativo (generado por la aplicación (que no es el DNI o similar), queda únicamente este código residual que ya no será asignado a otro usuario. Indican que tras realizar una búsqueda del usuario con los apellidos del reclamante se puede comprobar en el pantallazo adjunto que aparecen dos registros. Uno vacío que corresponde al usuario afectado y otro que corresponde a una usuaria con apellidos coincidentes. Por tanto, el único dato que permanece tras la baja es el antiguo código de usuario, manifestando los representantes de la parte reclamada que no representa un dato de carácter personal al no identificar al usuario de modo alguno (ANEXO 1, resultado de la búsqueda en toda la base de datos de los clientes con los apellidos del reclamante).

Aportan impresión de pantalla con dos ventanas de la aplicación superpuestas comprobándose que en una de ellas aparece una ficha de cliente con el nombre y apellidos del reclamante asociado a un código identificativo, en la cabecera de la ventana. En el cuerpo de la ventana, a pesar de que algunos campos de esta ventana se encuentran tapados por otra ventana superpuesta, no se aprecian más campos con contenido, salvo la fecha de baja 01/10/2024, el sexo (hombre), la dirección de correo electrónico y el centro. La otra ventana superpuesta a la anterior consiste en una búsqueda solo por los apellidos del reclamante. En los resultados de esta búsqueda aparece otra socia del centro con los mismos apellidos y otro nombre, así como con otro código identificativo.

Dado que ello parecía contradecir las manifestaciones de la parte reclamada, que ha manifestado que cuando un usuario se da de baja solo persiste su código identificativo, y considerando además que la búsqueda se ha realizado por apellidos y aparece el reclamante como resultado, parece claro que los apellidos se conservan, no siendo posible que solo se conserve el código de usuario. Por tanto, se realizó un requerimiento de información adicional solicitando a la parte reclamada aclaración sobre qué datos se conservan después de la baja de un cliente. Se ha requerido aportar impresión acreditativa de ello, LUDE aportó en fecha 18 de agosto de 2025 impresión con todos los datos que se conservan del reclamante. Ante ello han indicado lo siguiente:

“Se aclara que la baja del reclamante fue una baja rutinaria derivada de la finalización de su relación contractual con el centro deportivo, y no el ejercicio del derecho de supresión previsto en el artículo 17 del Reglamento (UE) 2016/679 (RGPD).

En estos supuestos, y conforme al principio de limitación del plazo de conservación (art. 5.1.e RGPD), la práctica habitual es conservar datos mínimos de contacto (a los que sólo tiene acceso determinado personal) durante un plazo máximo de 12 meses desde la fecha de baja, exclusivamente para:
• Atender posibles reclamaciones contractuales.
• Contactar con el usuario ante posibles devoluciones o incidencias bancarias derivadas de pagos domiciliados.

Además, en el presente caso, debido a que una parte de los gimnasios que operaban bajo la marca MACRO FIT cambiaron de titularidad, se llevó a cabo un proceso extraordinario de depuración de bases de datos antes de la transmisión del control, procediendo a la eliminación de todos los registros de usuarios dados de baja con independencia de la fecha de dicha baja.

Como consecuencia de esta depuración se han eliminado los datos del reclamante, así como los de la otra usuaria cuyos apellidos coincidían parcialmente."

Adjuntaban captura de pantalla en la que se observa una búsqueda realizada por los apellidos del reclamante, constatándose que el sistema arroja como resultado "No hay ninguna persona".

PUNTO 2. Sobre los centros deportivos de la cadena que utilizan el sistema y fechas de implementación. Entidades intervinientes en el tratamiento de datos con indicación del cometido de cada una, y del conjunto de datos que tiene acceso. Posibles destinatarios de los datos del sistema de control de acceso. Se solicitó incluir la descripción de los tratamientos efectuados por LUDE GESTIONES Y SERVICIOS, S.L., MACROFIT CANARIAS, S.L., ***EMPRESA.1 Y ***EMPRESA.2 Ante ello, MACROFIT CANARIAS, S.L con fecha 2 de octubre de 2024 manifestó lo siguiente:

*"Cabe destacar que todos los gimnasios que operaban bajo la marca MACRO FIT, han sido vendidos al ***EMPRESA.3 a través de la compra de la mercantil ***EMPRESA.1. empresa que operaba dos de los centros y que, tras un proceso de reorganización, pasó a ser propietario de la totalidad de la gestión de los centros.*

*Por lo tanto, desde el pasado 26 de julio del presente 2024, todos los gimnasios MACRO FIT pertenecen a la sociedad ***EMPRESA.1 que a su vez pertenece a* ******EMPRESA.3***.

Igualmente, hay que reseñar que, si bien la reclamación que nos ocupa, interpuesta por […el reclamante…], se dirigió a la empresa MACRO FIT CANARIAS S.L., con CIF B76175355, esta empresa solo gestionaba un centro, el gimnasio MACRO FIT VECINDARIO.

Por otro lado, la nueva propietaria de MACRO FIT, va a integrar, en los próximos meses, los centros adquiridos en Canarias, a su red de gimnasios por lo que pasarán a operar bajo la marca ******EMPRESA.3*** *lo que supone que adapte todos los procedimientos de trabajo entre los que están el cambio de software de gestión y cambio de procesos de acceso que pasarán a realizarse mediante código QR que se generará a través de la APP en el teléfono del cliente minutos antes de acceder al*

centro deportivo, por lo que no usarán la huella ni ningún otro dispositivo de acceso específico.

No obstante, y tras la aclaración, las empresas que operaban centros con la marca MACRO FIT eran las siguientes:

*- ***EMPRESA.2*
o MACRO FIT CASTILLO. - Desde octubre de 2013 y hasta julio de 2024.
o MACRO FIT ARRECIFE. - Desde abril de 2017 y hasta mayo de 2024.
o MACRO FIT LA LAGUNA. - Desde diciembre de 2019 y hasta mayo de 2024

- LUDE GESTIONES Y SERVICIOS S.L.
o MACRO FIT LA BALLENA. - Desde enero de 2017 y hasta marzo de 2024
o MACRO FIT PUERTO DEL ROSARIO. - Desde 2019 y hasta la actualidad (este centro, al estar en una instalación privada, no se incluyó en la operación de venta).
*o MACRO FIT ***CENTRO.1. – (…)*

*- ***EMPRESA.1*
o MACRO FIT LAS PALMAS. - Desde febrero de 2015.
o MACRO FIT ALISIOS. - Desde febrero de 2019.
o TODOS LOS CENTROS (excepto MACRO FIT PUERTO DEL ROSARIO), desde julio de 2024.

- MACRO FIT CANARIAS S.L.
o MACRO FIT VECINDARO. - Desde diciembre de 2014 y hasta julio de 2024

Desde octubre de 2015, todos los centros, tras los numerosos problemas de seguridad, implantaron el sistema de control por doble factor (dispositivo y huella). En aquel momento, existían 3 centros que operaban bajo la marca MACRO FIT.

La base de datos de los diferentes gimnasios es única, ya que los clientes de un MACRO FIT, lo son de todos y, a pesar de estar separados por tipo de cuota según la instalación a la que se inscriben, como pueden acceder a cualquier centro de la cadena, se requiere una única base de datos.

Los destinatarios de los datos del sistema de control de acceso, solo son los trabajadores de las diferentes empresas con permisos para trabajar con el software […]"

Se hace notar que el reclamante ha sido cliente del centro *MACRO FIT ***CENTRO.1*, gestionado por la entidad LUDE, si bien todas las entidades son responsables del tratamiento ya que los usuarios podían ir a cualquiera de los centros deportivos de MACRO FIT, operados varias entidades.

El centro *MACRO FIT ***CENTRO.1*, operado por LUDE GESTIONES Y SERVICIOS SL (operó hasta marzo de 2024) fue vendido a ***EMPRESA.3** a través de ***EMPRESA.1.

Dado que han declarado que *"todos los gimnasios que operaban bajo la marca MACRO FIT, han sido vendidos al ***EMPRESA.3*" y sin embargo indican sobre

MACRO FIT Puerto del Rosario que este centro no se incluyó en la operación de venta, se ha requerido en un nuevo requerimiento aportar información sobre la situación actual del centro MACRO FIT Puerto del Rosario, y si la entidad que lo opera sigue siendo LUDE GESTIONES Y SERVICIOS, SL, así como sobre si este centro sigue utilizando control de acceso por huella dactilar.

Ante ello, la parte reclamada ha manifestado que el centro *MACRO FIT* Puerto del Rosario no ha sido vendido, y está gestionado por LUDE GESTIONES Y SERVICIOS, S.L. Este centro mantiene el sistema de control de acceso mediante huella dactilar en combinación con dispositivo físico. Indican que este sistema cumple con el criterio de proporcionalidad indicado por la propia Agencia Española de Protección de Datos en el Procedimiento Sancionador ******REFERENCIA.1***, al almacenar el patrón biométrico exclusivamente en un dispositivo bajo control del usuario, sin que la entidad conserve dicho dato en sus sistemas.

No obstante, indican que se ha establecido la fecha 1 de octubre de 2025 para la sustitución definitiva de este sistema por un método de acceso mediante código QR dinámico generado en la aplicación móvil del cliente, cesando a partir de esa fecha el uso del control de acceso por huella dactilar. Indican que el nuevo sistema debería haber estado en funcionamiento en junio de 2025 pero que, por motivos de configuración, se ha retrasado su implantación.

Se comprobó que adjuntaron una factura del proveedor del nuevo sistema, de fecha 31 de enero de 2025, factura a nombre de LUDE GESTIONES Y SERVICIOS SLU, donde se aprecia la existencia de seis lectores de códigos QR entre otros dispositivos que componen el sistema de control de acceso.

Se comprobó que la inscripción en los gimnasios ******EMPRESA.3*** implica como primer paso la descarga de una app propia, que entre otras funcionalidades permite la identificación de los socios con un código QR, según la información obrante en la página web de la marca.

PUNTO 3. Sobre el número de usuarios total que utilizan el sistema y el número de usuarios que han mostrado su rechazo al sistema con huella dactilar, y si se les ha ofrecido alguna otra opción distinta para el acceso, MACROFIT CANARIAS, S.L., con fecha 2 de octubre de 2024, manifestó:

"El número de clientes varía por meses, si bien, la media supera los 20.000 clientes, aunque estimamos más de 120.000 personas diferentes en los más de 10 años desde la creación de los gimnasios que operan bajo la marca MACRO FIT.

Solo se han tenido dos reclamaciones. La primera, en noviembre del pasado año 2023, en la que una señora, que fue a informarse, interpuso reclamación ante la AEPD que no fue admitida a trámite (EXP202317369), además de la que nos ocupa, interpuesta por el actual reclamante.

Consideramos que ambos lo han hecho desde el desconocimiento de la normativa aplicable y de procedimientos llevados a cabo por esa agencia como el ******REFERENCIA.1*** *en el que recomienda a una entidad con idéntica actividad a la desarrollada por la nuestra, que los datos biométricos sean guardados en una tarjeta*

que portara el/la socio/a, figurando en su poder el sistema de autenticación completo sin que los datos sean almacenados por la empresa.

No se les ha ofrecido alternativa dado que el sistema actual no lo admite y en base al procedimiento mencionado considerábamos que se estaba realizando de manera correcta y acorde a la normativa actual."

PUNTO 4. Sobre la base legal (legitimación) para el tratamiento de datos biométricos (imágenes y/o plantillas biométricas), MACROFIT CANARIAS, S.L., con fecha 2 de octubre de 2024, manifestó:

"La base legal es el consentimiento del usuario, partiendo de que el cliente da su consentimiento únicamente a la grabación de su huella en una tarjeta o dispositivo similar, que se le entrega en el acto, no a su almacenamiento que no se da en ningún dispositivo propiedad de la empresa (ni en otra base de datos en la nube)."

PUNTO 5. Copia de toda la información facilitada a los usuarios con respecto al sistema. Copia de todas las comunicaciones o informaciones sobre protección de datos facilitadas al respecto, método de envío/puesta en conocimiento de los usuarios y su fecha.

MACROFIT CANARIAS, S.L., con fecha 2 de octubre de 2024, adjuntó la información/normativa que se entregaba a los usuarios requiriendo de su firma en el momento de registro en los centros en el ANEXO 2, donde consta que para formalizar la inscripción *"…Se realizará un registro de la huella dactilar para grabarla en la tarjeta, pulsera o llavero que debe adquirir el cliente y que les permitirá el acceso al centro de forma segura. La huella no quedará guardada en ningún archivo ni base de datos de la empresa y solo se vinculará con su dispositivo (tarjeta, pulsera o llavero)."*

Se informaba sobre protección de datos lo siguiente: *"Las diversas sociedades que gestionan gimnasios de la marca MACRO FIT (Lude Gestiones y Servicios, S.L., Macrofit Canarias, S.L, ***EMPRESA.1 y ***EMPRESA.2) son los Responsables del tratamiento de los datos personales del Interesado y le informa que estos datos serán tratados de conformidad con lo dispuesto en el Reglamento (UE) 2016/679 de 27 de abril (GDPR) y la Ley Orgánica 3/2018 de 5 de diciembre (LOPDGDD), por lo que se le facilita la siguiente información del tratamiento. Fin del tratamiento: mantener una relación comercial en base a un interés legítimo por parte del responsable y/o la celebración de un contrato con el usuario. Criterios de conservación de los datos: se conservarán durante no más tiempo del necesario para mantener el fin del tratamiento y cuando y cuando ya no sea necesario para tal fin, se suprimirán con medidas de seguridad adecuadas para garantizar la seudonimización de los datos o la destrucción total de los mismos. Comunicación de los datos: No se comunicarán datos a terceros salvo obligación legal (salvo aquellas cesiones necesarias entre las empresas del grupo mencionadas en la presente cláusula). Derechos que asisten al Interesado: Derecho a retirar el consentimiento en cualquier momento. Derecho de acceso, rectificación, portabilidad y supresión de sus datos y a la limitación u oposición a su tratamiento. Derecho a presentar una reclamación ante la Autoridad de control (www.aepd.es) si considera que el tratamiento no se ajusta a la normativa vigente.*

Datos de contacto para ejercer sus derechos: Lude Gestiones y Servicios, S.L. Macro Fit […]"

PUNTO 6. Sobre si se ha realizado previamente una Evaluación de Impacto relativa a la Protección de Datos (EIPD) con Análisis de Proporcionalidad (triple análisis de idoneidad, necesidad y proporcionalidad) o un estudio previo similar, MACROFIT CANARIAS, S.L., con fecha 2 de octubre de 2024, manifestó lo siguiente:

"*El artículo 35.3 del RGPD establece que la EIPD se requerirá en particular en el caso de:*

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;

b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10;

c) observación sistemática a gran escala de una zona de acceso público.

Consideramos que no se dan ninguna de las 3 situaciones. Respecto al apartado b), insistimos en que no tratamos categorías especiales de datos a gran escala más allá de la grabación de la huella del usuario en una tarjeta, llavero o pulsera, que le entregamos inmediatamente tras su grabación. Por otro lado, respecto a la lista de criterios publicada por la AEPD para decidir si realizar una EIPD, se han analizado los mismos cuidadosamente no cumpliéndose dos criterios de los mismos (como mínimo) que indicasen la idoneidad de realizar dicha Evaluación."

PUNTO 7. Sobre las medidas de seguridad y garantías específicas para el tratamiento de datos biométricos, MACROFIT CANARIAS, S.L., con fecha 2 de octubre de 2024, manifestó lo siguiente:

- Sobre si se utiliza cifrado para los datos biométricos almacenados, tanto en el sistema como en la tarjeta del usuario:

Indicaron que no se almacenan datos biométricos en el sistema y solo se guarda en la tarjeta o dispositivo similar del usuario.

Indicaron en el ANEXO 3 que el lector que utilizan, de una marca determinada que aportan, tiene sensores/lectores de huellas, con características para extraer un código único sin que sea posible extraerlo:

> *"Este lector realiza un escaneo del dedo que es convertido a una trama de datos hexadecimal extraída a través de un algoritmo matemático propietario de […] basado en unos puntos que poseen unas características concretas denominadas minucias (posición, relación entre puntos, distancia y dirección). Esta trama*

permite verificar la identidad del usuario cada vez que realiza un acceso y se almacena en la tarjeta/pulsera del usuario. En ningún caso este dispositivo ni ninguna base de datos almacena dicha trama ni información alguna sobre la huella."

- Sobre el formato de datos o tecnologías específicas utilizadas, que imposibiliten la interconexión con otras bases de datos biométricos:

Indicaron que el lector escanea el dedo y lo convierte en una trama de datos hexadecimales extraída a través de un algoritmo matemático propiedad de la compañía del lector, basado en puntos que tienen unas características específicas llamada minucias.

Esta trama es la que permite verificar la identidad del usuario sin que sea posible extraerla en caso de pérdida del dispositivo de acceso, que es donde se guardan los datos de la huella.

- Sobre los medios técnicos implementados para asegurar la imposibilidad de utilizar los datos biométricos de los usuarios para cualquier otro propósito.

Indicaron que no se pueden utilizar los datos biométricos de los usuarios con ningún otro propósito ya que no disponemos de ellos y, tan solo el cliente, con su dispositivo de acceso, tiene el registro biométrico. Como hemos manifestado reiteradamente, el sistema no almacena dichos datos.

- Sobre la posibilidad de revocar el vínculo de identidad entre la plantilla biométrica y la persona física.

Indicaron que la destrucción de la tarjeta o el borrado de la misma desvincula el código que guarda el dato biométrico.

- Sobre si existen mecanismos automatizados de supresión de los datos biométricos.

Indicaron que, al almacenar los datos exclusivamente en la tarjeta, pulsera o llavero del cliente, no hay mecanismos automatizados de supresión de los datos y que la baja del cliente y la eliminación de datos de la ficha, desvinculan el código de la tarjeta de acceso y el lector no podrá leerlo, quedando un dato inutilizado.

- Sobre la aplicación de los principios de protección de datos desde el diseño, y minimización de los datos manifestaron que:

"El principio de minimización se cumple holgadamente ya que únicamente se almacena la huella en la tarjeta que queda en posesión del usuario.

Se hace por cuestiones de seguridad para evitar que dicha tarjeta pueda ser transferible y evitar el acceso a las instalaciones de personas que no estén registradas como usuarios de las mismas.

Respecto al resto de tratamientos (NO BIOMÉTRICOS), dichos principios han sido aplicados ya que nuestra entidad ha mantenido desde el inicio de su

actividad una actitud proactiva con respecto a la protección de datos. Únicamente tratamos los datos necesarios para la finalidad para la cual se recaban, trabajando con proveedores informáticos que ofrezcan garantías de seguridad, asegurando la disponibilidad e integridad de la información.

No solamente cumplimos escrupulosamente con el principio de minimización de datos, sino que ostentamos la condición de "supervisores" de los usuarios que acceden a nuestros centros, informándoles respecto a determinadas prácticas que no deben llevarse a cabo, tanto verbalmente como mediante carteles a tal efecto (evitar sacar fotos o grabar vídeos donde aparezcan otros usuarios, etc.).

El servicio de protección de datos fue integrado desde el inicio de la actividad, contando en todo momento con una empresa que nos ha acompañado a lo largo de estos años. Todos nuestros usuarios pueden conocer en cualquier momento el tratamiento que damos a sus datos, como ejercer sus derechos respecto a los mismos. En definitiva, todos los procesos llevados a cabo por nuestra entidad sin respetuosos con la privacidad. "

- Sobre la existencia de intervención humana en caso de error.

Indicaron que la única intervención humana es la necesaria para grabar la huella en la tarjeta del cliente que se hace accediendo a su ficha y vinculándola con la tarjeta, pulsera o llavero y que el error en el grabado de la huella ocasiona la imposibilidad del cliente de acceder al gimnasio, ya que el lector del torno no podrá vincular la huella con la tarjeta.

- Sobre si se basa en la utilización de dispositivos bajo el control exclusivo de los usuarios.

Indicaron que el único dispositivo (la tarjeta, llavero o pulsera) donde se almacenan datos biométricos, está efectivamente en posesión del usuario.

- Sobre otras garantías que hayan sido adoptadas en su caso.

Indicaron que una vez que el cliente causa baja, la eliminación de los datos de la ficha inutiliza el dispositivo de acceso donde se guarda la huella.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, la entidad LUDE es una empresa constituida en el año 2004, y con un volumen de negocios de 11.408.278 euros en el año 2023.

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 de la Ley

Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Presidencia de la Agencia Española de Protección de Datos.

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

II

Tratamiento de categorías especiales de datos personales

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente:

"1. 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;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

Los datos biométricos son una categoría especial de datos. Las Directrices 5/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público (Versión 2.0, de 26 de abril de 2023), determinan, en su apartado 12, que el concepto de dato biométrico incluye

tanto la autenticación como la identificación, y que, si bien son conceptos distintos, ambos implican el tratamiento de datos dirigidos a identificar a una persona física, por lo que constituyen tratamientos de categorías especiales conforme al artículo 9 del RGPD.

La posición mantenida por el CEPD fue acogida posteriormente por esta Agencia. Ahora bien, la AEPD considera, tal y como se recoge en la respuesta a la solicitud de consulta previa sobre la adecuación y proporcionalidad de sistemas biométricos para la autenticación de 18 de julio de 2025, que no todos los tratamientos biométricos tienen la misma intensidad de impacto, ni requieren idénticas medidas de protección, así señala que "*la identificación biométrica consiste en determinar la identidad de una persona comparando sus datos biométricos (por ejemplo, una huella dactilar o un patrón facial) con los datos de un conjunto amplio de personas almacenadas en una base de datos. Es decir, responde a la pregunta: ¿quién eres tú entre todos los posibles? Se trata de una operación uno-a-varios (1:N), y su principal implicación desde el punto de vista de la protección de datos es que implica una búsqueda activa dentro de un conjunto de identidades preexistentes, lo cual comporta mayores riesgos para los derechos fundamentales, especialmente en contextos de vigilancia masiva, control social o de seguridad. En cambio, la autenticación biométrica se basa en confirmar que una persona es quien dice ser, comparando sus datos biométricos con una plantilla única previamente vinculada a su identidad. Es una operación uno-a-uno (1:1), que responde a la pregunta: ¿eres tú realmente esta persona concreta? Suele utilizarse en el acceso a dispositivos o servicios*."

En consecuencia, el impacto de uno u otro tratamiento no es el mismo y en este sentido la AEPD ha declarado que "*en el contexto de la normativa de protección de datos que aquí interesa, sin perjuicio de que nos encontramos ante datos especialmente protegidos del artículo 9, no todos los tratamientos basados en el artículo 9 del RGPD comportan el mismo nivel de riesgo ni exigen el mismo grado de salvaguardas. Desde una perspectiva de la legalidad y, especialmente de la proporcionalidad y evaluación de riesgos, la identificación (1:N) suele presentar mayores riesgos para los derechos y libertades fundamentales, en especial por su carácter invasivo y su tendencia a extenderse sin control en el caso de la identificación remota. En cambio, la autenticación biométrica localizada, bien diseñada y según toda una serie de circunstancias a tener en cuenta en cada caso concreto, puede ser en muchos contextos más proporcionada y menos intrusiva, especialmente si existe regulación o consentimiento libre e informado y garantías adecuadas.*

Por tanto, aunque desde el plano formal ambos usos pueden estar incluidos en el artículo 9 del RGPD, el impacto real sobre los derechos y la intensidad de las medidas de protección requeridas pueden variar sustancialmente, debiendo valorarse caso por caso en función del contexto, la escala, la tecnología empleada y el control efectivo que conserve el interesado sobre sus datos biométricos".

III
Información que deberá facilitarse cuando los datos personales se obtengan del interesado

El artículo 13 del RGPD establece la información que deberá facilitarse cuando los datos personales se obtengan del interesado, en virtud del cual:

"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 fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.

2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;
d) el derecho a presentar una reclamación ante una autoridad de control;
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de 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.

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."

IV
Evaluación de impacto relativa a la protección de datos

La evaluación de impacto relativa a la protección de datos se regula en el artículo 35 del RGPD en los siguientes términos:

"1. Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:
a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar;
b) tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o
c) observación sistemática a gran escala de una zona de acceso público.

4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

7. La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

8. El cumplimiento de los códigos de conducta aprobados a que se refiere el artículo 40 por los responsables o encargados correspondientes se tendrá debidamente en cuenta al evaluar las repercusiones de las operaciones de tratamiento realizadas por dichos responsables o encargados, en particular a efectos de la evaluación de impacto relativa a la protección de datos.

9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.

10. Cuando el tratamiento de conformidad con el artículo 6, apartado 1, letras c) o e), tenga su base jurídica en el Derecho de la Unión o en el Derecho del Estado miembro que se aplique al responsable del tratamiento, tal Derecho regule la operación específica de tratamiento o conjunto de operaciones en cuestión, y ya se haya realizado una evaluación de impacto relativa a la protección de datos como parte de una evaluación de impacto general en el contexto de la adopción de dicha base jurídica, los apartados 1 a 7 no serán de aplicación excepto si los Estados miembros consideran necesario proceder a dicha evaluación previa a las actividades de tratamiento.

11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento."

V
Minimización de datos

La letra c) del artículo 5.1 del RGPD propugna:

"1. Los datos personales serán:
(…)
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);"

VI
Conclusión

La reciente STJUE de 24 de septiembre de 2024, en el asunto C-768/2021, señala (el subrayado es de la AEPD):

"37 A este respecto, ha de señalarse que el RGPD deja a la autoridad de control un margen de apreciación en cuanto a la manera en que debe subsanar la deficiencia constatada, puesto que el artículo 58, apartado 2, del mismo confiere a dicha autoridad la facultad de adoptar diversas medidas correctoras. Así, el Tribunal de Justicia ya ha declarado que la elección del medio adecuado y necesario corresponde a la autoridad de control, que debe realizar tal elección tomando en consideración todas las circunstancias del caso concreto y cumpliendo con toda la diligencia requerida su misión consistente en velar por el pleno respeto del RGPD (véase, en este sentido, la sentencia de 16 de julio de 2020, Facebook Ireland y Schrems, C-311/18, EU:C:2020:559, apartado 112).
38 Sin embargo, este margen de apreciación está limitado por la necesidad de garantizar un nivel coherente y elevado de protección de los datos personales mediante una aplicación rigurosa de las normas, como se desprende de los considerandos 7 y 10 del RGPD
…
41 En consecuencia, no puede deducirse ni del artículo 58, apartado 2, del RGPD ni del artículo 83 de este la existencia de una obligación a cargo de la autoridad de control de adoptar, en todos los casos, cuando constate una violación de la seguridad de datos personales, una medida correctora, en particular una multa administrativa, siendo su obligación, en tales circunstancias, reaccionar adecuadamente para subsanar la deficiencia constatada. (…) En estas circunstancias, como señaló el Abogado General en el punto 81 de sus conclusiones, el autor de una reclamación cuyos derechos han sido vulnerados no dispone de un derecho subjetivo a que la autoridad de control imponga una multa administrativa al responsable del tratamiento.
(…)
43 A este respecto, no se excluye que, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, la autoridad de control pueda abstenerse de adoptar una medida correctora aunque se haya constatado una violación de la seguridad de datos personales. Tal puede ser el caso, en particular, cuando la violación constatada no haya persistido, por ejemplo cuando el responsable del tratamiento, que, en principio, había aplicado medidas técnicas y organizativas apropiadas en el sentido del artículo 24 del RGPD, haya adoptado, tan pronto como haya tenido conocimiento de dicha violación, las medidas adecuadas y necesarias para que la violación finalice y no vuelva a producirse, habida cuenta de las obligaciones que le incumben, en particular, en virtud de los artículos 5, apartado 2, y 24 del mencionado Reglamento.
44 La interpretación según la cual la autoridad de control, cuando constata una violación de la seguridad de datos personales, no está obligada a adoptar en todos los casos una medida correctora con arreglo al artículo 58, apartado 2, del RGPD se ve corroborada por los objetivos perseguidos por este artículo 58, apartado 2, y por el artículo 83 de dicho Reglamento, respectivamente.
45 Por lo que respecta al objetivo perseguido por el artículo 58, apartado 2, del RGPD, del considerando 129 de este se desprende que esta disposición tiene por objeto garantizar la conformidad del tratamiento de datos personales con dicho

Reglamento y la regularización de las situaciones de incumplimiento de este para que se ajusten al Derecho de la Unión, mediante la intervención de las autoridades de control nacionales (sentencia de 14 de marzo de 2024, Újpesti Polgármesteri Hivatal, C-46/23, EU:C:2024:239, apartado 40).
46 De lo anterior se infiere que la adopción de una medida correctora puede, con carácter excepcional y habida cuenta de las circunstancias particulares del caso concreto, no imponerse, siempre que la situación de infracción del RGPD ya haya sido subsanada y que se garantice la conformidad de los tratamientos de datos personales con dicho Reglamento por su responsable y que tal abstención de la autoridad de control no menoscabe la exigencia de una aplicación rigurosa de las normas, tal como se ha recordado en el apartado 38 de la presente sentencia.".

El TJUE incide, por tanto, en el margen de apreciación que tienen las autoridades de control para, en el ejercicio de sus funciones, desarrollar y optar entre los poderes atribuidos por el artículo 58 del RGPD, teniendo en cuenta las circunstancias del caso concreto, así como velando por el pleno respeto del RGPD. La consigna que debe regir siempre la actuación de una autoridad de control es asegurar un nivel alto de protección de los datos personales.

Así, cabe que, aun cuando se hubiera constatado o se tuvieran indicios de que se ha producido una vulneración en materia de protección de datos, las autoridades de control se abstengan de ejercitar sus poderes correctivos cuando esta presunta infracción hubiera sido subsanada y se garantice la conformidad de los tratamientos de datos personales con el RGPD.

Lo señalado por el TJUE en la sentencia antes citada, refuerza la idea de proporcionalidad de actuación de las autoridades de control que se recoge, con anterioridad a que fuera dictada la mencionada sentencia, en los artículos 65.4 y 65.6 de la LOPDGDD, por los que se permite a la AEPD, en atención a las circunstancias del caso concreto, la inadmisión a trámite o el archivo de reclamaciones, cuando, tras el traslado de las mismas al responsable del tratamiento, este demostrara haber adoptado medidas para el cumplimiento de la normativa aplicable.

En el presente caso, los hechos que impulsaron el inicio de actuaciones previas de investigación conforme al artículo 67 de la LOPDGDD -tras la recepción de una reclamación por la AEPD- se referían a la utilización por las reclamadas de un sistema de autenticación biométrica de acceso a las instalaciones deportivas de las que es responsable basado en el uso de la huella digital de sus socios.

Durante las actuaciones previas de investigación se ha comprobado que, efectivamente, las reclamadas contaban, desde el año 2015, con el mencionado sistema:

> *"Desde octubre de 2015, todos los centros, tras los numerosos problemas de seguridad, implantaron el sistema de control por doble factor (dispositivo y huella). En aquel momento, existían 3 centros que operaban bajo la marca MACRO FIT."*

No obstante, desde principios de 2025 se han iniciado actuaciones para proceder a la sustitución de este sistema por un método de acceso mediante código QR dinámico generado en la aplicación móvil del cliente, cesando a partir de esa fecha el uso del control de acceso por huella dactilar. Indican que el nuevo sistema debería haber estado en funcionamiento en junio de 2025 pero que, por motivos de configuración, se ha retrasado su implantación:

> *"Por otro lado, la nueva propietaria de MACRO FIT, va a integrar, en los próximos meses, los centros adquiridos en Canarias, a su red de gimnasios por lo que pasarán a operar bajo la marca* ******EMPRESA.3*** *lo que supone que adapte todos los procedimientos de trabajo entre los que están el cambio de software de gestión y cambio de procesos de acceso que pasarán a realizarse mediante código QR que se generará a través de la APP en el teléfono del cliente minutos antes de acceder al centro deportivo, por lo que no usarán la huella ni ningún otro dispositivo de acceso específico."*

Así, ha sido aportada a este expediente una factura del proveedor del nuevo sistema, de fecha 31 de enero de 2025, factura a nombre de LUDE GESTIONES Y SERVICIOS SLU, donde se aprecia la existencia de seis lectores de códigos QR entre otros dispositivos que componen el sistema de control de acceso.

Esto pone de manifiesto la diligencia con la que el responsable del tratamiento actuó al conocer el posicionamiento de la AEPD sobre los sistemas de autenticación biométrica y que el sistema por él elegido podía vulnerar la normativa en materia de protección de datos, respondiendo adecuadamente, en esencia, al principio de responsabilidad proactiva, elemento vertebrador del RGPD previsto en su artículo 5.2 y desarrollado en el artículo 24 de la misma norma.

En consecuencia, de conformidad con la STJUE de 24 de septiembre de 2024, en el asunto C-768/2021 y atendiendo a las singulares circunstancias que conforman este caso, en particular, la especial diligencia del responsable para asegurar el cumplimiento de la normativa de protección de datos, así como la desaparición del sistema de acceso objeto de investigación, esta Agencia considera que no procede el despliegue de sus poderes correctivos previstos en el artículo 58 del RGPD.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Por lo tanto, de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos
SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a LUDE GESTIONES Y SERVICIOS, S.L. y MACROFIT CANARIAS, S.L. y a la parte reclamante.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la Presidencia de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-Administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

940-101025

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos