- **Expediente N.º: EXP202313347**

Procedimiento Sancionador Nº. PS/00289/2024

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR RECONOCIMIENTO DE RESPONSABILIDAD Y PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 1 de mayo de 2025, la Presidencia de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***SIDECU, S.A.*** (en adelante, ***SIDECU***), mediante el acuerdo que se transcribe:

<<

Expediente N.º: EXP202313347

Procedimiento Sancionador Nº. PS/00289/2024

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

De las actuaciones practicadas por la Agencia Española de Protección de Datos y en base a los siguientes

HECHOS

PRIMERO: Con fecha 4 de agosto de 2023 se interpuso reclamación por ***A.A.A.*** ante la Agencia Española de Protección de Datos por una posible infracción imputable a ***SIDECU, S.A.*** con NIF ***A15435092*** (en adelante, SIDECU).

En su reclamación señala que es socio del Centro Deportivo Supera Entrepuentes y que se le está denegando el acceso a las instalaciones de la entidad reclamada, desde que se ha implementado un nuevo método de acceso a través de un sistema de reconocimiento facial, a lo que se niega la parte reclamante por entender que dicho sistema es invasivo al respecto de su intimidad y supone un tratamiento de datos que considera excesivo para el acceso a dicho establecimiento, entendiendo que pudieran habilitarse fórmulas alternativas para el acceso que no impliquen dicho tratamiento de datos. Y señala también que previamente se utilizaba un sistema de acceso mediante tarjeta, que el nuevo método es de cumplimiento obligatorio, y que la empresa no ha dado aviso previo ni consultado a los socios sobre la instalación de este nuevo método de acceso.
Junto con su reclamación, ***A.A.A.,*** aporta:

- Capturas de pantalla de las comunicaciones intercambiadas con la entidad reclamada a través de un sistema de mensajería, donde acusan recibo de su reclamación solicitando el documento de consentimiento para tratar sus datos, y le informan que se ha instalado este nuevo tratamiento pero que este no almacena las imágenes, sino que captura partes del rostro para configurar un algoritmo matemático que “queda al margen de la normativa del RGPD” según manifiesta el fabricante del programa, y le aporta información sobre el responsable del tratamiento.
- Correo electrónico remitido por el reclamante al centro solicitando poder acceder mediante tarjeta.

Posteriormente, se presentan otras 2 reclamaciones contra el centro de SUPERA Entrepuentes de SIDECU y una denuncia contra el centro deportivo SUPERA por la misma razón, por parte de socios del mismo que no están de acuerdo con el acceso a través de reconocimiento facial. En concreto:

- Reclamación de fechas de 22/08/2023, por parte de ***B.B.B.*** (en adelante, B.B.B.).
  Señala que solicitó a SIDECU el 10/08/2023: (i) la supresión de su huella digital usada previamente para acceder al centro deportivo y (ii) información acerca de la legalidad del nuevo sistema de acceso de reconocimiento facial implantado. Y que tras contestarle SIDECU que no se almacenaba la huella ni la imagen del reconocimiento facial, por lo que no se trataban datos personales, el reclamante reiteró la solicitud de borrado de huella, lo que fue

negado por el centro deportivo. Se aportan los 4 correos electrónicos intercambiados con el centro.

- Reclamación de 04/09/2023 por ***C.C.C.*** (en adelante, C.C.C.).

Señala que es socio durante unos años del gimnasio, y que desde el inicio el procedimiento de acceso a sus instalaciones ha sido mediante un torno controlado por tarjeta magnética y un sistema biométrico de reconocimiento de huella dactilar, si bien no fue informado en su momento del tratamiento de esos datos (adjunto doc01: hoja de registro).

Aproximadamente a principios de julio se incluyen sistemas de reconocimiento facial que entiende se aplican como alternativos ante la falta de información personalizada al respecto (no recibe ninguna información relativa a qué se pretendía). Al coexistir ambos sistemas de acceso no le dio importancia al asunto hasta el momento que en uno de los accesos de control de acceso original está desactivado y se le indica por el personal que es obligatorio pasar por el control biométrico basado en el reconocimiento facial.

Que se negó a utilizar el método de reconocimiento facial, habiendo requerido en múltiples ocasiones información al respecto, contestando el centro con una explicación que, a su juicio, es insuficiente, y que: "*se ha ignorado e incluso negado que la plantilla obtenida del reconocimiento facial fuese un dato de carácter personal y esa ha sido en parte la justificación de la no necesidad de informar ni de declarar las acciones necesarias para su protección".* Se señala que se han realizado preguntas concretas sobre el sistema, tales como el sistema de cifrado, el almacenamiento, la autenticación-identificación…etc y que la empresa se ha limitado a contestar que no se tratan datos personales al no almacenarse las imágenes. Y que el software utilizado es ******APP.1*** de la empresa ***EMPRESA.1.

No aporta el intercambio de correos, si bien transcribe los mismos.

- Denuncia de 20/09/2023 por la **ASOCIACION DE CONSUMIDORES Y USARIOS EN ACCION-FACUA** (en adelante, FACUA).

Señala que la mercantil denunciada es gestora y propietaria de la cadena de gimnasios Supera, cuya extensión geográfica abarca diversas provincias de todo el país. Y que ha tenido conocimiento de que la entidad utiliza un sistema de control biométrico para controlar el acceso de los usuarios a sus centros deportivos. Y se considera que el sistema establece una condición de acceso completamente desproporcionada, en tanto que se están solicitando datos de carácter personal especialmente protegidos, no siendo ni necesario ni proporcional.

Se acompañan: (i) Se aporta imagen como documento n.º 1 correspondiente a uno de los controles biométricos instalados a la entrada de los gimnasios que así lo acredita; (ii) como documento n.º 2 copia del documento tipo que de

acuerdo con la asociación se ha utilizado por el gimnasio para contestar a los usuarios que han formulado reclamación sobre el sistema.

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 las 3 reclamaciones presentadas a SIDECU con fecha de 2/10/2023, 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.

TERCERO: Con fecha de 2/11/2023, SIDECU contesta al primer traslado de reclamación realizado en el expediente (en adelante, 1ª Respuesta de SIDECU), señalando, básicamente, lo siguiente:

- En relación con la primera reclamación de ***A.A.A.***, señala que desde SIDECU se ha dado respuesta escrupulosa a todos y cada uno de los puntos detallados en las cuatro comunicaciones remitidas por el mismo, en las que éste hacía constar que el nuevo método de acceso conllevaba un tratamiento de datos de categoría especial, y se acompaña, como documento nº 1, cadena de emails intercambiados entre el 9/08/2023 y el 31/08/2023. En ellas se le informa de que no es necesario recabar el previo consentimiento de los socios para poder instalar este método de acceso por reconocimiento facial, según la empresa: "por no entenderse como un tratamiento de datos como tratamiento de categoría especial, pues el sistema no identifica, en ningún caso, a la persona física ni existe tratamiento de dato alguno", dado que el sistema instalado no almacena la imagen, ni supone un riesgo para los datos personales de los usuarios.

- En relación con la reclamación de ***C.C.C.,*** se manifiesta haber contestado al mismo en el mismo sentido que al anterior, tanto verbalmente por el personal del centro como por escrito contestando a su correo electrónico de 4/8/23, tal y como el mismo ha aportado al expediente.

- En relación con la reclamación de ***B.B.B.***, se manifiesta haber contestado al mismo puntualmente y se acompaña como documento nº 2 cadena de emails intercambiados entre el 10/08/2023 y el 17/08/2023. Con fecha 11/08/2023 SIDECU le respondió trasladándole información acerca del nuevo sistema implantado y de la imposibilidad de identificar al usuario a través de dicho sistema, tal y como se le había explicado a los demás usuarios. Ese mismo día se recibió nuevo email del usuario solicitando nuevamente el borrado de su huella digital. El 17/08/2023 desde SIDECU se le trasladó a esta persona que no podían atender a la solicitud de supresión de su "huella dactilar" por cuanto los sistemas utilizados a efectos de control de acceso no guardaban este dato y se le trasladó información acerca del nuevo sistema de acceso.

- En relación con "*EL ANÁLISIS DE RIESGOS PREVIAMENTE REALIZADO POR SIDECU",* se señala que con anterioridad se había instalado un sistema de acceso mediante huella que había tenido fallos de funcionamiento, y que tras analizar los riesgos de la nueva modalidad de reconocimiento facial de ***EMPRESA.1, se interpretó en base a la información proporcionada por el

fabricante que el sistema no suponía ningún riesgo puesto que no trataba datos personales.

En concreto, manifiesta lo siguiente (el subrayado es nuestro):

> *"La sociedad SIDECU, S.A. analizó diferentes modalidades de sistemas de acceso a sus centros deportivos, en virtud de los cuales se evitase, por un lado, el acceso de personas a los centros que no tuviesen la condición de abonados y, por otro lado, que cumpliesen con la condición de evitar el tratamiento de datos adicionales e innecesarios para los que hubiera que obtener el consentimiento expreso del usuario.*
> *Con anterioridad al uso de este sistema de acceso los centros deportivos tenían instalados unos sistemas que también utilizaban complejos algoritmos matemáticos desarrollados por el fabricante NITGEN, en los que el usuario accedía a través de su huella dactilar, pero sin que, en ningún caso, el sistema pudiera almacenarla. Se trataba de un sistema similar al utilizado en la actualidad, pero el análisis de la plantilla numérica se realizaba por medio de la huella dactilar en vez del reconocimiento facial.*
> *Ese sistema ya fue objeto de análisis en el año 2022 por esa Agencia Española de Protección de Datos en otro expediente, siendo inadmitida finalmente la reclamación por parte de esa Agencia al entender que SIDECU había cumplido todos los trámites establecidos y que no procedía la supresión de dato alguno por nuestra parte al no llegarse a tratar datos biométricos del usuario.*
> *Sin embargo, el sistema presentó fallos de funcionamiento en el acceso (fallos mecánicos frecuentes, en todo caso), lo que motivó a SIDECU a buscar otro sistema que fuese similar y no invasivo o intrusivo en los derechos de los usuarios y, en particular, que no tratase datos o almacenase datos de los usuarios.*
> *Así, se obtuvo diferente información acerca de diferentes sistemas biométricos, optando SIDECU por el sistema de la empresa ***EMPRESA.1 y realizando un análisis de riesgos previamente a su adquisición. Conforme a las explicaciones detalladas por el fabricante, este sistema no almacena la imagen procesada del individuo como si ocurre en otro tipo de registros, no realizando pues tratamiento de datos personales.*
> *Según la información que nos transmitió el fabricante, se crea un modelo con el algoritmo NIR, patentado por este fabricante, que utiliza algoritmos matemáticos complejos, generando un modelo numérico al usar información de alguno de los puntos del a captura. En ningún momento puede deducirse de este modelo características físicas de la persona. Esto es, los datos escaneados no quedan almacenados en el sistema y, mucho menos, en las bases de datos de SIDECU. En el momento del registro inicial de un usuario para la utilización de este tipo de sistemas, el sistema analiza puntos concretos de la imagen del individuo y crea un modelo numérico que funciona como una clave propia de cada usuario con la finalidad de acceso a las instalaciones. Así, el proceso posterior de identificación de la persona consiste en que, tras ponerse el usuario delante del sistema de reconocimiento*

facial, éste crea una nueva plantilla que se compara con las ya almacenadas. Si esta operación genera un resultado positivo, se considera al usuario correctamente identificado y se permite el acceso al centro deportivo. La plantilla codificada se asemeja pues a una clave alfanumérica que debiese ser tecleada para permitir el acceso a las instalaciones o a una tarjeta de acceso con chip, banda magnética o sistema RFID, por ejemplo, con la ventaja de que no se permite identificación personal de la persona a través de este sistema. Asimismo, a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno.

*En consecuencia, con la información técnica facilitada por el fabricante se concluyó que la instalación de estos sistemas en los CENTROS SUPERA no suponían ningún riesgo para el tratamiento de datos de carácter personal de los usuarios, dado que los datos extraídos por los lectores de ***EMPRESA.1 no podrían ser en ningún caso desencriptados ni desmontados, estando únicamente en posesión del fabricante las claves para el algoritmo, sin que se almacenase ningún tipo de información sobre la imagen de los usuarios.*
Acompañamos como documento nº 3 el certificado de protección de identidad facilitado por el fabricante".

- Por otra parte, se señala en este mismo apartado que se colocó un cartel informativo del funcionamiento del sistema en todos los centros y se aportan fotografías como documento 4: *"En cualquier caso, desde SIDECU se acordó que en todos los centros deportivos se colocaría en un lugar visible un cartel informativo acerca de estos sistemas con el fin de informar a los usuarios acerca de la protección de datos de carácter personal, del funcionamiento de los lectores y de su alcance.*

  Se acompaña, como documento nº 4 una fotografía del cartel expuesto en el centro deportivo SUPERA Entrepuentes, donde no se observa la fecha de colocación.

  Y, posteriormente, en el apartado 4 relativo a las MEDIDAS ADOPTADAS, se indica que (el subrayado es nuestro):

  "Habida cuenta que los tres usuarios son abonados del centro deportivo Supera Entrepuentes de Sevilla, se ha investigado internamente cuales han podido ser las causas que han motivado que estos tres usuarios presentasen la referida reclamación y si ese centro estaba ofreciendo a sus usuarios la información mediante la publicación de los carteles informativos en las instalaciones y a través del personal que trabaja en las mismas con motivo del cambio en el sistema de acceso. Se ha comprobado y verificado que el centro deportivo ha incorporado en un lugar visible y accesible a todos los usuarios los carteles informativos que proporcionan a los usuarios la información necesaria acerca del

uso de este sistema y en el que se les traslada que este sistema no trata ningún dato personal"

- *En el apartado "MOTIVOS QUE HAN PODIDO LLEVAR A LA RECLAMACIÓN",* se hacen constar los motivos por los que no se ha recabado el consentimiento a los interesados para tratar sus datos personales, por entender la reclamada que el nuevo sistema de acceso al gimnasio no trata datos personales en base a lo siguiente:

> *"Si bien es cierto, que en la documentación de alta de usuario no aparece contemplada la autorización para la recogida de datos personales relativos al uso de datos biométricos o de categorías especiales, ello es debido a que, atendiendo a las características del funcionamiento del sistema de acceso, no solo no se guarda la imagen de los usuarios por parte de SIDECU, S.A. como teórico responsable del tratamiento, sino que no se conserva ningún tipo de dato personal, pues la plantilla generada por el sistema no permite la asociación a ninguna persona concreta.*
> *Tal y como señaló esa Agencia Española de Protección de Datos en su Informe 36/2020, no se trata de un tratamiento de datos como tratamiento de categoría especial, pues no identifica, en ningún caso, de manera unívoca a una persona física.*
> *Los CENTROS SUPERA únicamente acceden a registros de entrada y salida y presencia en las instalaciones obteniendo exclusivamente información correspondiente a las horas y número de personas, pero no a su identificación personal.*
> *Asimismo, el segundo ordinal del artículo 4 del RGPD, señala que se entenderá por "tratamiento" de datos: "Cualquier operación o conjunto de operaciones realizadas sobre datos personales 0 conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción ". Es por dicha razón que no puede entenderse como tratamiento de datos personales el caso que nos ocupa, pues no se encuentra dentro de la categoría de los mismos. Reiteramos que, a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno. La generación de las plantillas mediante los complejos algoritmos matemáticos desarrollados por ***EMPRESA.1 no permite que el sistema guarde la imagen ni que la plantilla generada se asocie a usuarios concretos, por lo que no puede existir tratamiento de datos si éstos no se someten a ninguna de las operaciones recogidas en el artículo antes referido.*
>
> *El funcionamiento de este sistema queda al margen de la aplicación del artículo anteriormente mencionado del RGPD, ya que, en ningún caso, puede someterse al cumplimiento de lo dispuesto por la normativa en*

materia de protección de datos a un sistema de mero control de acceso que no trata dato personal alguno, pues ni los recoge, ni los conserva, ni permite la identificación de las personas. En consecuencia y al no existir ningún tratamiento de datos personales, no resulta pues aplicable el contenido de la normativa relativa a protección de datos personales ni, por ello, el deber de notificación de tratamiento de datos, motivo por el cual nuestra entidad no ha procedido previamente a solicitar su consentimiento para el uso de su imagen pues, como indicamos, no se trata ni almacena en ningún caso."

- Por último, en relación con lo supuesta exfiltración de datos personales de ***EMPRESA.1 que según la reclamación de **C.C.C.** afectó a más de 27 millones de usuarios, señalan que: *"Les informamos que tras consultarlo con el fabricante y analizar los sistemas implantados, no es posible que ninguna supuesta filtración haya afectado a las plantillas correspondientes los usuarios de nuestros centros deportivos, por cuanto éstas se guardan en nuestros propios servidores informáticos (dotados de los oportunos sistemas de seguridad), sin que en ningún caso la compañía suministradora de los equipos de acceso biométrico haya podido tener acceso a los mismos".*

La empresa reclamada aporta los siguientes documentos con su escrito:

- Como documentos 1 y 2. Cadena de intercambio de correos electrónicos con cada reclamante.
- Como documento nº 3. El certificado de protección de identidad facilitado por el fabricante ***EMPRESA.1, redactado en inglés (GDPR Compliance Statement).
- Como documento nº4. Una fotografía de los carteles que de acuerdo con la reclamada han sido expuestos en los centros deportivos.

CUARTO: Con fecha 7 de noviembre de 2023, de conformidad con el artículo 65 de la LOPDGDD, se admitieron a trámite las tres primeras reclamaciones presentadas y remitió acuse de recibo a los reclamantes.
QUINTO: Con fecha de 15/11/2023, 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.

Durante la misma, se llevaron a cabo las siguientes actuaciones previas de investigación:

- 14/12/2023. Se remite un requerimiento de información a SIDECU por parte del inspector del procedimiento para que aporte en el plazo de diez días hábiles información y documentación con relación al sistema de reconocimiento facial instalado en los centros de la entidad:

PUNTO 1. Datos tratados y técnicas empleadas. Descripción del sistema utilizado, respondiendo acerca de determinados puntos que concreta el inspector.
PUNTO 2. Número total de centros de la entidad que tienen implementado reconocimiento facial de usuarios. Número de usuarios total aproximado de estos centros. Numero usuarios del centro de Entrepuentes-Sevilla. Número de personas que han mostrado su rechazo al sistema o no han querido acceder a reconocimiento facial.
PUNTO 3. Bases jurídicas (de legitimación) para el tratamiento de datos personales con reconocimiento facial. Confirmación sobre que no se ha recabado el consentimiento de los usuarios para este tratamiento de datos.
PUNTO 4. Información facilitada a los usuarios con respecto al reconocimiento facial. 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.
PUNTO 5. Copia del Registro de Actividades del Tratamiento (RAT) al que se refiere el art. 30 del RGPD.
PUNTO 6. Información sobre si se realizó una Evaluación de Impacto o un Estudio previo similar con relación a los tratamientos de datos basados en reconocimiento facial. Copia de la misma en caso afirmativo. Copia de la documentación acreditativa de la valoración previa de métodos alternativos a la implementación del sistema de reconocimiento facial.

- 16/12/2023: Se expide Diligencia para hacer constar que en esta fecha se obtiene impresión de la siguiente información obtenida a través de Internet sobre el programa de reconocimiento facial de "***EMPRESA.1" con su algoritmo NIR que se alude en las contestaciones a los reclamantes por parte de la entidad reclamada. En el que queda capturada la pantalla sobre "Certificado de Protección de Datos Faciales de ***EMPRESA.1", en la que se certifica que ***EMPRESA.1 ***APP.2 y ***APP.3 extraen los puntos de las imágenes faciales en bruto y crean una plantilla a partir de estos datos.

- 03/01/2024. **Reclamación** presentada por ***D.D.D.*** en relación con el centro deportivo San Diego de Coruña, de la que se da traslado a SIDECU el 20/2/2024.

- 19/01/2024**.**Tras solicitarse y ampliarse el plazo para contestar, SIDECU responde al requerimiento de información realizado durante la fase de investigación (en adelante, Respuesta 2), reiterando lo indicado anteriormente respecto a que el programa ***EMPRESA.1 no trata datos personales, y añadiendo, en esencia, lo siguiente:

    - En relación con el funcionamiento del sistema implantado:

        "(…) Así, el proceso posterior de identificación de la persona consiste en que, tras ponerse el usuario delante del sistema de reconocimiento facial, éste crea una nueva plantilla que se compara con las ya almacenadas. Si esta operación genera un resultado positivo, se considera al usuario correctamente identificado y se permite el acceso al centro deportivo. La

plantilla codificada se asemeja pues a una clave alfanumérica que debiese ser tecleada para permitir el acceso a las instalaciones o a una tarjeta de acceso con chip, banda magnética o sistema RFID, por ejemplo, con la ventaja de que no se permite identificación personal de la persona a través de este sistema. A partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno. Es decir, no se utiliza ningún dispositivo adicional a la cámara del propio sistema, que no almacena datos del usuario más allá de la plantilla codificada y que no permite recuperar la imagen del usuario.

Asimismo, es preciso destacar que el sistema de autentificación se realiza 1 a N (comparando la plantilla codificada en el momento de identificación).

- Se acompañan fotografías del cartel informativo de los centros con la información indicada por el fabricante como Documento 2.

- Los CENTROS SUPERA únicamente acceden 3 registros de entrada y salida y presencia en las instalaciones obteniendo exclusivamente información correspondiente a las horas y número de personas, pero no a su identificación personal. Es decir, únicamente se registra la fecha y hora de acceso, junto con el código del usuario (número de socio). Se aporta, como documento nº 3, evidencia de un registro de entrada y salida de un centro.

- Actualmente el referido sistema de reconocimiento facial se encuentra instalado en cinco centros deportivos, siendo el número total de usuarios de dichos centros de 36.483. Uno de esos centros es el de Entrepuentes de Sevilla, el cual cuenta actualmente con 8.978 usuarios (a fecha 4/01/2024). De estos usuarios del centro deportivo Entrepuentes un total de 26 usuarios han manifestado su oposición al sistema de acceso, habilitándose por parte de SIDECU una alternativa de acceso mediante identificación en la recepción del centro mediante la exhibición del Documento Nacional de Identidad al personal de dicho centro deportivo y la apertura manual del tomo de acceso.

- En contestación al requerimiento acerca de las bases de legitimación del tratamiento: la empresa no menciona ni las bases de licitud del artículo 6 del RGPD ni la excepción del artículo 9.2 del RGPD que habilitan al tratamiento, indicando de nuevo que no es necesario cumplir la normativa de protección de datos personales, puesto que el programa no trata datos personales. A lo ya indicado, se añade que:

  "Tal y como señaló esa Agencia Española de Protección de Datos en su Informe 36/2020, no se trata de un tratamiento de datos como tratamiento de categoría especial, pues no identifica, en ningún caso, de manera unívoca a una persona física.

Los CENTROS SUPERA únicamente acceden a registros de entrada y salida y presencia en las instalaciones obteniendo exclusivamente información correspondiente a las horas y número de personas, pero no a su identificación personal.
Asimismo, el segundo ordinal del artículo 4 del RGPD, señala que se entenderá por "tratamiento" de datos: "Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción(…)
El funcionamiento de este sistema queda al margen de la aplicación del artículo anteriormente mencionado del RGPD, ya que, en ningún caso, puede someterse al cumplimiento de lo dispuesto por la normativa en materia de protección de datos a un sistema de mero control de acceso que no trata dato personal alguno, pues ni los recoge, ni los conserva, ni permite la identificación de las personas".

- En cuanto a la información proporcionada a los usuarios: Se señala que se contestaron todas las solicitudes de información y que se colocaron carteles en todos los centros deportivos que se aportan como documento 2, en un lugar visible y accesible a todos, siendo ésta la única información proporcionada.

- Por lo que respecta a la documentación aportada:

  Como documento 1 se aporta poder de designación/ representación.
  aportado como documento.
  Como documento 2 se aportan fotografía de los carteles expuestos, idénticas a las aportadas en la 1ª Respuesta (del centro de Entrepuentes).
  Como documento 3, la hoja de registro de entradas y salidas.
  Como documento nº 4 el mismo certificado de protección de datos del fabricante que ya fue aportado anteriormente como documento nº1 de la 1ª Respuesta.
  Como documento nº 5 se acompaña por primera vez el análisis de riesgos realizado y "conclusiones alcanzadas acerca de la necesidad de obtener el consentimiento previo de los usuarios", a las que se hacía referencia en la 1ª Respuesta. Documento de 2 páginas, fechado el 2-9-22 y realizado por SUPERA.
  Y como documento nº 6, copia del Registro de Actividades del Tratamiento de GRUPO SIDECU.

- 04/03/2024: Se presenta escrito de FACUA solicitando información sobre el estado de las actuaciones. Con fecha de 05/06/2024 se reitera tal solicitud de

información. Y con fecha de 18/06/2024 se contesta a la misma que se han iniciado actuaciones previas de investigación.

- 11/03/2024. Reclamación de ***E.E.E.*** en relación con el centro deportivo de Valladolid, de la que se da traslado a SIDECU el 18/3/2024.
- 1/04/2024. Respuesta de SIDECU al traslado de la reclamación de ***D.D.D.*** (en adelante, 3ª Respuesta de SIDECU) frente al centro deportivo de San Diego La Coruña, en el que se aportan los mismos 3 documentos ya aportados anteriormente (certificado protección datos, fotografía carteles, y análisis de riesgos) y se reiteran los argumentos indicados en las anteriores respuestas, añadiendo lo siguiente:

    - En el punto segundo se acredita haber contestado a la reclamación interpuesta por la citada reclamante, en el mismo sentido que a los anteriores reclamantes, y se acompaña como documento nº 4 copia de la comunicación recibida y la respuesta enviada por SIDECU.
    - Se manifiesta que se ha comprobado que este centro también había expuesto los carteles informativos, y aporta fotografía de exposición del CM SAN DIEGO.
    - Se afirma que *"En cualquier caso, todos los centros de Supera están preparados con sistemas alternativos de acceso, como el presencial clásico de exhibición del documento de identidad que se contrasta con los datos incluidos en el sistemas de Centros Supera".*

- 03/04/2024: Se remite escrito de admisión a trámite de la reclamación de ***D.D.D..***

- ******FECHA.1.*** Se contesta por SIDECU a la reclamación presentada por ***E.E.E.*** (en adelante, 4ª Respuesta de SIDECU) frente al Centro Deportivo Supera de Valladolid, aportando las fotografías de los carteles expuestos en dicho centro como documento 2 del "CDO El Palero", y las respuestas dadas a la reclamación interpuesta por el mismo como documentos 4 y 5, además de reiterar lo manifestado y aportar de nuevo el certificado de protección y el análisis de riesgos.

- ******FECHA.2.*** Se remite escrito de admisión a trámite de la reclamación presentada por ***E.E.E..***

- ***FECHA.2. Se expide Diligencia para unir al procedimiento los documentos que aparecen al acceder a los enlaces "protección de datos", "condiciones generales" y "Reglamento de Régimen Interno" que aparecen en el formulario de inscripción aportado junto con las primeras reclamaciones presentadas.

- ***FECHA.2. Diligencia haciendo constar la información básica obtenida de la herramienta Axesor acerca de la empresa reclamada.

- 06/06/2024. Se remite y notifica por error un requerimiento de información a

  SIDECU que correspondía a número de actuaciones previas (AI/00194/2024), y con fecha de 07/06/2024, se le remite comunicación informando de que se ha

anulado el requerimiento de 06/06/2024, y que no es necesario que conteste al mismo.

- 14/06/2024. **Reclamación** presentada contra SIDECU por ***F.F.F.,*** señalando que el "*En el Centro de Deporte y Ocio La Lanera de Palencia se ha implantado un sistema de acceso mediante el sistema de análisis biométrico facial (llevando ya instalado unos 10 años también el acceso mediante tarjeta y detección de huella). El análisis biométrico facial se ha realizado a los usuarios sin informarles en absoluto del riesgo de los datos que están aportando y sin un consentimiento escrito de ello*".

Concluidas las actuaciones previas de investigación, **con fecha de 21/06/2024, se emite informe de actuaciones previas de investigación por el inspector** (en adelante, informe API), que valora el resultado de las actuaciones realizadas hasta el momento. Entre sus afirmaciones, el informe señala:

PUNTO 1. Procedimiento de Admisión a Trámite

En el marco de las actuaciones de admisión a trámite de las reclamaciones la parte reclamada ha manifestado que han trasladado a los reclamantes información acerca del nuevo sistema señalando los motivos por los cuales no resultaba necesario el consentimiento previo del usuario "*por no entenderse como un tratamiento de datos como tratamiento de categoría especial, pues el sistema no identifica, en ningún caso, a la persona física ni existe tratamiento de dato alguno".*

Han indicado también que *"el sistema implantado no almacenaba la imagen, ni suponían un riesgo para los datos personales de los usuarios y no era necesario recabar un consentimiento previo puesto que, dadas las características del sistema, ni se guardaba la imagen ni ningún dato que permitiese identificar al usuario, no realizando tratamiento alguno de datos"*.

Los representantes de la parte reclamada han manifestado en general al contestar a los escritos de traslado de las reclamaciones interpuestas que han atendido las solicitudes ejercitadas por los usuarios, remitiéndoles las explicaciones de un modo exhaustivo, aclarándoles que el uso de los sistemas utilizados en sus centros deportivos no suponía un tratamiento de sus datos, puesto que estos sistemas únicamente analizan puntos concretos de la imagen del individuo creando un modelo numérico (plantilla) que funciona como una clave propia de cada usuario con la finalidad de acceso a las instalaciones. Indican que a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. Manifiestan que por tanto no hay tratamiento de dato personal alguno.

En concreto, han manifestado en el escrito de respuesta de 2-11-23 al traslado de las 3 primeras reclamaciones del presente expediente, además que:

> *"La sociedad SIDECU, S.A. analizó diferentes modalidades de sistemas de acceso a sus centros deportivos, en virtud de los cuales se evitase, por un*

lado, el acceso de personas a los centros que no tuviesen la condición de abonados y, por otro lado, que cumpliesen con la condición de evitar el tratamiento de datos adicionales e innecesarios para los que hubiera que obtener el consentimiento expreso del usuario.
Con anterioridad al uso de este sistema de acceso los centros deportivos tenían instalados unos sistemas que también utilizaban complejos algoritmos matemáticos desarrollados por el fabricante NITGEN, en los que el usuario accedía a través de su huella dactilar, pero sin que, en ningún caso, el sistema pudiera almacenarla.
Se trataba de un sistema similar al utilizado en la actualidad, pero el análisis de la plantilla numérica se realizaba por medio de la huella dactilar en vez del reconocimiento facial.
Ese sistema ya fue objeto de análisis en el año 2022 por esa Agencia Española de Protección de Datos en otro expediente, siendo inadmitida finalmente la reclamación por parte de esa Agencia al entender que SIDECU había cumplido todos los trámites establecidos y que no procedía la supresión de dato alguno por nuestra parte al no llegarse a tratar datos biométricos del usuario.
Sin embargo, el sistema presentó fallos de funcionamiento en el acceso (fallos mecánicos frecuentes, en todo caso), lo que motivó a SIDECU a buscar otro sistema que fuese similar y no invasivo o intrusivo en los derechos de los usuarios y, en particular, que no tratase datos o almacenase datos de los usuarios.
*Así, se obtuvo diferente información acerca de diferentes sistemas biométricos, optando SIDECU por el sistema de la empresa ***EMPRESA.1 y realizando un análisis de riesgos previamente a su adquisición.*
Conforme a las explicaciones detalladas por el fabricante, este sistema no almacena la imagen procesada del individuo como sí ocurre en otro tipo de registros, no realizando pues tratamiento de datos personales. Según la información que nos transmitió el fabricante, se crea un modelo con el algoritmo NIR, patentado por este fabricante, que utiliza algoritmos matemáticos complejos, generando un modelo numérico al usar información de alguno de los puntos de la captura. En ningún momento puede deducirse de este modelo características físicas de la persona. Esto es, los datos escaneados no quedan almacenados en el sistema y, mucho menos, en las bases de datos de SIDECU.
En el momento del registro inicial de un usuario para la utilización de este tipo de sistemas, el sistema analiza puntos concretos de la imagen del individuo y crea un modelo numérico que funciona como una clave propia de cada usuario con la finalidad de acceso a las instalaciones.

Así, el proceso posterior de identificación de la persona consiste en que, tras ponerse el usuario delante del sistema de reconocimiento facial, éste crea una nueva plantilla que se compara con las ya almacenadas. Si esta operación genera un resultado positivo, se considera al usuario correctamente identificado y se permite el acceso al centro deportivo.
La plantilla codificada se asemeja pues a una clave alfanumérica que debiese ser tecleada para permitir el acceso a las instalaciones o a una tarjeta de acceso con chip, banda magnética o sistema RFID, por ejemplo, con la ventaja de que no se permite identificación personal de la persona a través de este sistema.

Asimismo, a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno.
*En consecuencia, con la información técnica facilitada por el fabricante se concluyó que la instalación de estos sistemas en los CENTROS SUPERA no suponían ningún riesgo para el tratamiento de datos de carácter personal de los usuarios, dado que los datos extraídos por los lectores de ***EMPRESA.1 no podrían ser en ningún caso desencriptados ni desmontados, estando únicamente en posesión del fabricante las claves para el algoritmo, sin que se almacenase ningún tipo de información sobre la imagen de los usuarios."*

PUNTO 2. **Información a los usuarios**.

En el documento de registro (procedimiento administración y recepción en los centros*),* formulario de inscripción a los centros, se recogen los datos personales del nuevo socio (nombre y apellidos, número de DNI, fecha de nacimiento, dirección, teléfonos, email, datos bancarios) y se informa de lo siguiente:

"Con la firma del presente documento afirmo que he leído y acepto las condiciones de protección de datos,
☐ Ud. consiente y autoriza expresamente a que SIDECU, S.A. trate los datos que ha facilitado para realizar estudios estadísticos y para ofrecerle periódicamente información sobre productos, actividades, servicios y acciones comerciales de promoción y/o marketing relacionadas con proveedores de transportes, deportes, seguros, servicios inmobiliarios, financieros y bancarios, con el fin de informar de sus productos o servicios y hacer ofertas comerciales, incluyendo por medios de comunicación electrónica."

En este documento de registro existen varios enlaces, uno de "Protección de Datos", en el que se ha comprobado que ofrece la siguiente información:

"CLÁUSULA RESPONSABLE DEL TRAMIENTO DE DATOS PERSONALES
Los datos que Vd. proporcione a fin de desarrollar el objeto del presente contrato, serán incorporados a las bases de datos propiedad de SIDECU, S.A., que actuará como Responsable del Tratamiento.
Los datos referentes a datos personales y datos médicos relativos a salud que Vd. pueda facilitar, con la finalidad de la adecuada prestación de los servicios que solicite en cada momento, se emplearán única y exclusivamente a los efectos de cumplir con el objeto del presente contrato y, en particular, con las finalidades siguientes: gestión de clientes, premiar su fidelidad, mantenerlos informados (envío boletín de noticias), por cualquier medio (electrónico o no), de ofertas de productos y/o servicios y/o promociones relacionadas con las actividades propias del presente contrato y del objeto social de SIDECU, S.A.
Con el fin de poder ofrecerle productos y/o servicios de acuerdo con sus intereses y mejorar su experiencia, podremos elaborar un perfil comercial en base a la información facilitada por Vd. No obstante, no se tomarán decisiones automatizadas en base a dicho perfil.
De conformidad con la normativa vigente en materia de protección de datos de carácter personal, tiene derecho a ejercitar en cualquier momento sus derechos de acceso, rectificación, portabilidad, limitación, supresión u

oposición de los datos referentes a su persona incluidos en nuestras bases de datos ante el Delegado de Protección de Datos, acreditando debidamente su identidad; así como presentar una reclamación ante la autoridad de control estatal en caso de que el titular de los datos de carácter personal considere que se han vulnerado sus derechos.
En todo caso, el consentimiento tiene carácter revocable, pudiendo Ud. retirar en cualquier momento el consentimiento prestado o ejercitar cualquier de los derechos mencionados en la forma indicada en la presente cláusula. Ud. responderá de la veracidad de los datos facilitados a SIDECU, S.A. reservándose éste la facultad de excluirle de cualesquiera actuaciones y/o servicios en caso de que facilite datos falsos, sin perjuicio de cualesquiera otras acciones que puedan proceder. Del mismo modo, Ud. es responsable de mantener actualizados los datos personales que haya facilitado a SIDECU, S.A.
Los datos facilitados serán conservados y tratados por SIDECU, S.A. mientras se mantenga la relación contractual, mientras no se solicite su supresión y, en cualquier caso, hasta el vencimiento de los plazos legalmente exigibles"

En el enlace de "condiciones generales" no se encuentra información de protección de datos. En el enlace Reglamento de Régimen Interno, que varía para cada uno de los centros, se encuentra la siguiente información de Protección de Datos:

"*1.8. A los efectos de la Ley Orgánica 15/1999 de 13 de Diciembre de protección de datos de carácter oficial, al inscribirse en la instalación se autoriza la utilización de los datos personales y su tratamiento informático para la gestión de la instalación y en su caso el envío de información comercial inherente a la gestión del Centro."*

Los representantes de la parte reclamada indican que han colocado carteles informativos sobre el sistema de reconocimiento facial en todos los centros, aportando fotografía de su colocación así como el contenido del mismo que se reproduce a continuación:

"¿Qué es un sistema de identificación biométrico?
*Este tipo de sistemas biométricos utilizan alguna característica física e intransferible de la persona para realizar su identificación o verificación. Los sistemas biométricos de ***EMPRESA.1, extraen los puntos de datos faciales de las imágenes sin procesar y crea una plantilla a partir de estos datos.*

¿Qué ventajas tienen los sistemas biométricos?
- Garantizan la identificación y verificación del usuario de una manera rápida, fácil y fiable.
- Es una tecnología robusta ampliamente estudiada y probada.
- Al utilizar una característica intransferible, no es posible el uso fraudulento de llaves remplazando la identidad de otras personas.

¿Privacidad y protección del usuario?
*Los sistemas biométricos de ***EMPRESA.1 no guardan la imagen procesada, crea una plantilla con el algoritmo NIR patentado por ***EMPRESA.1. Mediante complejos algoritmos matemáticos se genera la plantilla numérica utilizando la*

información de algunos puntos de la captura. En ningún se puede deducir a partir de la plantilla características físicas, el algoritmo de extracción sólo es conocido por el fabricante.

Funcionamiento
*La plantilla de la cara no es una imagen en bruto. Se crea utilizando la tecnología y el algoritmo NIR patentados de ***EMPRESA.1, y la plantilla es un conjunto de datos que es una fusión de características 2D y 3D de la cara de un usuario la cual es adquirida por una cámara visual y una cámara NIR. Para proteger esta plantilla, se utilizan herramientas criptográficas y métodos de encriptación, como la encriptación AES de 256 bits."*

PUNTO 3. Sobre el funcionamiento del sistema

Sobre el funcionamiento del sistema, la parte reclamada repite en todos los escritos de respuesta que el programa de ***EMPRESA.1 que utiliza para realizar el reconocimiento facial de los socios no almacena la imagen facial sino una plantilla generada por un algoritmo matemático; y que a partir de la plantilla no es posible recuperar la imagen facial ni características físicas de la persona, manifestando que por tanto no se realizan tratamientos de datos personales.

Para acreditar esta cuestión aportan un certificado del fabricante en cada uno de los cuatro escritos de respuesta donde se menciona que nunca se almacena la imagen facial en el dispositivo sino una plantilla que se genera y cifra, no siendo posible recuperar la imagen original del rostro a partir de la plantilla. No se realiza ninguna mención en este certificado sobre si se tratan o no datos personales.

La empresa mantiene que el programa no implica tratamiento de datos personales a la vista de que:

"*(..) El segundo ordinal del artículo 4 del RGPD, señala que se entenderá por "tratamiento" de datos: «Cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.»*
Es por dicha razón que no puede entenderse como tratamiento de datos personales el caso que nos ocupa, pues no se encuentra dentro de la categoría de los mismos. Reiteramos que, a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno."

Indican que no se utiliza ningún dispositivo adicional a la cámara del propio sistema (tarjetas o pulsaras identificadoras) realizándose la comparación 1 a N, es decir, comparando la plantilla obtenida en el momento de la entrada con las almacenadas en el sistema.

En la segunda respuesta (respuesta al requerimiento de investigación), indican que únicamente se registra la fecha y hora de acceso, junto con el código del usuario (número de socio). Aportan como evidencia al respecto de esta cuestión la impresión de pantalla del sistema en la que se comprueba que se aprecian los siguientes datos para cada una de las entradas a uno de los Centros: fecha y hora, id del dispositivo (torno), Centro, Identificador del usuario, y resultado de la comparación, que en todos los casos listados figura como “Autenticación 1:N correcta (Cara)”.

PUNTO 4. Registro Actividades de Tratamiento (RAT), Análisis de Riesgos (AR) y Evaluación de Impacto (EIPD)

Junto con el segundo escrito de respuesta, se aporta también copia del RAT, en el que en el apartado 5 relativo al tratamiento de los datos personales de los clientes(abonados) en el que como fines del tratamiento se indica la “gestión de la relación con los clientes o potenciales clientes”. En la sección de categorías de datos tratados no se mencionan datos biométricos.

Y acompañan también el Análisis de Riesgos, que se titula “ANÁLISIS DE RIESGOS PREVIO A UNA EIPD” y se refiere a la iniciativa de implantación de sistemas de reconocimiento facial de ***EMPRESA.1 para el acceso a los centros deportivos de GRUPO SUPERA. En este, se cita que no se van a tratar datos personales y como conclusión:

> *“Según la información facilitada por el fabricante, la implantación del sistema de reconocimiento facial fabricado por ***EMPRESA.1 no supone ningún tratamiento de dato personal para los usuarios de los centros deportivos que accedan al mismo.*
>
> *El sistema genera una plantilla a partir de la imagen del usuario (la primera vez que accede) que no asocia a ninguna persona en particular, sino que simplemente analiza si el usuario que accede tiene o no derecho a ello.*
> *En particular, los datos extraídos por los lectores de ***EMPRESA.1 no podrían ser en ningún caso desencriptados ni desmontados, estando únicamente en posesión del fabricante las claves para el algoritmo, sin que se almacenase ningún tipo de información sobre la imagen de los usuarios.*
> *El sistema de reconocimiento facial tampoco se conecta a la base o listado de usuarios de los centros deportivos en ningún momento.*
> *Se aporta al presente informe el certificado emitido por el fabricante a tal efecto.*
>
> *En definitiva, no procede realizar ninguna Evaluación de Impacto al no existir tratamiento de datos al no poderse, en ningún caso, recuperar la imagen personal del usuario, ni siquiera deducir características físicas concretas de la misma, no pudiendo identificar a la persona.*
> *Se acuerda poner a disposición de los usuarios carteles informativos que informen acerca del nuevo sistema implantado y de sus características.*
> *Al no existir tratamiento de datos, ni poder ser considerado como tratamiento de categoría especial, tampoco procede recabar previamente el consentimiento del usuario. En cualquier caso, se podrá poner a disposición de los usuarios*

alternativas de acceso en los casos en los que se nieguen a utilizar este sistema.

En definitiva, se deduce que el sistema propuesto no resulta intrusivo ni atenta contra los derechos de los usuarios de los centros deportivos al no tratar ni almacenar su imagen personal ni ningún otro dato que permita identificarlos."

PUNTO 5. Medidas de seguridad

En el RAT constan las siguientes medidas de seguridad para los tratamientos de datos de los abonados con carácter general: control acceso perimetral; control acceso CPD; seguridad hardware; control de dispositivos extraíbles; seguridad soluciones cloud; seguridad sistemas operativos; antivirus; segmentación red y firewall; seguridad aplicaciones; documentos en papel bajo sistemas de seguridad.

En la documentación técnica aportada por el fabricante se cita:

- *"Devices are equipped with a secure tamper feature, which ensures the security of data stored in the devices. If the device is removed from the wall and tampered with, the secure data (biometric templates, User ID, Logs) within the device will automatically be deleted"* que se puede traducir como: "los dispositivos están equipados con una función de manipulación segura que garantiza la seguridad de los datos almacenados en los dispositivos. Si el dispositivo se retira de la pared y se manipula, los datos seguros (plantillas biométricas, ID de usuario, registros) dentro del dispositivo se eliminarán automáticamente."

- También se cita que se utilizan técnicas de cifrado como 256bit AES, que existen pistas de auditoría sobre los accesos y que la tasa de falsos negativos es menor del 1% y la de falsos positivos menor que 0,00002%.

SEXTO: Con fecha de 24/06/2024 se obtiene como evidencia la política de privacidad de SUPERA, en la que consta SIDECU como responsable del tratamiento de datos personales de la URL centrosupera.com, y se une al procedimiento.

SÉPTIMO: Con posterioridad a la emisión del informe de actuaciones previas de investigación se han presentado y admitido a trámite las siguientes reclamaciones presentadas por socios de los diferentes centros deportivos en los que SIDECU ha instalado el citado sistema de reconocimiento facial, que se unen y acumulan dentro del presente expediente, dado que su contenido es análogo a las presentadas con anterioridad.

- 25/06/2024. Se admite a trámite la reclamación de ***F.F.F.***, que fue presentada el 14-6-24.

- 08/07/2024 Admisión a trámite de la reclamación presentada por ***G.G.G.*** el 26/06/204.

- 07/10/2024. Admisión a trámite de la reclamación presentada por ***H.H.H.*** con fechas de 16/09/2024, y 27/09/2024.

Así mismo, se une al presente procedimiento la denuncia interpuesta por ***J.J.J.*** informando de la instalación de un sistema de reconocimiento facial para acceder al "Centro Deportivo Supera Guadalquivir" con fecha de 2/08/2024.

OCTAVO: De acuerdo con el informe recogido de la herramienta AXESOR con fecha de 12/03/2025, la entidad SIDECU es una empresa de tamaño grande constituida en el año 1993 dedicada a la gestión de instalaciones deportivas, y con un volumen de negocios de **16.154.950 euros** en el año 2023.

NOVENO: Con fecha de 13 de marzo de 2025 se expide Diligencia para incorporar al expediente electrónico la información que aparece publicada en la url de la entidad ***EMPRESA.1 ******EMPRESA.1 | Security & Biometrics*** (***EMPRESA.1.inc.com/es), en la que se ofertan diferentes sistemas y funcionalidades de la plataforma ******APP.1*** de seguridad -que incluyen un sistema centralizado o distribuido de acceso a los centros con identificación basada en biometría-, y diversos productos de hardware como lectores biométricos de huella dactilar y reconocimiento facial.

DÉCIMO: Con fecha de 2 de abril de 2025 se expide Diligencia para reflejar los centros SUPERA que se encuentran publicados en la URL centrossupera.com, que asciende a 33.

FUNDAMENTOS DE DERECHO

I. Competencia

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 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Presidencia de la Agencia Española de Protección de Datos.

II. Procedimiento

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".*

De acuerdo con el artículo 64 de la LOPDGDD, y teniendo en cuenta las características de las presuntas infracciones cometida, se inicia un procedimiento sancionador.

El procedimiento tendrá una duración máxima de doce meses a contar desde la fecha del acuerdo de inicio. Transcurrido ese plazo se producirá su caducidad y, en consecuencia, el archivo de actuaciones, de conformidad con lo establecido en el artículo 64 de la LOPDGDD.

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP).

III. Cuestiones previas.

3.1. Datos personales objeto de tratamiento.

Definición de los datos biométricos de carácter personal.

Los sistemas de procesamiento de datos biométricos son métodos automáticos que se basan en recoger y procesar datos personales relativos a las características físicas, fisiológicas o conductuales de las personas físicas, entre las que cabe incluir las características neuronales de estas, mediante dispositivos o sensores, creando plantillas biométricas (también denominadas firmas o patrones) que posibilitan la identificación, seguimiento o perfilado de dichas personas.

Como ya señaló el Dictamen 4/2007 del grupo de trabajo del artículo 29 (ART. 29 de la Directiva 95/46 CE, como organismo de la UE, de carácter consultivo e independiente), sobre el concepto de datos personales (WP136), de 20/06/2007, los datos biométricos pueden definirse como:

> *"… propiedades biológicas, características fisiológicas, rasgos de la personalidad o tics, que son, al mismo tiempo, atribuibles a una sola persona y mensurables, incluso si los modelos utilizados en la práctica para medirlos técnicamente implican un cierto grado de probabilidad. Ejemplos típicos de datos biométricos son los que proporcionan las huellas dactilares, los modelos retinales, la estructura facial, las voces, pero también la geometría de la mano, las estructuras venosas e incluso determinada habilidad profundamente arraigada u otra característica del comportamiento (como la caligrafía, las pulsaciones, una manera particular de caminar o de hablar, etc.). Una particularidad de los datos biométricos es que se les puede considerar tanto como contenido de la información sobre una determinada persona (Fulano tiene estas huellas dactilares) como un elemento para vincular una información a una determinada persona (este objeto lo ha tocado alguien que tiene estas huellas dactilares y estas huellas dactilares corresponden a Fulano; por lo tanto, Fulano ha tocado este objeto). Como tales, pueden servir de «identificadores». En*

efecto, al corresponder a una única persona, los datos biométricos pueden utilizarse para identificar a esa persona. Este carácter dual también se da en el caso de los datos sobre el ADN, que proporcionan información sobre el cuerpo humano y permiten la identificación inequívoca de una, y sólo una, persona."

El RGPD define el art.4.14 datos biométricos como una categoría de datos personales, señalando que son: "*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*". (el subrayado es nuestro).

Por su parte, el artículo 4.1 del RGPD, al definir los datos de carácter personal incide en esta misma finalidad de identificación única de la persona, señalando que "*"1. Datos personales: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona".*
83
Así pues, de acuerdo con lo previsto en el RGPD, para poder determinar **si estamos en presencia de datos biométricos de carácter personal, deben concurrir los siguientes requisitos** que se deducen de la interpretación conjunta del artículo 4.14 (definición de datos biométricos) y el artículo 4.1 del RGPD (definición de datos personales):

(i) La naturaleza de los datos: deben ser relativos a las características físicas, fisiológicas o conductuales de una persona física.

Si el tratamiento requiere el registro previo de la imagen, huella dactilar, voz, iris,..etc; tiene en cuenta comportamientos, o diferencia características como la raza, sexo…etc, cumple con esta característica inicial, aunque no las almacene y solo las emplee para generar el patrón biométrico.

(i) La finalidad del tratamiento: los datos biométricos deben *permitir o confirmar la identificación única de dicha persona*.

No todos los datos biométricos sirven para la identificación de personas físicas. Pero los sistemas biométricos dirigidos a permitir o confirmar la identificación única de una persona sí tratan datos biométricos de carácter personal.

Las tecnologías biométricas permiten utilizar dos grandes tipos de sistemas biométricos que se dirigen a identificar de manera única a las personas, según señaló el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas de 27/04/2012 del Grupo de Trabajo del Artículo 29, -órgano consultivo independiente europeo en materia de protección de datos, precedente del actual Comité Europeo de Protección de Datos- (en adelante, Dictamen 3/2012):

"-Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios). (En adelante, 1:N)

-Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno)."(En adelante, 1:1).

Si bien esta cuestión ha sido objeto de diversas directrices y dictámenes, lo cierto es que desde la aprobación del RGPD se entiende que las menciones a "permitan" pueden entenderse a la identificación, la de "confirmen" a la autenticación. En ambos casos, sea verificación-autenticación, o identificación las técnicas utilizadas se basan en una concordancia estimada entre plantillas: la que se compara y la(s) de referencia. Desde este punto de vista, son técnicas probabilísticas: la comparación deduce una probabilidad mayor o menor de que la persona sea efectivamente quien se ha de autenticar o identificar; y si esta probabilidad supera un determinado umbral en el sistema, definido por su usuario o su desarrollador, el sistema entenderá que existe una coincidencia.

Pero, con independencia de las diferencias existentes entre ambos sistemas biométricos respecto a la probabilidad de errores, o desde el punto de vista de las medidas de seguridad, lo cierto es que la finalidad de ambas técnicas es la misma, toda vez que ambas se dirigen a identificar de forma unívoca a una persona, considerándose que ambas tratan datos biométricos de carácter personal.

(ii) Los medios y las formas de tratamiento: datos "*obtenidos a partir de un tratamiento técnico específico*"; que "*permitan o confirmen la identificación única de dicha persona*".

Ya desde el Dictamen WP80 del Grupo de Trabajo del Artículo 29 se señalaba que los sistemas biométricos son: «*aplicaciones de las tecnologías biométricas que permiten la identificación automática, y/o la autenticación/comprobación de una persona. Se suelen utilizar aplicaciones de autenticación/comprobación para diversas tareas en campos muy distintos y bajo la responsabilidad de una amplia gama de entidades diferentes*.»

Y todo sistema biométrico dirigido a permitir o confirmar la identificación unívoca de las personas, para poder ser usado, ha de registrar antes la identidad del usuario en el sistema por medio de la captura de una serie de parámetros biométricos en bruto.

Es preciso aclarar que la información biométrica de las personas (sobre las características físicas, fisiológicas o conductuales) puede procesarse y almacenarse de diferentes formas:

a) A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar (muestra) o una grabación de voz. Estas serán un dato personal pero según el artículo 4.14 del RGPD no serán un dato biométrico de carácter personal puesto que no se cumple con el requisito de que el dato biométrico en bruto haya sido procesada mediante un tratamiento técnico que permita su identificación por una máquina a través de un tratamiento automatizado.

Por este motivo, las imágenes de una persona que figuran en un sistema de videovigilancia son datos personales según el artículo 4.1 del RGPD, pero no pueden considerarse datos biométricos de carácter personal (y de categoría especial según nuestro RGPD) si no se han tratado técnicamente de una forma específica con el fin de contribuir a la identificación única de esa persona a través de un sistema. Tal y como lo dispone el Considerando 51 del RGPD también se refiere expresamente a ello, cuando 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."*

Y de la misma forma, la imagen digital o muestras tomadas de una huella dactilar (sea de su totalidad o algunos de sus fragmentos), tampoco se considerarán datos biométricos de carácter personal si no son procesadas para permitir la identificación de la persona a través de un tratamiento técnico específico (que generalmente, es automatizado).

b) Otra opción -la que emplean los sistemas biométricos como el presente- es que esta información biométrica se manifieste en forma de plantilla biométrica o patrón biométrico (código alfanumérico).

En estos casos, la información biométrica bruta capturada es tratada técnicamente por un software de manera que solo se extraen de la misma ciertas características o rasgos (como fragmentos de la muestra de huella o puntos de la imagen de la cara…etc) y se salvan como una plantilla biométrica, llamado "vector" o "patrón biométrico" que permite la identificación de su titular de forma automatizada.

Las Directrices sobre el uso de las tecnologías de reconocimiento facial dictadas por el Consejo de Europa el 28/04/2021 (**Guidelines on Facial Recognition, Council of Europe), definen la plantilla biométrica** como "*una representación digital de las características únicas que se han extraído de una muestra biométrica y se almacenan en una base de datos biométrica".*

Una plantilla biométrica o patrón biométrico es una forma de escritura de una característica biométrica humana, como un rostro o una huella dactilar, que se manifiesta en forma de código alfanumérico, de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados. La plantilla biométrica no está orientada a ser interpretada por una persona, como una fotografía, sino que está orientada a ser tratada en un proceso automatizado, es decir, ser eficiente y eficazmente interpretable por una máquina. Esta forma de almacenamiento permitiría singularizar a un individuo y ejecutar acciones de forma automática, perfilar o inferir información sobre un sujeto como actitudes o patrones de comportamiento, etc.

En otras palabras, la plantilla o patrón biométrico es la forma de medición de las características "físicas, fisiológicas o conductuales de una persona física" que son procesadas para asignar un código identificador único a cada individuo, de forma que éste pueda ser interpretado automáticamente al realizar cada lectura por el software y los dispositivos de hardware asociados a un sistema de verificación/identificación de la identidad biométrico, permitiendo la comparación de los datos y verificación de la identidad de forma automatizada.

En definitiva, según el artículo 4.14 del RGPD, para que exista un tratamiento de datos biométricos de carácter personal se requiere, precisamente, que se aplique sobre la información biométrica tomada en bruto (imagen digital de la huella, cara, grabación de voz…etc) un procesamiento técnico (software o programa como el utilizado en el presente supuesto) del que se obtenga un "patrón biométrico" de las muestras recogidas. Por ello, el patrón biométrico o plantilla biométrica es verdaderamente el dato biométrico de carácter personal al que se refiere el artículo 4.14 del RGPD, puesto que la muestra en bruto de la huella dactilar o la cara, iris, voz…etc de una persona no permite identificar a la misma de forma automatizada.

En consecuencia, siempre que se emplee un sistema biométrico que procese características físicas, fisiológicas o conductuales de las personas en bruto para convertirlas en un patrón o plantilla biométrica que pueda interpretar una máquina de forma automatizada para verificar la identidad de una persona de forma unívoca, no hay duda de que se estarán tratando datos biométricos de carácter personal que están sometidos a las obligaciones que el RGPD establece, siendo considerados de categoría especial, y requiriendo la previa elaboración y superación de una EIPD.

- Características y riesgos del tratamiento de los datos biométricos de carácter personal.

Los sistemas que tratan datos biométricos de carácter personal emplean una tecnología que puede ser realmente intrusiva y requiere de un debate ético y jurídico sosegado, toda vez que puede tener efectos muy adversos en los valores fundamentales y la integridad humana. Véanse solo alguna de sus características especiales y piénsese en el impacto significativo que producen cuando se comprometen estos datos-generando riesgos adicionales en los derechos y libertades de los interesados-, en comparación a cuando se tratan otro tipo de datos de carácter personal:

- Los sistemas biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación. Cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar corresponde con una muestra registrada. Por lo tanto, son únicos, permanentes o definitivos en el tiempo y la persona no puede liberarse de ellos, no se pueden cambiar nunca, ni con la edad, por lo que el daño creado en caso de compromiso-pérdida o intrusión en el sistema es irreparable en este caso. A diferencia de una contraseña, en caso de pérdida, los datos de nuestra huella dactilar o cara no se pueden cambiar.

- Además, debido a que los datos biométricos son propios de una persona y perpetuos, el usuario puede utilizar los mismos datos en diferentes sistemas.

- Mientras que los métodos tradicionales de autenticación como las contraseñas requieren una coincidencia del 100% de carácter por carácter para permitir que el usuario acceda por ejemplo a una cuenta o aplicación (métodos deterministas), los métodos de biometría se denominan “probabilísticos”, porque se basan en la probabilidad de que el usuario que intenta acceder a un determinado dispositivo o aplicación sea la misma persona que el usuario registrado. Podemos medir el rendimiento de un sistema biométrico a partir de tres características principales. Estas son: tasa de falsos rechazos (FRR), tasa de falsas aceptaciones (FAR) y tasa de errores iguales (ERR). La tasa de falsos rechazos representa la probabilidad de errores de detección por parte de un sistema biométrico, lo que significa que no puede reconocer a un usuario cuyas características biométricas ya están en la base de datos. En caso de rechazo, la persona debe verificar su identidad de nuevo. Desde una perspectiva de seguridad y protección, esta tasa no significa que sea necesariamente un resultado negativo. Cada método biométrico, ya sea lectura de cara, de huella dactilar, huella palmar, iris, etc., tiene diferentes valores para diferentes tasas en función de las cuales un sistema rechaza o acepta las entradas.

Por último, cabe señalar que el Dictamen 11/2024 de 23 de mayo de 2024 del CEPD sobre el uso del reconocimiento facial para racionalizar el flujo de pasajeros del aeropuerto recuerda y confirma la necesidad de considerar el elevado nivel de riesgo que conllevan este tipo de tratamientos biométricos y hace hincapié en la necesidad de evaluar sus riesgos e impacto, y en especial, en determinar si existen medios alternativos menos intrusivos para lograr la finalidad de que se trate (verificar la identidad de los alumnos que se presentan al examen en este caso), con menciones

como las siguiente:

> *"Como observación preliminar, el Comité recuerda que el uso de datos biométricos y, en particular, de tecnología de reconocimiento facial conlleva mayores riesgos para los derechos y libertades de los interesados. Se refiere al tratamiento de datos biométricos a los que se concede una protección especial en virtud del artículo 9 del RGPD. Antes de utilizar dichas tecnologías, incluso si se consideraran especialmente eficaces, los responsables del tratamiento deben evaluar el impacto en los derechos y libertades fundamentales de los interesados y considerar si medios menos intrusivos pueden alcanzar su finalidad legítima del tratamiento".*

3.2. Los datos biométricos de carácter personal como de categoría especial y alto riesgo.

Tal y como se ha señalado, de acuerdo con el artículo 4.14 del RGPD (en relación con el artículo 4.1 del RGPD) son datos biométricos de carácter personal todos aquellos que: (i) sean relativos a las características físicas, fisiológicas o conductuales de una persona física; (ii) su finalidad sea la de permitir o confirmar la identificación única de una persona física (incluyendo sistemas de autenticación 1-1 e identificación 1-N); (iii) y que se sometan a un tratamiento técnico específico dirigido a permitir o confirmar la identidad unívoca de las personas de forma automatizada (que de lugar a la generación, archivo, explotación y destrucción de plantillas biométricas obtenidas de las muestras del dato capturado en bruto).

Tras la aprobación del actual RGPD, y a diferencia del régimen aplicable con anterioridad al mismo, siempre que se realice un tratamiento de datos que sean biométricos de carácter personal de acuerdo con la definición del artículo 4.14 del RGPD, estos serán: (i) considerados como datos personales de categoría especial según el artículo 9 RGPD, cuyo tratamiento está prohibido de forma general si no se dispone de una de las excepciones reguladas en dicho precepto (ii) y el tratamiento de los mismos será considerado de "alto riesgo" según el artículo 35 del RGPD.

Hay que tener presente que la evolución tecnológica en esta materia está avanzado a un nivel agigantado e imparable, máxime en los últimos años en la que la tecnología biométrica puede combinarse con técnicas de inteligencia artificial. La regulación anterior al actual RGPD databa del año 1995, donde todavía no se aplicaban tecnologías biométricas en el ámbito de la identificación de las personas. Por ello, la anterior "Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respeta al tratamiento de datos personales y a la libre circulación de estos datos" no hacía referencia alguna al concepto de datos biométricos. Únicamente se contenía una definición de lo que se consideraba como dato personal en el artículo 2 de la Directiva. Y al no existir entonces los datos biométricos, tampoco se incluían entre las categorías especiales de datos personales cuyo tratamiento estaba prohibido -con excepciones- por el anterior artículo 8.
En este sentido, hay que tener en cuenta que la **aprobación del RGPD ha supuesto un cambio de paradigma** en materia de protección de datos personales que pretende

garantizar aún más a los ciudadanos el control de sus datos personales, estableciendo unos estándares de protección elevados y adaptados al entorno digital en que vivimos.

Esto es, siempre que se traten datos de carácter personal, de cualquier tipo que sean, el responsable deberá cumplir con los principios y obligaciones previstos en la normativa de protección de datos para todo tipo de datos personales.

Pero cuando los datos personales a tratar sean biométricos cuya finalidad sea la identificación unívoca de las personas, se debe considerar además que -a diferencia de lo que sucedía bajo el régimen anterior al RGPD- desde la entrada en vigor del RGPD el 25 de mayo de 2018 según su artículo 9, los datos biométricos de carácter personal que encajen en la definición del artículo 4.14 del RGPD están considerados como **datos personales de categoría especial** según lo previsto en artículo 9 del RGPD, cuyo tratamiento está generalmente prohibido, salvo que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD. Lo que no exime de que siempre deba existir además una base de licitud prevista en el artículo 6 del mismo, entre otros muchos requisitos y principios que deberá cumplir aquel que decida optar por este tipo de tratamientos.

Así pues, de acuerdo con el artículo 9.1 del RGPD, queda prohibido el tratamiento de datos biométricos cuando sean: "*datos biométricos dirigidos a identificar de manera unívoca a una persona física*".

Es necesario recalcar que la calificación de los datos biométricos como datos de categoría especial implica, necesariamente, la observancia de una especial cautela por el responsable a la hora de determinar si es posible llevar a cabo un tratamiento de datos de esta naturaleza. Entre otras cosas, y además de existir una excepción que permita salvar la prohibición del artículo 9.1 del RGPD, de que exista una base de licitud del artículo 6 del RGPD y de que se cumplan los principios del RGPD, el sujeto que pretenda implantar sistemas de datos biométricos, (en este caso, SIDECU) debería haber analizado previamente la concurrencia de los preceptivos criterios de necesidad, idoneidad y proporcionalidad del tratamiento.

Esto es, quien pretenda instaurar un tratamiento de datos personales de esta naturaleza debe, antes que nada, asegurarse de que se supere lo que se ha denominado en la jurisprudencia como "el triple juicio de proporcionalidad", planteándose en especial si el tratamiento de datos biométricos es idóneo, proporcionalidad, y sobre todo, necesario. Si existen otros sistemas no biométricos que permitan conseguir la misma finalidad de identificar-verificar la identidad de las personas con eficacia y seguridad, no será necesario iniciar tratamientos biométricos, y, por tanto, implantar este sistema se considerará contrario al RGPD. Este juicio debe ser el punto de partida de su análisis, pues sólo en caso de que estos métodos superen el citado triple juicio, se exigirá el cumplimiento de otros requisitos o garantías.

Por otra parte, además de ser datos de categoría especial, el **tratamiento de datos biométricos se considera de siempre alto riesgo** a tenor de lo previsto en el apartado 4 del artículo 35, que dispone que "*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", dado que consta entre los tratamientos incluidos en la Lista de tipos de tratamiento de datos que requieren evaluación de impacto relativa a la protección de datos, hecho público por la AEPD en desarrollo de la previsión contemplada en el apartado cuarto del referido artículo 35.

No hay duda del carácter de alto riesgo de los datos biométricos, habida cuenta de que todos los datos biométricos que se dirijan a identificar de manera unívoca a una persona cumplen con al menos dos de los 3 criterios contenidos en dicha lista, puesto que le son aplicables los correspondientes a los números 4, 5 y 10 de dicho documento (aquellos que impliquen el uso de categorías especiales de datos; el uso de datos biométricos y los que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas).

Por tanto, desde la entrada en vigor del RGPD, cuando un tratamiento es de "alto riesgo", como sucede con los métodos de control de presencia o acceso basados en métodos de fichaje biométricos, **es obligatorio realizar siempre una evaluación de impacto (EIPD), de acuerdo con lo previsto en el artículo 35.1 del RGPD**, debiendo esta EIPD ser previa al inicio del tratamiento, pero realizarse a su vez de forma continua. Y no bastará con realizarla, sino que la misma deberá considerarse válida, porque cumpla con los requisitos previstos en el citado artículo, en especial, que contenga como mínimo la información del art. 35.7 del RGPD, que señala lo siguiente:

"*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".*

En conclusión, el responsable que trate datos biométricos de carácter personal deberá ser consciente de que este tratamiento está calificado como un tratamiento de alto riesgo que requiere la previa elaboración y superación de una EIPD, que cumpla con todos los requisitos previstos por el citado artículo 35 del RGPD, y que está tratando datos de categoría especial, por lo que deberá justificar que concurre una de las excepciones del artículo 9.2 del RGPD, antes de iniciar o continuar con dicho tratamiento. Lo que se producirá, con carácter general, tanto cuando se empleen métodos de identificación basados en sistemas de detección de huella dactilar como los basados en sistemas de reconocimiento facial.

3.3. Análisis del supuesto presente: tratamiento realizado por el nuevo sistema de registro de jornada implantado.

3.3.1. Datos personales objeto de tratamiento.

En el presente supuesto, consta acreditado que la empresa reclamada SIDECU es gestora y propietaria de la cadena de gimnasios Supera, que dispone de varios centros deportivos situados en el territorio nacional y fuera de éste, de acuerdo con lo que se ha hecho constar en la Diligencia de 2-4-25.
En relación con el presente procedimiento, se han presentado un total de 9 reclamaciones contra la implantación del nuevo método de acceso mediante reconocimiento facial a 5 centros deportivos SUPERA gestionados por SIDECU (Entrepuentes de Sevilla, San Diego de Coruña, La Lanera de Palencia, Palero Superior de Valladolid, y Guadalquivir de Sevilla), así como 2 denuncias contra el sistema presentadas por FACUA y un particular.

SIDECU ha presentado 3 escritos de contestación a los traslados de las reclamaciones que se le han realizado por esta Agencia, así como un escrito de respuesta al requerimiento de información realizado por el inspector durante la fase de actuaciones previas de investigación. Y ha reconocido los siguientes hechos:

- En primer lugar, que ha implantado un nuevo método de acceso en 5 de sus centros deportivos basado en el software de reconocimiento facial desarrollado por ***EMPRESA.1, y que previamente a este sistema, implantó un método de acceso basado en la detección de huella dactilar que vino a sustituir el anterior de acceso mediante tarjeta identificativa. Incluso manifiesta haber habilitado a raíz de las reclamaciones presentadas en el centro de Entrepuentes de Sevilla un método de acceso mediante exhibición de DNI.

  Así pues, en su 1ª Respuesta al traslado de las reclamaciones, SIDECU, manifiesta que:

  > "*Con anterioridad al uso de este sistema de acceso los centros deportivos tenían instalados unos sistemas que también utilizaban complejos algoritmos matemáticos desarrollados por el fabricante NITGEN, en los que el usuario accedía a través de su huella dactilar, pero sin que, en ningún caso, el sistema pudiera almacenarla. Se trataba de un sistema similar al utilizado en la actualidad, pero el análisis de la plantilla numérica se realizaba por medio de la huella dactilar en vez del reconocimiento facial. (…)*
  > *Sin embargo, el sistema presentó fallos de funcionamiento en el acceso (fallos mecánicos frecuentes, en todo caso), lo que motivó a SIDECU a buscar otro sistema que fuese similar y no invasivo o intrusivo en los derechos de los usuarios y, en particular, que no tratase datos o almacenase datos de los usuarios.*
  > *Así, se obtuvo diferente información acerca de diferentes sistemas biométricos, optando SIDECU por el sistema de la empresa ***EMPRESA.1 y realizando un análisis de riesgos previamente a su adquisición. Conforme a las explicaciones detalladas por el fabricante, este sistema no almacena la imagen procesada del individuo como si ocurre en otro tipo de registros, no realizando pues tratamiento de datos personales.*

- En su 2ª Respuesta, contestando al requerimiento de información durante la fase de investigación, SIDECU amplía información, señalando que*: "Actualmente el referido sistema de reconocimiento facial se encuentra instalado en cinco centros deportivos, siendo el número total de usuarios de dichos centros de 36.483. Uno de esos centros es el de Entrepuentes de Sevilla, el cual cuenta actualmente con 8.978 usuarios (a fecha 4/01/2024).* De estos *usuarios del centro deportivo Entrepuentes un total de 26 usuarios han manifestado su oposición al sistema de acceso, habilitándose por parte de SIDECU una alternativa de acceso mediante identificación en la recepción del centro mediante la exhibición del Documento Nacional de Identidad al personal de dicho centro deportivo y la apertura manual del tomo de acceso".*

- De acuerdo con lo que se hace constar en las Diligencias de 30 de abril de 2024 y 13 de marzo de 2025, la entidad con la que la empresa reclamada dice haber contratado la implantación del nuevo método de acceso a los centros deportivos mediante reconocimiento facial es *****EMPRESA.1,** que ha venido a sustituir al anterior de acceso mediante huella dactilar de **NITGEN**, de acuerdo con la información publicada en su sitio web (***EMPRESA.1.inc.com/es), oferta entre sus productos lectores biométricos y es especialista en desarrollar e implantar varios métodos de acceso que emplean técnicas de identificación basadas en el reconocimiento facial (******APP.2*** y ******APP.3***), además de ofertar métodos de acceso basados en la detección de huella dactilar (******APP.1***), que son compatibles con las tarjeta identificativas (tarjeta RFID).

- No obstante, la empresa reclamada no ha aportado los contratos suscritos con ***EMPRESA.1 para el suministro de este software de reconocimiento facial ni el previamente suscrito con NITGEN para el sistema de acceso mediante huella dactilar, ni aporta documentación acreditativa alguna al respecto.

  La reclamada no ha concretado tampoco cuáles fueron las fechas de implantación/puesta en marcha de cada método de acceso en los centros, y durante cuánto tiempo han coexistido en el tiempo, no habiéndose concretado cuál ha sido el ciclo de vida del tratamiento realizado por la reclamada con la finalidad de controlar el acceso de sus socios a sus centros. También manifiesta la reclamada que ha colocado carteles informativos en los 5 centros y aporta sus fotografías, pero no señala cuando, y en las fotografías no aparece fecha alguna de la que pueda deducirse cuando fueron difundidos en cada centro.

  No obstante, centrando el objeto del presente procedimiento en el sistema de reconocimiento facial frente al que se han presentado todas las reclamaciones y denuncias que forman parte del expediente, si existen evidencias de que este nuevo sistema de reconocimiento facial se implantó, al menos desde julio- agosto de 2023 y que permanece en la actualidad:

  - Las 9 reclamaciones y las dos denuncias se han presentado ante esta Agencia entre el 4/8/23 y 16/09/24.

  - La empresa aporta el intercambio de correos mantenido con los 9 reclamantes, en los que se observa que los primeros correos electrónicos remitidos por los mismos en relación con este nuevo sistema datan del

mes de agosto de 2023 en adelante.

- La reclamación presentada por ***C.C.C.***, señala que hasta "aproximadamente julio de 2023", el procedimiento de acceso a las instalaciones del centro de Entrepuentes ha sido mediante un torno controlado por tarjeta magnética y un sistema biométrico de reconocimiento de huella dactilar, y que a partir de entonces se instaló el nuevo método de acceso por reconocimiento facial sin que se informase a los socios sobre su utilización, por lo que estuvo siendo utilizado como sistema alternativo hasta que la empresa decidió implantarlo como método obligatorio para todos los socios, desactivando los métodos anteriores.

- Y por otra parte, la presentada por ***F.F.F.,*** señalando que el "*En el Centro de Deporte y Ocio La Lanera de Palencia se ha implantado un sistema de acceso mediante el sistema de análisis biométrico facial (llevando ya instalado unos 10 años también el acceso mediante tarjeta y detección de huella). El análisis biométrico facial se ha realizado a los usuarios sin informarles en absoluto del riesgo de los datos que están aportando y sin un consentimiento escrito de ello*".

- Por otra parte, al contestar al requerimiento de información realizado por el inspector (escrito de 19/01/24), la empresa señala que no ha elaborado una Evaluación de Impacto del Tratamiento, por considerar que no trata datos personales de categoría especial, y aporta los siguientes documentos:

  - Como documento nº3. Hoja de registro de eventos por el programa ***EMPRESA.1. Donde se observan los siguientes tipos de datos que se captan al registrar la entrada al centro:

    FECHA/ PUERTA/ ID-DISPOSITIVO/TORNO ENTRADA/ GRUPO USUARIO(centro entrepuentes)/ USUARIO (códigos numéricos)/EVENTO (en todos aparece: Auntenticación 1:N (Cara).

  - Como documento nº 6, copia del Registro de Actividades del Tratamiento de GRUPO SIDECU, cuyo apartado 5 relativo al tratamiento de los datos personales de los clientes(abonados) en el que como fines del tratamiento se indica la "gestión de la relación con los clientes o potenciales clientes". En la sección de categorías de datos tratados no se mencionan datos biométricos.

  - Como documento nº 5 dice aportar el análisis de riesgos realizado.

    Se trata de un documento de 2 páginas, fechado el 2-9-22 y realizado por SUPERA, que se titula "ANÁLISIS DE RIESGOS PREVIO A UNA EIPD", que no contiene un apartado de descripción ni de finalidad del tratamiento, sino que se refiere a:

    "FECHA. 2-9-22

INICIATIVA: Implantación de sistemas de reconocimiento facial de ***EMPRESA.1 para el acceso a los centros deportivos de GRUPO SUPERA".
MOTIVACIÓN: Innovación en los sistemas de acceso a los centros deportivos de SUPERA como consecuencia de los fallos de seguridad existentes…

DATOS PERSONALES OBJETO DE TRATAMIENTO: Se marca NO.
CONCLUSIÓN:

*Según la información facilitada por el fabricante, la implantación del sistema de reconocimiento facial fabricado por ***EMPRESA.1 no supone ningún tratamiento de dato personal para los usuarios de los centros deportivos que accedan al mismo.*
El sistema genera una plantilla a partir de la imagen del usuario (la primera vez que accede) que no asocia a ninguna persona en particular, sino que simplemente analiza si el usuario que accede tiene o no derecho a ello.
*En particular, los datos extraídos por los lectores de ***EMPRESA.1 no podrían ser en ningún caso desencriptados ni desmontados, estando únicamente en posesión del fabricante las claves para el algoritmo, sin que se almacenase ningún tipo de información sobre la imagen de los usuarios.*
El sistema de reconocimiento facial tampoco se conecta a la base o listado de usuarios de los centros deportivos en ningún momento.
Se aporta al presente informe el certificado emitido por el fabricante a tal efecto.
En definitiva, no procede realizar ninguna Evaluación de Impacto al no existir tratamiento de datos al no poderse, en ningún caso, recuperar la imagen personal del usuario, ni siquiera deducir características físicas concretas de la misma, no pudiendo identificar a la persona.
Se acuerda poner a disposición de los usuarios carteles informativos que informen acerca del nuevo sistema implantado y de sus características.
Al no existir tratamiento de datos, ni poder ser considerado como tratamiento de categoría especial, tampoco procede recabar previamente el consentimiento del usuario. En cualquier caso, se podrá poner a disposición de los usuarios alternativas de acceso en los casos en los que se nieguen a utilizar este sistema.
En definitiva, se deduce que el sistema propuesto no resulta intrusivo ni atenta contra los derechos de los usuarios de los centros deportivos al no tratar ni almacenar su imagen personal ni ningún otro dato que permita identificarlos."

- La única documentación técnica que hace referencia a las características, y funcionamiento del software de reconocimiento facial contratado con ***EMPRESA.1 son los certificados que aporta SIDECU de forma reiterada, en sus cuatro escritos de respuesta. Se trata de dos certificados emitidos por ***EMPRESA.1, en los que no consta fecha ni firma, redactados en inglés, que son los siguientes:

1. Certificado de cumplimiento del RGPD, referido al funcionamiento y características técnicas de los sistemas de detección de huella dactilar y reconocimiento facial desarrollados por ***EMPRESA.1.

1. Certificado de Protección de Datos Faciales, centrado en el funcionamiento y características técnicas del sistema empleado para el reconocimiento facial, cuya publicación en el sitio web de ***EMPRESA.1 en castellano ha sido unida al procedimiento mediante Diligencia del inspector, expedida el 2 de noviembre de 2023.

- Y por último, es de relevancia la información contenida en la respuesta dada a la reclamación del **C.C.C.**, en la que al contestar sobre la supuesta filtración de datos de la base de datos de ***EMPRESA.1, la reclamada informa de que almacena las plantillas biométricas en sus servidores informáticos: *"Les informamos que tras consultarlo con el fabricante y analizar los sistemas implantados, no es posible que ninguna supuesta filtración haya afectado a las plantillas correspondientes los usuarios de nuestros centros deportivos, por cuanto éstas se guardan en nuestros propios servidores informáticos (dotados de los oportunos sistemas de seguridad), sin que en ningún caso la compañía suministradora de los equipos de acceso biométrico haya podido tener acceso a los mismos".*

Una vez expuestos todos los datos que la reclamada, y reclamantes han aportado acerca de la implantación del nuevo método de acceso de estos centros deportivos, la **cuestión controvertida principal del procedimiento estriba en determinar cuál es la naturaleza jurídica de los datos** que trata el software de reconocimiento facial ***EMPRESA.1 (******APP.2/***APP.3***) empleado para realizar la identificación de los socios que acceden a los 5 centros deportivos de la reclamada en la actualidad.

En los 4 escritos presentados ante esta Agencia y en todas las respuestas a las reclamaciones de los socios que se han aportado a este procedimiento, SIDECU niega que el software de reconocimiento facial empleado actualmente para permitir el acceso de sus socios trate datos biométricos personales de categoría especial, en incluso, que trate datos personales de ningún tipo, en base a la siguiente argumentación:

- En su primera contestación al traslado de las tres primeras reclamaciones presentadas ante esta Agencia, SIDECU explica los motivos por los que entiende que "según les ha explicado el fabricante" el software ***EMPRESA.1 de reconocimiento facial no trata datos biométricos de categoría especial, ni tampoco datos personales, y que por ello entiende que no genera ningún riesgo, y que no deben cumplirse los requisitos previstos en la normativa de protección de datos personales. En términos literales:

  "Si bien es cierto, que en la documentación de alta de usuario no aparece contemplada la autorización para la recogida de datos personales relativos al uso de datos biométricos o de categorías especiales, ello es debido a que, atendiendo a las características del funcionamiento del sistema de acceso, no solo no se guarda la imagen de los usuarios por parte de SIDECU, S.A. como teórico responsable del tratamiento, sino que no se

conserva ningún tipo de dato personal, pues la plantilla generada por el sistema no permite la asociación a ninguna persona concreta.

Tal y como señaló esa Agencia Española de Protección de Datos en su Informe 36/2020, no se trata de un tratamiento de datos como tratamiento de categoría especial, pues no identifica, en ningún caso, de manera unívoca a una persona física.

Los CENTROS SUPERA únicamente acceden a registros de entrada y salida y presencia en las instalaciones obteniendo exclusivamente información correspondiente a las horas y número de personas, pero no a su identificación personal.

*Asimismo, el segundo ordinal del artículo 4 del RGPD, señala que se entenderá por "tratamiento" de datos: "Cualquier operación o conjunto de operaciones realizadas sobre datos personales 0 conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción . Es por dicha razón que no puede entenderse como tratamiento de datos personales el caso que nos ocupa, pues no se encuentra dentro de la categoría de los mismos. Reiteramos que, a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno. La generación de las plantillas mediante los complejos algoritmos matemáticos desarrollados por ***EMPRESA.1 no permite que el sistema guarde la imagen ni que la plantilla generada se asocie a usuarios concretos, por lo que no puede existir tratamiento de datos si éstos no se someten a ninguna de las operaciones recogidas en el artículo antes referido.*

El funcionamiento de este sistema queda al margen de la aplicación del artículo anteriormente mencionado del RGPD, ya que, en ningún caso, puede someterse al cumplimiento de lo dispuesto por la normativa en materia de protección de datos a un sistema de mero control de acceso que no trata dato personal alguno, pues ni los recoge, ni los conserva, ni permite la identificación de las personas.

En consecuencia y al no existir ningún tratamiento de datos personales, no resulta pues aplicable el contenido de la normativa relativa a protección de datos personales ni, por ello, el deber de notificación de tratamiento de datos, motivo por el cual nuestra entidad no ha procedido previamente a solicitar su consentimiento para el uso de su imagen pues, como indicamos, no se trata ni almacena en ningún caso."

- En el escrito de 19/01/24 contestando al requerimiento de información realizado durante la fase de investigación, al describir el funcionamiento técnico del programa, se insiste en que el sistema no almacena la imagen, y se señala que el

algoritmo NIR patentado por el fabricante obtiene un “modelo numérico que funciona como una clave propia de cada usuario con la finalidad de acceso a las instalaciones”, y “plantilla que funciona como una clave alfanumérica” sin ser consciente de que ésta es la plantilla biométrica que se considera el verdadero dato biométrico personal, en lugar de la imagen.

No obstante, contrariamente a lo que mantiene la reclamada, lo que realmente se deduce de la documentación técnica de la fabricante es que el software de reconocimiento facial desarrollado por ***EMPRESA.1 trata datos biométricos personales considerados como de categoría especial por el artículo 9.1 del RGPD.

Es de señalar que los certificados del fabricante, que están redactados en inglés, se describe lo que es un sistema de procesamiento biométrico común, al que se aplica un algoritmo que genera plantillas biométricas y las almacena, sin almacenar las imágenes de las que toma la muestra, y otras herramientas criptográficas que cifran posteriormente las plantillas biométricas de los socios. Pero en ningún caso se afirma en estos certificados que el sistema no trate datos personales de ningún tipo, como alega la reclamada.
A la vista de los dos certificados aportados, no cabe duda de que al emplear el software de reconocimiento facial desarrollado por ***EMPRESA.1 como método de identificación de los socios que acceden y salen de las instalaciones de sus centros deportivos, SIDECU está tratando los datos biométricos personales de los socios que emplean dicho método de acceso, puesto que se cumplen los 3 requisitos que establece el artículo 4.14 del RGPD:

1. En primer lugar, los datos que el programa utiliza para realizar las comprobaciones de identidad se basan en características físicas, fisiológicas o conductuales de una persona física.

   La propia empresa reclamada reconoce que estuvo utilizando durante un tiempo un programa como método de identificación de las personas que acceden a sus centros deportivos basado en la lectura de la huella dactilar de los socios, y, que posteriormente y ante los fallos de funcionamiento detectados, ha contratado e implantado un método de acceso a 5 de sus centros deportivos basado en la identificación mediante reconocimiento facial, que requiere la lectura del rostro de los socios para poder ser identificados y permitirles dicho acceso. Por lo que no cabe duda de que ambos métodos, el anterior y el actual, tratan datos personales basados en rasgos biológicos de los socios.

   Centrándonos en el actual sistema de reconocimiento facial cuya implantación ha sido objeto de las reclamaciones que dan origen al presente procedimiento, el certificado de protección de datos faciales de SUPERA no deja lugar a dudas, como veremos seguidamente al transcribirlo, que el sistema obtiene un patrón facial a partir de una muestra que se obtiene de los puntos de los extremos de la cara.

2. En segundo lugar, de la documentación aportada se desprende también que la finalidad del sistema de reconocimiento facial (al igual que los anteriores de huella dactilar/tarjetas magnéticas) es “la identificación de los socios que entran

/salen de los centros deportivos al objeto de permitirles acceder a los mismos" (o lo que es lo mismo, en palabras del artículo 9 del RGPD, la identificación unívoca de los socios).

En el presente supuesto, al contestar a requerimiento de investigación SIDECU manifiesta que el software empleado para realizar el reconocimiento facial se basa en un sistema de identificación de 1 a varios (1-N), por lo que no hay duda alguna de que se dirigía a identificar de forma unívoca a los socios que tienen acceso al club.

Y al describir el funcionamiento de ***EMPRESA.1 señala que: *"el sistema analiza puntos concretos de la imagen del individuo y crea un modelo numérico que funciona como una clave propia de cada usuario con la finalidad de acceso a las instalaciones.", y "Así, el proceso posterior de identificación de la persona consiste en que, tras ponerse el usuario delante del sistema de reconocimiento facial, éste crea una nueva plantilla que se compara con las ya almacenadas. Si esta operación genera un resultado positivo, se considera al usuario correctamente identificado y se permite el acceso al centro deportivo".*

Ello se deduce así mismo del documento nº3 que fue aportado por la misma junto con tal escrito: Hoja de registro de eventos por el programa ***EMPRESA.1. Donde se observan los tipos de datos que se captan al registrar la entrada al centro, en el que aparece como evento registrado en todos los casos: Autenticación 1:N (Cara). Así como, del proceso de identificación que describen los certificados del fabricante a los que se hará referencia seguidamente.

3. En tercer lugar, porque el software de reconocimiento facial (***APP.2/***APP.3) de ***EMPRESA.1 que ha contratado para servir de método de identificación de los socios que accedan a sus centros deportivos realiza un procesamiento técnico de las imágenes en bruto obtenidas de los socios (fotografía de la cara), mediante el que se *extrae los puntos de datos faciales de las imágenes captadas en bruto y se crea una plantilla biométrica o patrón facial a partir de estos datos*. Patrón facial que se genera y que se almacena para realizar cada lectura o comprobación de identidad que se realiza cada vez que se registra la entrada y salida del centro utilizando los dispositivos de reconocimiento facial instalados por la empresa.

   Ello se deduce claramente de la documentación técnica del fabricante en los que ***EMPRESA.1 certifica que el software empleado genera una plantilla o patrón biométrico en forma de código identificador de cada socio, que se encripta y almacena:

   - Por una parte, el "GDPR Compliance Statement" (Certificado de cumplimiento del RGPD), emitido por ***EMPRESA.1, señala expresamente que durante el proceso de registro se genera una plantilla (template) de la cara/huella que no se guarda en el servidor o en el dispositivo directamente. Sino que la plantilla se crea, y se encripta en base a un algoritmo diferente en función de donde va a ser almacenada (en el servidor, dispositivo, o smartcard), que son los diferentes medios que

permite adquirir la fabricante de acuerdo con lo que consta en los servicios ofertados en su página web según la Diligencia expedida en el presente procedimiento.

(…) Each element of sensitive data handled by the ***EMPRESA.1 system is protected by the following mechanisms:

- Fingerprint / Face templates: During the process of enrollment, the raw image of the fingerprint / face is never stored in the device or server. Instead, a template is created, which is also encrypted by 128bit AES, 256bit AES, DES/3DES depending on the location where it is stored (Device, Server, SmartCard).

(Traducción al español por esta Agencia):

*"Cada elemento de datos sensibles manejados por el sistema ***EMPRESA.1 está protegido por los siguientes mecanismos:*

- *Plantillas de huellas dactilares / caras:*

*Durante el proceso de inscripción, la imagen en bruto de la huella digital / cara **nunca** se almacena en el dispositivo o servidor. En su lugar, se crea una plantilla, que también está encriptada por AES de 128 bits, AES de 256 bits, DES/3DES dependiendo de la ubicación donde se almacene (Dispositivo, Servidor, SmartCard).*

o Y por otra parte, en el "Face data protection certificate" (Certificado de protección de datos faciales), se detalla exactamente como se produce el proceso de generación, almacenamiento del patrón facial o plantilla, así como el proceso de comparación realizado para verificar la identidad:

La versión original aportada indica que:

"***EMPRESA.1 Inc(hereafter ***EMPRESA.1), certify that ***EMPRESA.1 ***APP.2 extracts the face data points from the raw images and create a template from this data and does not keep the raw images in the device.*

*The face template is not a raw image. It is created by using ***EMPRESA.1's patented NIR technology and algorithm, and the face template is a dataset which is a fusion of 2D and 3D feature of a user's face which is acquired by a visual camera and NIR camera. In order to secure this template, cryptographic tools and encryption methods are used such as 256bit AES encryption making it very difficult to access the necessary data to reverse engineer the process. The ability to reduplicate the original image and prove the identity via a face recognition expert is not possible.*

****APP.2 also calculates a matching score when executing an authentication. The matching score is a calculation of the match between a pre-registered face template and the actual face to be authenticated. The matching score helps protect ***APP.2 against spoofing. ***EMPRESA.1 also certifies that FAR(False Acceptance Rate) and FRR(False Rejection Rate) in face recognition algorithm in ***APP.2 are as below.*

► *FRR: Less than or equal to 1%* ► *FAR: Less than or equal to 0.00002% (1/5,000,000."*

Mediante diligencia del inspector de 12 de diciembre de 2023 se refleja la versión en español de este mismo certificado que se halla publicada en el sitio web de ***EMPRESA.1, que coincide con el aportado por la reclamada en inglés:

*"***EMPRESA.1 Inc., (en adelante ***EMPRESA.1), certifica que ***EMPRESA.1 Face Station 2 y ***APP.3 extraen los puntos de datos faciales de las imágenes en bruto y crean una plantilla a partir de estos datos.*
*La plantilla de rostro no es una imagen en bruto. Se crea utilizando la tecnología y el algoritmo NIR patentados de ***EMPRESA.1. La plantilla de la cara es un conjunto de datos que se obtiene de la fusión de las características en ZD y 3D del rostro de un usuario. adquiridos a través. de una cámara visual y una cámara NIR… Para asegurar esta plantilla, se utilizan herramientas criptográficas y métodos de encriptación. como AES de 256 bits. lo que dificulta el acceso a los datos necesarios para realizar ingeniería inversa en el proceso. La capacidad de duplicar la imagen original para luego tratar de autenticar suplantando identidad de un usuario en un reconocimiento facial experto no es posible.*
****APP.2 y ***APP.3 también calculan una puntuación de coincidencia al ejecutar una autenticación. La puntuación de coincidencia es un cálculo entre una plantilla de cara previamente registrada y la cara actual que se pretende autenticar.(…)*
****EMPRESA.1 también certifica que el FAR (Tasa de Falsa Aceptación — False Acceptance Rate por sus siglas en inglés) y FRR (Tasa de Falso Rechazo - False Rejection Rate por sus siglas en inglés), en el algoritmo de reconocimiento facial en ***APP.2 y ***APP.3 son los siguientes:*
FRR: Menor o igual al 196 — FAR; Menor :— igual al 0.00002% (1/5,000.000)(…)"

A la vista de las evidencias aportadas, no cabe duda de que la reclamada ha interpretado erróneamente la documentación técnica o instrucciones del fabricante del software de reconocimiento facial así como el contenido del informe número 0036/2020 del gabinete jurídico de esta Agencia que cita en sus respuestas, que fue dictado en relación con el expediente E/05454/2021 de fecha 27 de julio de 2021, con ocasión de una consulta realizada sobre el uso de datos biométricos por parte de universidades e instituciones educativas (reconocimiento facial como método de evaluación de los alumnos), realizando un análisis del concepto y algunos de los requisitos de los datos biométricos de categoría especial del artículo 9.1 del RGPD que habían sido objeto de consulta.

A la vista de las manifestaciones realizadas, se observa que la reclamada ha llegado a la conclusión de que este software no trata datos biométricos de categoría especial, porque parte de varias premisas erróneas:

- Primero, al entender que el dato biométrico personal (de categoría especial) al que se refiere el artículo 4.14 del RGPD es sólo la imagen de la cara de los socios o abonados, en lugar de considerar también la plantilla biométrica o patrón facial que se genera por el programa.

  La argumentación de la empresa se ha basado principalmente en entender que el dato biométrico personal al que se refiere el artículo 4.14 del RGPD es la imagen de la cara obtenida en bruto (información biométrica en bruto), y no la plantilla biométrica (patrón facial extraído de varios puntos de la imagen de la cara), por lo que al no almacenarse las imágenes, considera que no está tratando datos biométricos de categoría especial. Cuando es precisamente al revés, puesto que como ya se ha explicado en el Fundamento de Derecho 3.1 es la plantilla/patrón facial la que es el dato biométrico de categoría especial, y no la imagen (ni los fragmentos tomados de la misma).

  Para argumentar que ***EMPRESA.1 no trata datos biométricos de carácter personal, la parte reclamada describe el funcionamiento del programa sin percatarse de que está describiendo lo que es un sistema de procesamiento biométrico que genera, almacena y explota una plantilla biométrica para realizar la identificación de los socios que acceden a su centro, que cumple con las 3 características y requisitos del artículo 4.14 del RGPD (y por ende, del artículo 9.1 del RGPD).

  Y por ello, tal y como se ha aclarado en el apartado 3.1 de este acuerdo, siempre que se emplee un sistema que genera este patrón facial o plantilla biométrica que se utiliza para verificar la identidad de las personas que acceden/salen de un recinto, se cumplirán los requisitos del artículo 4.14 del RGPD, y del artículo 9.1 del RGPD, lo que es el caso planteado en este supuesto.

- En segundo lugar, entiende erróneamente que el código alfanumérico que genera el sistema (plantilla o patrón facial) no es un dato personal de acuerdo con la definición del artículo 4.1 del RGPD, toda vez que "a *partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma".*

  Señala la reclamada que: "Según la información que nos transmitió el fabricante, se crea un modelo con el algoritmo NIR, patentado por este fabricante, que utiliza algoritmos matemáticos complejos, generando un modelo numérico al usar información de alguno de los puntos de la captura. En ningún momento puede deducirse de este modelo características físicas de la persona.(…) Asimismo, a partir de las plantillas no se puede, en ningún caso, recuperar la imagen personal del usuario ni siquiera deducir características físicas concretas de la misma. No hay pues tratamiento de dato personal alguno".

  No obstante, como se ha dicho anteriormente, el hecho de que no se pueda reconstruir la imagen de la huella (información biométrica en bruto) a partir de la muestra capturada por los dispositivos para generar el patrón biométrico, es habitual en los sistemas de procesamiento de datos biométricos, así como no

almacenar las imágenes originales completas, pero ello no implica que: (i) no se traten datos biométricos de carácter personal, puesto que se genera y almacena un patrón biométrico, aunque no se almacene la imagen de la cara; (ii) ni tampoco implica que no pueda ser descifrada la identidad del titular de la cara como alega la reclamada, puesto que el patrón biométrico permite singularizar a un individuo y verificar que es él y sólo él, a través de "*elementos propios de la identidad física, fisiológica, genética, psíquica*" que se manifiestan bajo la forma de un código alfanumérico, y este código es susceptible de ser descifrado por un sistema automatizado, sin necesidad de disponer de la muestra o dato en bruto de la huella.

Lo que plantea la reclamada es necesario en los sistemas tradicionales de verificación manual o presencial realizados persona-persona (por ejemplo, mediante la comprobación de su DNI por el personal de la empresa), en los que si es necesario comparar imágenes, por lo que sería necesario conocer las características físicas de la persona para comprobar su identidad por otra persona. Pero ello no es necesario en el caso de sistemas biométricos automatizados, puesto que los dispositivos (máquina) que se encargan de verificar la identidad no analizan imágenes, sino los códigos que se han obtenido al procesar estas imágenes previamente.

Por ello, decíamos que es del todo indiferente que este código numérico no se pueda revertir para obtener la imagen de la persona a quien pertenece, puesto que el sistema no precisa la imagen para poder conocer quién ha accedido al centro. Este código que es la plantilla permite identificar a la persona "indirectamente" (comprobando a qué socio pertenece cada código), por lo que es sin duda un dato personal a los efectos del artículo 4.1 del RGPD, además de ser un dato biométrico personal de categoría especial, como ya se ha dicho.

- En tercer lugar, el argumento del cifrado de la plantilla biométrica como motivador para justificar que el código numérico cifrado no es un dato personal, tampoco es válido.

  Por último, señala la reclamada al argumentar que no hay tratamiento de datos personales que: "*En consecuencia, con la información técnica facilitada por el fabricante se concluyó que la instalación de estos sistemas en los CENTROS SUPERA no suponían ningún riesgo para el tratamiento de datos de carácter personal de los usuarios, dado que los datos extraídos por los lectores de ***EMPRESA.1 no podrían ser en ningún caso desencriptados ni desmontados, estando únicamente en posesión del fabricante las claves para el algoritmo, sin que se almacenase ningún tipo de información sobre la imagen de los usuarios".*

  Más adelante se hará referencia a que no es cierto que el tratamiento de los datos biométricos personales que constan en las plantillas obtenidas del programa no genere riesgos por el hecho de haberse aplicado medidas de cifrado de los mismos, según consta en los certificados de la compañía.

En este momento, cabe aclarar que los procesos de cifrado aplicados por la reclamada: (i) no se realizan por el algoritmo NIR, que genera la plantilla, sino que según el "certificado de protección de datos faciales" de ***EMPRESA.1 se realizan mediante herramientas criptográficas y métodos de cifrado como el cifrado AES de 256 bits; (ii) se aplican posteriormente a haber creado la plantilla y sobre la misma, cifran el dato biométrico personal; (iii) no es cierto exactamente que el cifrado impida reduplicar la imagen original sino que lo hace el algoritmo NIR aplicado, siendo el cifrado posterior una medida de seguridad adicional que dificulta acceder a los datos necesarios para realizar ingeniería inversa del proceso.

Pero, en cualquier caso, aunque la plantilla biométrica esté encriptada para que no pueda ser legible para terceros ajenos que pudieran acceder sin autorización a los datos, siempre será legible e inteligible para los sistemas del responsable del tratamiento, que dispondrán de la clave de descifrado, y la emplearan cada vez que se realice un acceso/salida del centro para conocer a qué persona se asocia cada plantilla biométrica cada vez que se realiza el proceso de verificación de identidad. Por lo que la plantilla biométrica cifrada que se almacena es un siempre y sin lugar a dudas también, un dato personal biométrico de categoría especial. Sin que el proceso de cifrado cambie su naturaleza jurídica.

En conclusión, de todo lo expuesto se deduce que no cabe duda de que la reclamada **ha estado tratando datos biométricos de carácter personal que** encajan en la definición del artículo 4.14 del RGPD, toda vez que: (i) el software parte de características físicas de los socios (imagen de la cara, de la que extrae una muestra); (ii) las procesa técnicamente para convertirlas en un patrón facial (plantilla biométrica), que es un código identificador único de cada socio que se cifra y almacena en el sistema (iii) y el patrón biométrico se genera y se utiliza para realizar la identificación de identidad de cada socio por los dispositivos de reconocimiento facial que se hallan instalados cuando éste accede/sale del centro.
En consecuencia, cabe considerar que el método de acceso mediante reconocimiento facial empleado por la reclamada trata datos biométricos personales calificados como de categoría especial por el artículo 9.1 del RGPD. Y en caso de que el anterior método de acceso mediante huella dactilar contratado con NITGEN cumpliera estos requisitos, lo que es altamente probable (generar una plantilla o código numérico basado en la muestra de fragmentos de la huella de los socios que se emplea para realizar una identificación de los socios que acceden al centro), no cabe duda de que al implantar este sistema la reclamada habría estado tratando también datos biométricos de categoría especial.

3.3.2. Sobre las operaciones de tratamiento de datos biométricos incluidas en el sistema de acceso al centro.

El artículo 4.2 del RGPD define el "tratamiento de datos personales" como: "*cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjunto de datos personales ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier*

otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción;"

Cabe aclarar además que dentro del concepto de operaciones de tratamiento previsto en el artículo 4.2 del RGPD cabe incluir tanto:

El tratamiento material de los datos personales, que cuando se procesan técnicamente a través de un programa o software constan de diferentes procesos tales como la recogida de datos, el registro, almacenamiento, y su explotación o utilización, su cesión, eliminación o bloqueo…etc.

Así pues, consta en el procedimiento que la empresa reclamada ha comenzado a identificar a sus socios a través de este sistema de reconocimiento facial en 5 centros deportivos, implantando este como único método de acceso obligatorio a los mismos, aproximadamente desde julio- agosto de 2023, habiendo aportado como documento 3 la hoja de registros de un día determinado que acredita que ha recogido las muestras (sin almacenarlas) y ha generado las plantillas de cada socio que han accedido a utilizarlo, las ha registrado en el sistema, almacenado, y explotado al realizar cada acceso y salida del centro, según lo que la misma manifiesta al señalar que el programa registra las horas de entrada y salida del mismo.

El diseño del propio tratamiento es también considerado como una operación de tratamiento que debe estar sometida a los Principios y obligaciones previstos en el RGPD. Ello es así dado que de acuerdo con lo señalado por el Comité Europeo de Protección de Datos en sus Directrices 7/2020 sobre el responsable y encargado del tratamiento de 7 de julio de 2021, y el Tribunal de Justicia de la Unión Europea (en sentencias como la de 5 Oct. 2023, C-659/2022), el artículo 4.2 del RGPD recoge un concepto amplio de tratamiento de datos personales. Un concepto amplio que comienza con el diseño del tratamiento, que es a partir del cual nacen las obligaciones de respetar los principios de protección de datos y resto de obligaciones previstas en el RGPD.

De acuerdo con lo expuesto, la implantación del sistema de reconocimiento facial desarrollado por ***EMPRESA.1 supuso la realización de un tratamiento de datos personales por SIDECU, que no se refleja en el RAT aportado por la empresa, cuya finalidad era posibilitar el acceso y salida de los socios a los 5 centros deportivos que señala la misma, que estaba compuesto varias operaciones de tratamiento sobre un conjunto de datos personales diferentes, entre los que se encontraba el patrón facial de las personas a las que cabía permitir el acceso (los socios/abonados registrados en el sistema).

Este tratamiento debió reflejarse en el RAT, y por ser considerado de alto riesgo, debió precederse de un riguroso análisis de la necesidad, idoneidad y proporcionalidad de este nuevo método de acceso en comparación con otras alternativas menos intrusivas, y de un riguroso análisis de los riesgos, y en caso de considerar que el riesgo fuera aceptable y el tratamiento necesario, idóneo y proporcional, elaborar una única EIPD sobre el tratamiento que incluya y valore todos los métodos de acceso aplicables en los centros, que cumpla con los requisitos previstos en el artículo 35 del RGPD, pero todos responden a una misma finalidad y son parte de un único tratamiento. EIPD previa y conjunta que debió cumplir con el contenido mínimo previsto en dicho artículo.

Y que al incluir datos biométricos personales, que son considerados como de categoría especial, cuyo tratamiento se prohíbe de forma general por el artículo 9.1 del RGPD, la implantación de este método de acceso mediante reconocimiento facial, requería, a su vez, que la empresa se asegurase previamente de que concurría una excepción prevista en el artículo 9.2 del RGPD, que habilitase a poder realizar este tipo de tratamientos.

3.3.3. Sobre el responsable del tratamiento.

Por lo que respecta a la responsabilidad, el artículo 4. 7 del RGPD, define al: “7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros”.

Pese a que se señala que se contrató el desarrollo del programa con ***EMPRESA.1, no se aporta el contrato de encargo del tratamiento que permita acreditar que esta entidad actuaba como encargada del tratamiento, como se deduce de las manifestaciones de la reclamada.

No obstante, aún en el caso de que fuera acreditado que ***EMPRESA.1 actuó como encarga del tratamiento de los datos personales obtenidos, a la vista de la política de privacidad diligenciada en este procedimiento, y las condiciones generales de la empresa adjuntas a la hoja de registro aportada con una de las reclamaciones, no

cabe duda de que SIDECU ha actuado en todo momento como responsable del tratamiento, puesto que es la que decidió contratar este sistema determinando con ello los fines y medios del tratamiento.

Todo ello determina que SIDECU es la responsable del tratamiento a los efectos previstos en el artículo 4.7 del RGPD, y, en consecuencia, la presunta responsable frente a la que debe dirigirse el presente procedimiento sancionador iniciado para determinar si el tratamiento implantado por la misma incumplió alguna de las obligaciones del RGPD tipificadas como infracción, de acuerdo con lo previsto en el artículo 70. 1 a) de la Ley Orgánica 3/2018, de 5 de diciembre, de protección de datos personales y garantía de derechos digitales (en adelante, LOPPDD), que dispone lo siguiente:

"Artículo 70. Sujetos responsables.

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. b) Los encargados de los tratamientos. c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea. d) Las entidades de certificación. e) Las entidades acreditadas de supervisión de los códigos de conducta. (…)".*

IV. Obligación incumplida. Sobre el incumplimiento de disponer de una excepción del artículo 9.2 del RGPD que habilite a tratar datos de categoría especial.

4.1. Los datos biométricos como datos de categoría especial: prohibición general y excepciones de tratamiento.

El RGPD define el art.4.14 datos biométricos como "*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*".

De acuerdo con la definición dada por el artículo 4.14 del RGPD, los datos biométricos tratados por estos sistemas se convertirán en datos de carácter personal siempre y cuando la finalidad del tratamiento sea la identificación o autenticación de una persona, en el sentido previsto en el artículo 4.1 del RGPD.

Como ya se ha dicho anteriormente, no cabe duda de que tanto las minucias (huellas dactilares) como los patrones faciales que se extraen de la imagen de la cara de las personas para realizar la identificación unívoca de las personas que están autorizadas a acceder a un recinto son datos biométricos de carácter personal, puesto que la finalidad del sistema implantado es determinar la identidad, directa o indirectamente, de las personas autorizadas para acceder a los mismos, registrándose en su caso las horas de entrada y salida, como sucede en el supuesto presente. Toda vez que el proceso asigna un identificador numérico (la plantilla biométrica obtenida al recoger los puntos de la cara de los interesados) que permite singularizar a un individuo y, distinguirlo frente a otros, a través de "elementos propios de la identidad física, fisiológica, genética, psíquica".

Se debe considerar además que -a diferencia de lo que sucedía bajo el régimen anterior al RGPD- este tipo de datos biométricos están considerados como **datos personales de categoría especial** en el artículo 9, cuyo tratamiento está generalmente prohibido, salvo que concurra alguna de las excepciones previstas en el artículo 9.2 del RGPD. Lo que no exime de que siempre deba existir además una base de licitud prevista en el artículo 6 del mismo, entre otros muchos requisitos y principios que deberá cumplir aquel que decida optar por este tipo de tratamientos.

De acuerdo con el artículo 9.1 del RGPD, queda prohibido el tratamiento de datos biométricos cuando sean: "*datos biométricos dirigidos a identificar de manera unívoca a una persona física*".

En este orden de cosas tenemos que, siendo los datos biométricos datos de categoría especial, el RGPD impone una obligación adicional al responsable del tratamiento de los mismos, que estará obligado también a comprobar y acreditar que concurre una de las excepciones previstas en el artículo 9.2 del RGPD u otra legislación específica, antes de iniciar el tratamiento de ningún dato biométrico, lo que se aplica al supuesto presente, en el que se previno el fichaje biométrico como método general de fichaje basado en el reconocimiento facial de los empleados.

Hay que señalar que, estando prohibido el tratamiento de datos biométricos con carácter general, cualquier excepción a dicha prohibición habrá de ser objeto de interpretación restrictiva, tal y como se deduce de los considerandos 51 y 52 del RGPD. Así las cosas, las excepciones que posiblemente podrían permitir el levantamiento de la prohibición general de tratar datos biométricos dirigidos a identificar-verificar la identidad de personas físicas, son las que prevé el artículo 9.2. del RGPD, con el siguiente tenor literal, que deberá interpretarse restrictivamente, siempre en favor de proteger los derechos y libertades de los ciudadanos en caso de duda:

> *"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.*
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".

Por tanto, si el responsable no acredita que su tratamiento está dentro de alguna de estas excepciones, incurrirá en una infracción del artículo 9 del RGPD por iniciar un tratamiento prohibido.

4.2. Análisis del supuesto presente.

En el presente supuesto, consta acreditado que SIDECU ha tratado datos biométricos personales de categoría especial, **implantando como obligatorio**, al menos, entre julio y agosto de 2023 un nuevo método de acceso a 5 de sus centros deportivos mediante reconocimiento facial basado en el software ***EMPRESA.1, que genera, almacena y explota el patrón biométrico facial de las muestras obtenidas de la imagen de la cara de los socios que accedieron a los mismos, método que sigue empleándose en la actualidad. Y que anteriormente a este sistema, se implanto un sistema de acceso mediante huella dactilar, que también implica el tratamiento de datos biométricos personales de categoría especial.

Según lo expuesto, para poder tratar los datos que se derivan del empleo de un sistema biométrico empleado como método de identificación de las personas, el responsable debe asegurarse de que además de disponer de una base de licitud del artículo 6 del RGPD, concurre también una excepción del artículo 9.2 del RGPD, que levante la prohibición general de tratamiento de datos de categoría especial prevista en el artículo 9.1. del RGPD. Es más, solo en caso de concurrir una de estas excepciones que le habiliten a realizar el tratamiento, deberá entonces plantearse el responsable del tratamiento cuál es la base de licitud que concurre, puesto que, en caso contrario, el tratamiento de estos datos estaría prohibido por el artículo 9.1 del RGPD.

Se ha de aclarar que **no es una cuestión discutida que la empresa reclamada dispone de una base de licitud prevista en el artículo 6. 1 del RGPD** que le habilita a tratar datos personales con la finalidad de controlar el control de acceso de las personas a sus centros deportivos.

En el presente supuesto, el RAT aportado por la reclamada no hacía referencia alguna al tratamiento consistente en el control de acceso de los socios abonados al club, por lo que no consta en el mismo en qué base de licitud se apoya la empresa reclamada para realizar el tratamiento de datos personales en que consiste el mismo. Ni tampoco se ha realizado una EIPD donde se concrete el mismo, al entender la reclamada erróneamente que no tenía obligación de hacerlo.

Seguidamente, se entrará a valorar la falta de acreditación de una excepción que habilite a tratar estos datos de acuerdo con el artículo 9.2 del RGPD. Pero por lo que respecta a la base de licitud, lo cierto es que no cabe imputar en este caso una infracción administrativa del artículo 6.1 del RGPD, puesto que aunque la empresa responsable no haya reflejado por escrito qué base de licitud le habilita a tratar datos personales de los socios para el control de acceso a sus centros, para valorar si concurre una infracción del artículo 6 del RGPD, lo principal es comprobar que realmente exista una base jurídica legal, aunque el responsable no la haya determinado correctamente ni incluido en la EIPD.

Y en este caso, puede establecerse que de inicio si existe base de licitud que habilita al la parte reclamada para realizar tratamientos de datos personales en general (no para los biométricos, pues ello supone que además deberá concurrir una excepción del artículo 9). En concreto, la referida en el artículo 6.1.b), que se refiere a que: "*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".* Toda vez que la firma de la hoja de inscripción y la aceptación de las condiciones generales y

normas de régimen interno por los socios, en los términos que han sido diligenciados por el inspector, supone la creación de un vínculo contractual entre el socio y el centro deportivo, que se rige por estas normas. Por tanto, no cabe inicialmente imputar una infracción del artículo 6 del RGPD.

Ahora bien, pese a que concurría una base de licitud, hay que dejar claro que la misma legitimaba a la reclamada para tratar otros datos personales que no fueran biométricos, como los que son requeridos habitualmente para acceder por otros medios como el de las tarjetas identificativas o la exhibición de DNI (datos nominativos), pero no legitimaba en ningún caso a iniciar un tratamiento biométrico del patrón facial o de la minucia de la huella dactilar, si además no existe una excepción del artículo 9.2 que le permitiese levantar la prohibición de tratar datos biométricos.

Por tanto, no cabe duda de que el inicio de este tratamiento estaba condicionado a la previa concurrencia de una excepción del artículo 9.2 del RGPD, sin que la reclamada haya alegado que concurra ninguna excepción en su documentación y escritos puesto que niega estar realizando un tratamiento de datos biométricos personales de categoría especial, al entender erróneamente que la plantilla biométrica o patrón facial empleado para realizar la identificación no es un dato personal, sino un código numérico mediante el que no se puede conocer la identidad de la persona, habiéndose señalado en el Fundamento de Derecho III los motivos por los que se entiende que esta argumentación no se ajusta a derecho.

Cabe señalar que la definición del dato biométrico de categoría especial se halla contenida en el RGPD y debe conocerse por los responsables del tratamiento. Si bien no es obligatorio que existan directrices o guías que interpreten el contenido de las normas previstas en el RGPD para que se consideren de cumplimiento obligatorio por los responsables, se han aprobado diversas Guías y Directrices del Consejo Europeo de Protección de Datos (en adelante, CEPD) que el responsable del tratamiento debería conocer, en las que se detalla que la plantilla biométrica utilizada para identificar unívocamente a las personas es un dato biométrico de categoría especial.

Pero, al contrario de lo que sucede con la base de licitud del artículo 6 del RGPD, de la documentación aportada no puede deducirse la concurrencia de una excepción del artículo 9. 2 del RGPD que pueda ajustarse a la finalidad y tipo de tratamiento ante el que nos encontramos. Y en concreto, cabe señalar que, a priori y sin perjuicio de que lo pueda deducirse durante la instrucción, cabe descartar la concurrencia de las siguientes excepciones en el supuesto presente:

- Por una parte, no cabe considerar la aplicación de la excepción del consentimiento prevista en el artículo 9.2.a) del RGPD.

  El art. 4.11 del RGPD se refiere al consentimiento del interesado como "*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*".

  Por tanto, para que pueda ser considerado como una excepción válida, el consentimiento para tratar datos biométricos de categoría especial deberá ser libre,

específico, informado e inequívoco, de acuerdo con lo previsto en los artículos 7 del RGPD y 6 de la LOPDGDD.

- Específico porque se refiera expresamente al tratamiento de datos biométricos de categoría especial.
- Inequívoco porque no deje lugar a dudas y sea comprensible.
- Informado porque se proporcione en el mismo una información previa al interesado que exige el artículo 13 del RGPD, y toda aquella que le haga consciente a los interesados de los riesgos de dicho tratamiento (considerando 39 del RGPD), especialmente cuando afecta a personas se encuentre en situación de vulnerabilidad.
- Y para que se pueda considerar libre el consentimiento a un método de acceso que implique el tratamiento de datos biométricos, el responsable del tratamiento debe establecer un método alternativo para poder realizar el control de acceso, sin tener ninguna consecuencia para la persona que no quiera utilizar el control de acceso mediante un tratamiento de datos biométricos.

En el presente supuesto, la reclamada reconoce desde su primer escrito de respuesta que no está recabando de los socios el consentimiento para recoger sus datos personales biométricos, en los siguientes términos: "*Si bien es cierto, que en la documentación de alta de usuario no aparece contemplada la autorización para la recogida de datos personales relativos al uso de datos biométricos o de categorías especiales, ello es debido a que, atendiendo a las características del funcionamiento del sistema de acceso, no solo no se guarda la imagen de los usuarios por parte de SIDECU, S.A. como teórico responsable del tratamiento, sino que no se conserva ningún tipo de dato personal, pues la plantilla generada por el sistema no permite la asociación a ninguna persona concreta(…)".*

Por otra parte, esta versión se corrobora por el contenido de la hoja de inscripción que se firma por los socios, que ha sido aportada por uno de los reclamantes, que constituyendo un simple documento contractual en el que el socio acepta las condiciones de pertenencia, acceso y permanencia que se debe firmar para poder adquirir la condición de socio, cuyo contenido ha sido extraído y diligenciado por el inspector del procedimiento. Al aceptar las condiciones generales por el socio, se consiente una cláusula sobre protección de datos que se refiere al tratamiento de datos personales, en el que no se observa mención alguna al consentimiento de tratamiento de datos biométricos de categoría especial con la finalidad de controlar el acceso de los socios a los centros.

Así pues, tal y como se hace constar en el punto segundo del informe de actuaciones previas de investigación de 21/06/2024:

"En el documento de registro (procedimiento administración y recepción en los centros*),* formulario de inscripción a los centros, se recogen los datos personales del nuevo socio (nombre y apellidos, número de DNI, fecha de nacimiento, dirección, teléfonos, email, datos bancarios) y se informa de lo siguiente:

"Con la firma del presente documento afirmo que he leído y acepto las condiciones de protección de datos,

☐ *Ud. consiente y autoriza expresamente a que SIDECU, S.A. trate los datos que ha facilitado para realizar estudios estadísticos para ofrecerle periódicamente información sobre productos, actividades, servicios y acciones comerciales de promoción y/o marketing relacionadas con proveedores de transportes, deportes, seguros, servicios inmobiliarios, financieros y bancarios, con el fin de informar de sus productos o servicios y hacer ofertas comerciales, incluyendo por medios de comunicación electrónica."*

En este documento de registro existen varios enlaces, uno de "Protección de Datos", en el que se ha comprobado que ofrece la siguiente información:

> *"CLÁUSULA RESPONSABLE DEL TRAMIENTO DE DATOS PERSONALES.*
>
> *Los datos que Vd. proporcione a fin de desarrollar el objeto del presente contrato, serán incorporados a las bases de datos propiedad de SIDECU, S.A., que actuará como Responsable del Tratamiento.*
>
> *Los datos referentes a datos personales y datos médicos relativos a salud que Vd. pueda facilitar, con la finalidad de la adecuada prestación de los servicios que solicite en cada momento, se emplearán única y exclusivamente a los efectos de cumplir con el objeto del presente contrato y, en particular, con las finalidades siguientes: gestión de clientes, premiar su fidelidad, mantenerlos informados (envío boletín de noticias), por cualquier medio (electrónico o no), de ofertas de productos y/o servicios y/o promociones relacionadas con las actividades propias del presente contrato y del objeto social de SIDECU, S.A.*
>
> *Con el fin de poder ofrecerle productos y/o servicios de acuerdo con sus intereses y mejorar su experiencia, podremos elaborar un perfil comercial en base a la información facilitada por Vd. No obstante, no se tomarán decisiones automatizadas en base a dicho perfil.*
>
> *De conformidad con la normativa vigente en materia de protección de datos de carácter personal, tiene derecho a ejercitar en cualquier momento sus derechos de acceso, rectificación, portabilidad, limitación, supresión u oposición de los datos referentes a su persona incluidos en nuestras bases de datos ante el Delegado de Protección de Datos, acreditando debidamente su identidad; así como presentar una reclamación ante la autoridad de control estatal en caso de que el titular de los datos de carácter personal considere que se han vulnerado sus derechos.*
>
> *En todo caso, el consentimiento tiene carácter revocable, pudiendo Ud. retirar en cualquier momento el consentimiento prestado o ejercitar cualquier de los derechos mencionados en la forma indicada en la presente cláusula. Ud. responderá de la veracidad de los datos facilitados a SIDECU, S.A. reservándose éste la facultad de excluirle de cualesquiera actuaciones y/o servicios en caso de que facilite datos*

falsos, sin perjuicio de cualesquiera otras acciones que puedan proceder. Del mismo modo, Ud. es responsable de mantener actualizados los datos personales que haya facilitado a SIDECU, S.A.

Los datos facilitados serán conservados y tratados por SIDECU, S.A. mientras se mantenga la relación contractual, mientras no se solicite su supresión y, en cualquier caso, hasta el vencimiento de los plazos legalmente exigibles"

En el enlace de "condiciones generales" no se encuentra información de protección de datos. En el enlace Reglamento de Régimen Interno, que varía para cada uno de los centros, se encuentra la siguiente información de Protección de Datos:

"*1.8. A los efectos de la Ley Orgánica 15/1999 de 13 de Diciembre de protección de datos de carácter oficial, al inscribirse en la instalación se autoriza la utilización de los datos personales y su tratamiento informático para la gestión de la instalación y en su caso el envío de información comercial inherente a la gestión del Centro."*

Por tanto, no cabe duda de que no concurre la excepción del artículo 9.2.a) del RGPD, toda vez que: (i) además de que se ha reconocido que no se estaba recabando un consentimiento específico, inequívoco e informado para el tratamiento de datos biométricos, (ii) constan evidencias de que el empleo de este método de acceso mediante reconocimiento facial se impuso a los socios como único y obligatorio entre julio y agosto de 2023, no permitiendo el uso de medios alternativos, lo que generó según la reclamada un total de 26 reclamaciones solo en el centro de Entrepuentes, y la presentación ante esta Agencia de un total de 9 reclamaciones de los socios de 5 centros deportivos y 2 denuncias, por lo que existen evidencias de que tampoco existía un consentimiento libre de los socios al empleo de este medio. Situación que la reclamada dice haber corregido en el centro de Entrepuentes tras recibir varias reclamaciones de los socios, instalando un nuevo método de acceso mediante exhibición de DNI, lo que, por otra parte, no ha sido acreditado.

- Por otra parte, cabe aclarar de antemano también que, a la vista de las evidencias que constan en el procedimiento y las manifestaciones de la parte reclamada, no concurre en este supuesto la excepción del 9.2.g) del RGPD, referida a la concurrencia de un interés público esencial.

En la Guía aprobada por esta Agencia sobre sobre tratamientos de control de presencia mediante sistemas biométricos, se analiza la aplicación de algunas de las excepciones previstas en el artículo 9.2 para supuestos como el presente, en los que el tratamiento tiene por finalidad de control de acceso de personas a recintos públicos o privados, y se señala que no cabe alegar en estos supuestos ni que sea necesario para ejecutar un contrato (no estando la relación contractual prevista como excepción del artículo 9.2 del RGPD, sino como base de licitud), ni tampoco la excepción del interés legítimo del artículo 9.2.g) del RGPD, por no tratarse de "un tratamiento que sea 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".

Así pues, la Guía señala expresamente que:

> "*Únicamente cabe excepcionar la prohibición de tratamiento de los datos de categoría especial cuando concurra alguna de las circunstancias que se especifican en el apartado 2 del art. 9 del RGPD. El responsable tiene la obligación de valorar muy seriamente y con diligencia si tiene una razón sólida para tratar categorías especiales que aparezca enumerada en dicho art. 9.2 del RGPD.*
>
> *Entre las circunstancias enumeradas no se encuentra el interés legítimo, la ejecución de un contrato o medidas precontractuales.*

En el apartado segundo del informe 0036/2020 de 8 de mayo de 2020, emitido por el Gabinete jurídico de esta Agencia (al que alude la reclamada), se realizan unas consideraciones generales respecto a cuando concurre la excepción del artículo 9.2.g) del RGPD en el supuesto de tratamiento de datos biométricos de categoría especial, donde se manifiesta expresamente que para tratar datos biométricos de categoría especial al amparo de la misma, se requiere que: (i) exista un interés público (y no el privado de garantizar que solo acceden al recinto las personas que tienen la condición de socio y han abonado su cuota),(ii) que el interés público sea, además, esencial, (iii) que éste interés público esencial este previsto en una norma con rango de ley; esto es, que la norma con rango de ley deberá además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, sin que sea suficiente a estos efectos la imposición de un interés público, y dicha Ley deberá además establecer las garantías adecuadas de tipo técnico, organizativo y procedimental.

En concreto, dicho informe analiza la jurisprudencia del Tribunal Supremo y el Tribunal Constitucional y, señala, entre otros aspectos, lo siguiente:

- *"Sin embargo, tratándose de categorías especiales de datos, el supuesto contemplado en la letra g) del artículo 9.2. no se refiere solo a la existencia de un interés público, tal y como hace en muchos otros de sus preceptos el RGPD, sino que es el único precepto del RGPD que requiere que el mismo sea "esencial", adjetivo que viene a cualificar dicho interés público, habida cuenta de la importancia y necesidad de mayor protección de los datos tratados. En relación con lo que debe entenderse por interés público esencial, debe tenerse igualmente en cuenta la Jurisprudencia del Tribunal Europeo de Derechos Humanos, que al amparo del artículo 8 del Convenio Europeo de Derechos Humanos, viene considerando que el tratamiento de datos personales constituye una injerencia licita en el derecho del respeto de la vida privada y solo puede llevarse a cabo si se realiza de conformidad con la ley, sirve a un fin legítimo, respeta la esencia de los derechos y libertades fundamentales y es necesario y proporcionado en una sociedad democrática para alcanzar un fin legitimo (D.L. contra Bulgaria, no 7472/14, 19 de mayo d 2016, Dragojević contra Croacia, no 68955/11, 15 de enero de 2015, Peck*

contra Reino Unido, no 44647/98, 28 de enero de 2003, Leander contra Suecia, n.o 9248/81, 26 de marzo de 1987, entre otras).(…)"

- *"Según reiterada doctrina constitucional, la reserva de ley no se limita a exigir que una ley habilite la medida restrictiva de derechos fundamentales, sino que también es preciso, conforme tanto a exigencias denominadas -unas veces- de predeterminación normativa y -otras- de calidad de la ley como al respeto al contenido esencial del derecho, que en esa regulación el legislador, que viene obligado de forma primaria a ponderar los derechos o intereses en pugna, predetermine los supuestos, las condiciones y las garantías en que procede la adopción de medidas restrictivas de derechos fundamentales(…)".*

- *"Por consiguiente, el tratamiento de datos biométricos al amparo del artículo 9.2.g) requiere que esté previsto en una norma de derecho europeo o nacional, debiendo tener en este último caso dicha norma, según la doctrina constitucional citada y lo previsto en el artículo 9.2 de la LOPDGDD, rango de ley. Dicha ley deberá, además especificar el interés público esencial que justifica la restricción del derecho a la protección de datos personales y en qué circunstancias puede limitarse, estableciendo las reglas precisas que hagan previsible al interesado la imposición de tal limitación y sus consecuencias, sin que sea suficiente, a estos efectos, la invocación genérica de un interés público. Y dicha ley deberá establecer, además, las garantías adecuadas de tipo técnico, organizativo y procedimental, que prevengan los riesgos de distinta probabilidad y gravedad y mitiguen sus efectos".*

No habiéndose acreditado por la reclamada, por tanto, la concurrencia de ninguna de las excepciones previstas en el artículo 9.2 del RGPD que permita levantar la prohibición general de tratamiento de datos biométricos de reconocimiento facial, se considera que al implantar como método obligatorio y único de acceso a sus 5 centros deportivos un sistema de identificación de los socios basado en un sistema de reconocimiento facial (y anteriormente según la misma, mediante un sistema basado en la detección de huella dactilar), la empresa reclamada pudo incurrir en una infracción administrativa del artículo 9 del RGPD, realizando un tratamiento prohibido de datos biométricos personales de categoría especial.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción del artículo 9 del RGPD, imputable a ***SIDECU***, por vulneración del artículo transcrito anteriormente.

V. Tipificación de la infracción del artículo 9 del RGPD y calificación a efectos de prescripción.

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración del artículo siguiente, que se sancionará, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de

una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"b) los derechos de los interesados a tenor de los artículos 12 a 22;"

Por su parte, la LOPDGDD en su artículo 71, Infracciones, señala que:

"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".

A los solos efectos del plazo de prescripción, el artículo 72.1 de la LOPDGDD establece lo siguiente:

"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran 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:
h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."

VI. Sanción por incumplimiento del artículo 9 del RGPD.

A fin de determinar la multa administrativa a imponer se han de observar las previsiones de los artículos 83.1 y 83.2 del RGPD, preceptos que señalan:

> *"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.*
>
> > *1. 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, y
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, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD 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 inducir 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 el presente caso, considerando la gravedad de la posible infracción cometida, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de ***SIDECU*** que se ha hecho a constar en la Diligencia de 30-4-24 (16.154.950 euros en el año 2023).

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados.

- 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 (artículo 83.2, letra a), del RGPD):

  La conducta en la que se concreta la naturaleza de infracción atribuida a la denunciada afecta a vulnerar la prohibición de tratar datos de categoría especial sin disponer de una excepción, prevista en el artículo 9 del RGPD que está sancionado como se ha dicho, con multa de hasta 20 millones de euros o el 4% del volumen de negocios de la reclamada.

  En el presente supuesto, para graduar la gravedad de la sanción se tiene en consideración, por una parte, el número de afectados cuyos datos personales biométricos fueron objeto de tratamiento en los 5 centros deportivos a los que se refieren las reclamaciones, en los que la reclamada ha reconocido haber implantado este sistema de reconocimiento facial, partiendo de los datos aportados por la propia reclamada, sin perjuicio de lo que se acredite en fase de instrucción, que hizo constar lo siguiente al responder al requerimiento de información de esta Agencia: "*Actualmente el referido sistema de reconocimiento facial se encuentra instalado en cinco centros deportivos, siendo el número total de usuarios de dichos centros de 36.483. Uno de esos centros es el de Entrepuentes de Sevilla, el cual cuenta actualmente con 8.978 usuarios (a fecha 4/01/2024)".*

  Y también se tienen en consideración las características y funcionamiento técnico, del sistema de reconocimiento facial que fue implantado que constan en los certificados del fabricante sobre el sistema ***EMPRESA.1 que han sido aportados por la reclamada, así como las medidas de seguridad adoptadas que han sido mencionadas en el punto quinto del informe de actuaciones previas de inspección.

  Por lo que respecta a la duración de la infracción, se considera que estamos en presencia de una infracción continuada que comenzó, al menos, desde la implantación del sistema de reconocimiento facial entre los meses de julio y agosto de 2023 y permanece en la actualidad, todo ello sin perjuicio de que de la instrucción se derive una fecha de implantación de sistemas biométricos diferente.

  - Art. 83.2b) "la intencionalidad o negligencia en la infracción".

Como responsable del tratamiento de los datos personales de los socios que han contratado sus servicios y tienen derecho a acceder a sus centros deportivos al objeto de poder disfrutar de los mismos, cuando la responsable del tratamiento escoge emplear un método de acceso que utiliza un sistema biométrico de identificación de los mismos, viene obligada a actuar con la especial diligencia que es exigible a este tipo de tratamientos, dados los elevados riesgos que genera su utilización.

A este respecto, procede recordar la Sentencia de la Audiencia Nacional de 17/10/2007 (rec. 63/2006), que respecto de entidades cuya actividad lleva aparejado el continuo tratamiento de datos de clientes, indica "…*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 entidad 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 previsiones legales al respecto*."

La parte reclamada alega que analizó los diferentes métodos de acceso y determinó en base al Informe 0036/2020 del gabinete jurídico de esta Agencia y la información dada por el fabricante que el programa no trataba datos biométricos de categoría especial, puesto que no almacenaba las imágenes de las que se extraía el patrón facial,

Se considera que la empresa reclamada ha actuado sin dolo pero con un nivel de negligencia grave: (i) primero, al interpretar que el programa ******EMPRESA.1*** no trataba ni siquiera datos personales, por interpretar de los certificados del fabricante que al no almacenarse la imagen de la cara de los socios y convertirse en una plantilla (código numérico o modelo matemático) que era encriptada, no podía deducirse la identidad de las personas de la misma; (ii) fue advertido por varios reclamantes al respecto de que la plantilla o patrón facial eran en realidad el dato personal biométrico de categoría especial, y en especial, consta que uno de los reclamantes (***C.C.C.***) describió con detalle el concepto y requisitos exigibles en este tipo de tratamientos, limitándose la empresa a contestar al mismo con el mismo escrito y argumentación que había planteado para todas las respuestas; (iii) consta además que la reclamada conocía de la existencia del informe nº 0036/2020 de esta Agencia en la que se analizaba también el concepto de datos biométricos de categoría especial, puesto que lo menciona entre sus argumentaciones, si bien lo interpreta erróneamente; (iv) pese a todo ello, no consta que presentase o consultase previamente a a esta Agencia (prevista en el artículo 36 del RGPD), ni solicitase la opinión de un consultor o experto en la materia, ni de la empresa encargada del desarrollo del programa acerca de estas reclamaciones que venían planteando los socios desde agosto de 2023, que solo en el centro de Entrepuentes ascendieron a un total de 26, según la misma , (v) y, como consecuencia de todo ello, no analizó exhaustivamente si concurría alguna de las excepciones del artículo 9.2 del RGPD, e inició un tratamiento que estaba prohibido.

- Artículo 76.2.f) de la LOPDGDD. *La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*

A este respecto, SIDECU, por la actividad a la que se dedica, trata numerosos datos personales y de forma continua, de los socios que se inscriben en sus centros deportivos. Consta en la diligencia reflejando la información básica obtenida de la herramienta Axesor de 30/04/24 que SIDECU es una gran empresa cuyo objeto social es la gestión de instalaciones deportivas con 267 empleados, que en el presente supuesto, está gestionando un volumen muy elevado de datos personales de los socios de los 33 centros deportivos que gestiona de acuerdo con lo que consta en su web según la Diligencia expedida el 2-4-25.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que 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 del RGPD, permite fijar inicialmente una sanción de multa administrativa de **80.000,00 euros (OCHENTA MIL EUROS).**

VI. Obligación incumplida. Sobre la obligación de realizar una EIPD previa que cumpla con los requisitos previstos en el artículo 35 del RGPD.

7.1. Sobre la necesidad de realizar y superar una EIPD en el presente supuesto.

La evaluación de impacto en la protección de datos personales, EIPD, aparece como la herramienta exigida por el RGPD para garantizar que se cumple con esta vertiente cuando el tratamiento se considerada de “alto riesgo”, según lo establecido en el artículo 35 en su apartado1 del RGPD (el subrayado es nuestro):

“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…”

Esta evaluación se hará con carácter previo al inicio del tratamiento, pero deberá entenderse como una evaluación continua o periódica, en el sentido establecido por el artículo 35.11 del RGPD, que dispone*: “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.*”

Como ya se ha avanzado anteriormente, una EIPD **debe cumplir con los requisitos o contenido mínimo relacionado en el artículo 35.7 del RGPD**, que dispone:

"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".

En definitiva, la superación de una EIPD exige que el responsable de un tratamiento de alto riesgo documente por escrito la totalidad de las operaciones de tratamiento que realiza y sus finalidades; que se supere la evaluación de idoneidad, necesidad y proporcionalidad del tratamiento, y que gestione desde el diseño los riesgos específicos del tratamiento, con la aplicación práctica de medidas orientadas a los mismos de forma que se garantice un umbral de riesgo aceptable durante todo el ciclo de vida del tratamiento, tal como se establece en el artículo 35 del RGPD. Además, obliga a la consulta previa a la autoridad de control en caso de que el responsable no haya tomado medidas que permitan mitigar el riesgo de acuerdo al artículo 36 del RGPD.

Tal y como se ha expuesto, el tratamiento de los datos personales biométricos en el ámbito de control de acceso de personas a recintos o instalaciones lleva aparejados riesgos relevantes y especialmente significativos para los derechos y libertades de las personas cuyo tratamiento ya entraña, por sí solos y por separado, una probabilidad de alto riesgo para los derechos y libertades de los empleados merecedora de una EIPD, previa y válida.

A mayor abundamiento, hay que señalar que datos biométricos dirigidos a la identificación-autenticación de las personas -como es el caso presente-, han sido expresamente incluidos en la Lista de tipos de tratamiento de datos que requieren evaluación de impacto relativa a la protección de datos, publicada por la AEPD el 6 de mayo de 2019, en desarrollo de la previsión contemplada en el apartado cuarto del referido artículo 35 del RGPD, que prevé que las autoridades de control establezcan y publiquen listas que definan los tratamientos que requieran EIPD.

En el caso del estado español, se ha optado por publicar una lista no exhaustiva, en la que se determina que "*será necesario realizar una EIPD, en la mayoría de los casos, en los que dicho tratamiento cumpla con dos o más criterios de la lista" (*criterios 4 y 5 en el caso de los datos biométricos para control de jornada o asistencia). No obstante, ello no excluye a otros tratamientos que no cumplan con estos criterios, pero a la luz de su naturaleza, alcance, contexto y fines exista probabilidad de que entrañen un alto riesgo a los efectos previstos en el artículo 35.1 del RGPD.

En el presente supuesto, constan evidencias de que el software de reconocimiento facial de ***EMPRESA.1 que puso en funcionamiento la empresa reclamada (al menos, en 5 de sus centros deportivos), trataba el patrón facial de los socios y almacenaba el mismo en los servidores de la responsable del tratamiento, por lo que está realizando un tratamiento de datos biométricos personales calificados de categoría especial en el artículo 9 del RGPD, tal como se ha expuesto detalladamente en el Fundamento de Derecho III, apartado 3.4.

Por tanto, como también se ha detallado en el apartado 3.2, no cabe duda de que la responsable del tratamiento debió ser consciente de que iba a iniciar un tratamiento de alto riesgo y que era obligatoria la realización y superación de una previa EIPD, de acuerdo con lo previsto en el artículo 35.1 del RGPD.

La empresa reclamada reconoce que no elaboró una EIPD previa -lo que supone de por si, sin lugar a dudas, un incumplimiento de la obligación señalada en el artículo 35 del RGPD- pero mantiene que obró con diligencia en sus funciones puesto que realizó un análisis de riesgos previo a la EIPD, en el que determinó que al no tratarse datos personales por el software de reconocimiento facial empleado según la documentación del fabricante, no era necesario elaborar una previa EIPD, ni cumplir con otros requisitos previstos en el RGPD.

- En el primer escrito de respuesta al traslado realizado por esta agencia, SIDECU manifiesta que: **"***La sociedad SIDECU, S.A. analizó diferentes modalidades de sistemas de acceso a sus centros deportivos, en virtud de los cuales se evitase, por un lado, el acceso de personas a los centros que no tuviesen la condición de abonados y, por otro lado, que cumpliesen con la condición de evitar el tratamiento de datos adicionales e innecesarios para los que hubiera que obtener el consentimiento expreso del usuario.(…)"; "Así, se obtuvo diferente información acerca de diferentes sistemas biométricos, optando SIDECU por el sistema de la empresa ***EMPRESA.1 y realizando un análisis de riesgos previamente a su adquisición"; "Según la información que nos transmitió el fabricante, se crea un modelo con el algoritmo NIR, patentado por este fabricante, que utiliza algoritmos matemáticos complejos, generando un modelo numérico al usar información de alguno de los puntos dela captura. En ningún momento puede deducirse de este modelo características físicas de la persona(…)..*

- En su escrito de 19/01/24, SIDECU contesta al requerimiento de información de la fase de investigación acerca del análisis de riesgos y EIPD del tratamiento, aportando como documento 5 un denominado "ANÁLISIS DE

RIESGOS PREVIO A UNA EIPD" de SUPERA, fechado el 2-9-22, que consta de dos páginas, en las que se hace constar que se realiza un análisis de la iniciativa de implantación de sistemas de reconocimiento facial de ***EMPRESA.1 para el acceso a los centros deportivos de GRUPO SUPERA; se cita que no se van a tratar datos personales, y posteriormente se emite directamente la siguiente conclusión:

> *"Según la información facilitada por el fabricante, la implantación del sistema de reconocimiento facial fabricado por ***EMPRESA.1 no supone ningún tratamiento de dato personal para los usuarios de los centros deportivos que accedan al mismo.*
> *El sistema genera una plantilla a partir de la imagen del usuario (la primera vez que accede) que no asocia a ninguna persona en particular, sino que simplemente analiza si el usuario que accede tiene o no derecho a ello.*
> *En particular, los datos extraídos por los lectores de ***EMPRESA.1 no podrían ser en ningún caso desencriptados ni desmontados, estando únicamente en posesión del fabricante las claves para el algoritmo, sin que se almacenase ningún tipo de información sobre la imagen de los usuarios.*
> *El sistema de reconocimiento facial tampoco se conecta a la base o listado de usuarios de los centros deportivos en ningún momento.*
>
> *Se aporta al presente informe el certificado emitido por el fabricante a tal efecto.*
>
> *En definitiva, no procede realizar ninguna Evaluación de Impacto al no existir tratamiento de datos al no poderse, en ningún caso, recuperar la imagen personal del usuario, ni siquiera deducir características físicas concretas de la misma, no pudiendo identificar a la persona.*
> *Se acuerda poner a disposición de los usuarios carteles informativos que informen acerca del nuevo sistema implantado y de sus características.*
> *Al no existir tratamiento de datos, ni poder ser considerado como tratamiento de categoría especial, tampoco procede recabar previamente el consentimiento del usuario. En cualquier caso, se podrá poner a disposición de los usuarios alternativas de acceso en los casos en los que se nieguen a utilizar este sistema.*
>
> *En definitiva, se deduce que el sistema propuesto no resulta intrusivo ni atenta contra los derechos de los usuarios de los centros deportivos al no tratar ni almacenar su imagen personal ni ningún otro dato que permita identificarlos."*

Sin embargo, no cabe admitir este argumento como válido para eludir el cumplimiento del deber de elaborar una EIPD del tratamiento, ni del resto las obligaciones que le eran exigibles como responsable del tratamiento, ya que en este caso el **"**análisis de riesgos previo a la EIPD**"** no fue un análisis de riesgos propiamente dicho, y, además, llegó a conclusiones contrarias a la realidad del tratamiento, toda vez que:

- Por una parte, y como ya se ha dicho, el documento elaborado por SUPERA (SIDECU según la política de privacidad antes señalada) en septiembre de 2022 parte de un enfoque erróneo de la naturaleza de los datos que trata el software de reconocimiento facial al interpretar la documentación proporcionada por el fabricante y entender que éste no trataba datos personales biométricos de categoría especial, e incluso, que el patrón facial o identificador numérico que creaba el programa no era tampoco un dato personal. Por tanto, llega a unas conclusiones que son contrarias a la normativa aplicable, no habiendo actuado con la diligencia exigible al analizar las categorías de datos personales que precisaba su tratamiento, por los motivos que ya se han señalado en el Fundamento de Derecho III de este acuerdo.

- Pero además de ello, el documento presentado no puede considerarse, en ningún caso, como un análisis de riesgos del tratamiento, de acuerdo con lo establecido en el RGPD.

  Como ya se ha dicho, una EIPD debe contener, de acuerdo con el artículo *artículo 35.7. c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1.*

  La evaluación de los riesgos concurrentes y el nivel de riesgo de un tratamiento tiene dos objetivos. El primero, optimizar los esfuerzos para mitigar y gestionar los riesgos de forma proporcional. El segundo, determinar si el nivel de riesgo exige cumplir con lo previsto en los artículos 35 y 36 del RGPD (supuestos de alto riesgo). No realizarla, o realizarla de forma incompleta y sin el rigor que requiere, implica consecuencias que pueden derivar en diversos incumplimientos de la normativa.

  La reclamada no ha seguido en este caso ninguna de las múltiples recomendaciones y herramientas que la ofrece la "**Guía sobre Gestión del riesgo y evaluación de impacto en tratamientos de datos personales de junio de 2021**" (en adelante, Guía EIPD) para elaborar su análisis de riesgos y determinar si era necesario en este caso una EIPD.

  Tal y como ha señalado esta Agencia, en la referida Guía de la EIPD, *en su apartado c), sobre el proceso de evaluación del riesgo:*

  "El proceso de evaluación del nivel de riesgo es una disciplina con una metodología consolidada y común a cualquier proceso de gestión del riesgo. Para la evaluación del nivel de riesgo asociado a un tratamiento hay que realizar las siguientes tareas:
  • • Identificar los factores de riesgo o amenazas para los derechos y libertades.
  • • Analizar los mismos, en su impacto y probabilidad, para poder llevar a cabo la evaluación del nivel de riesgo inherente que se deriva de cada uno de los factores de riesgo.
  • • Evaluar el nivel global del riesgo del tratamiento para los derechos y libertades del tratamiento".

El proceso de identificación de estos riesgos forma parte de la labor del responsable, sin que quepa trasladar a la Autoridad de Control el análisis de aquellos productos, servicios y sistemas existentes en el mercado que pudieran ser empleados, así como los riesgos asociados a los mismos en función de las tecnologías que incorporan, que solo puede y debe analizar el responsable que los implanta. Pese a ello, la Guía de EIPD es un instrumento útil que se contiene las pautas a seguir para identificar estos factores riesgos, y establece la necesidad de señalar cuáles son los riesgos inherentes al tratamiento y cuál es el riesgo residual o global tras aplicar las medidas de mitigación de los riesgos que sean necesarias.

Pues bien, la empresa reclamada, pese a tener a su disposición la normativa y los instrumentos (guías y directrices) que le hubieran podido llevar a realizar un adecuado análisis de riesgos, elaboró un documento de "análisis previo a la realización de una EIPD" que no describió las operaciones de tratamiento, ni identificó los factores de riesgo de las diversas operaciones incluidas en el mismo, ni analizó los riesgos concurrentes, su impacto o probabilidad de concurrencia individual, ni evaluó posteriormente el nivel global de riesgo del tratamiento (riesgo residual).

Por tanto, en este caso, se entiende que la reclamada no basó su decisión de no elaborar una EIPD en un análisis de riesgos propiamente dicho, de cada una de las actividades objeto de tratamiento, por la que llegase a la conclusión de que no era exigible la EIPD, basándose en la evaluación del riesgo inherente o global del tratamiento al completo que se había realizado. Puesto que se limitó a documentar los motivos por los que había llegado a la conclusión de que no era necesario cumplir con los requisitos exigibles al tratamiento de datos personales biométricos, y, en especial, porqué a su entender, no era necesario recabar un consentimiento de los socios ni elaborar una EIPD, en base a un análisis jurídico de la naturaleza jurídica de los datos tratados, que no consideraba datos personales, pero no en base a los riesgos concurrentes, que es lo que debe incluirse en el análisis de riesgos.

Lo que supone un claro incumplimiento de sus obligaciones como responsable del tratamiento, máxime en este supuesto en el que está claro que el programa diseñado por ***EMPRESA.1 trata datos personales biométricos de categoría especial, y que el tratamiento es de alto riesgo, siendo la EIPD obligatoria de acuerdo con el artículo 35.1 del RGPD.

A mayor abundamiento, cabe añadir que, en este caso, además de no haber elaborado una EIPD ni haber realizado un adecuado análisis de riesgos del tratamiento, la empresa reclamada tampoco ha acreditado haber cumplido con el resto de requisitos mínimos que establece el artículo 35.7 del RGPD, puesto que:

- En primer lugar, no consta que haya cumplido con el requisito del artículo 35.7.a) del RGPD, puesto que ninguno de los documentos aportados por la reclamada (ni el RAT ni este mal denominado "análisis de riesgos previo a la EIPD") contiene "*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*".

- No consta en este supuesto tampoco que la reclamada haya realizado un análisis previo de necesidad, proporcionalidad e idoneidad del nuevo método de acceso a través de reconocimiento facial, antes de tomar la decisión de su implantación, de acuerdo con lo exigido en el artículo 35.7.b), referido a incluir: *"una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad".*

> La única referencia que realiza al respecto es en el citado documento de "análisis de riesgos previo a la EIPD", cuando indica que "*En definitiva, se deduce que el sistema propuesto no resulta intrusivo ni atenta contra los derechos de los usuarios de los centros deportivos al no tratar ni almacenar su imagen personal ni ningún otro dato que permita identificarlos."*
>
> Dada su relevancia, se hará referencia a la misma en el apartado siguiente.

- Y se incumplió también con el requisito previsto en el artículo 35.7. d), sobre*: "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".*

> Al respecto de esta cuestión, y sin entrar en detalle sobre las posibles medidas que hubieran sido necesarias toda vez que no es labor de esta autoridad el identificarlas sino del propio responsable que conoce su organización y sistemas y debe determinar qué medidas son apropiadas en aplicación del Principio de Responsabilidad Proactiva, si se ha de señalar que las medidas de seguridad aplicadas al tratamiento que constan señaladas en el informe de inspector (punto quinto) no cumplen con el requisito previsto en el artículo 35.7.d) del RGPD, puesto que no son adecuadas para demostrar la conformidad del tratamiento con este RGPD, considerándose del todo insuficientes, e inadecuadas a los riesgos concurrentes, que no se habían analizado.
>
> Y es que, tanto las medidas que el fabricante dice aplicar a su software de reconocimiento facial, como las reflejadas en el RAT en torno a otros tratamientos relacionados con la gestión de clientes que puedan haberse aplicado a este tratamiento de control de acceso de los socios, son únicamente medidas de seguridad de carácter técnico, que además no contemplan la totalidad de las medidas que serían posibles en el estado actual de la técnica para afrontar los riesgos generados por este tipo de tratamiento de datos biométricos.
>
> Y es que para entender superado este requisito de la EIPD ésta deberá contener todas las medidas técnicas y organizativa apropiadas, de todo tipo, evitando la materialización de los daños y para garantizar los derechos y libertades de las personas físicas afectadas por el tratamiento.

7.2. En especial, sobre el requisito previsto en el artículo 35.7.b) referido a que el tratamiento sea necesario, idóneo y proporcional.

De la documentación aportada se deduce, además, que la empresa reclamada no ha realizado tampoco una valoración previa sobre la necesidad, idoneidad y proporcionalidad de su nuevo sistema de control de acceso de los socios a sus centros deportivos, cuyo análisis exhaustivo y superación debe ser documentada en la EIPD, según el artículo 35.7.b) del RGPD.

Hay que decir que la obligatoriedad de realizar esta previa evaluación se aplica a todo tratamiento y debe hacerse siempre (aunque el tratamiento no sea de alto riesgo), de acuerdo con lo previsto en el artículo 5.1.c) del RGPD recoge el denominado "Principio de minimización de datos personales" y dispone lo siguiente:

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

Así pues, el respeto de este principio **deberá ser el punto de partida del inicio de todo tratamiento**, debiendo plantearse el responsable si este tratamiento será realmente necesario, idóneo, y proporcional antes de iniciarlo -siendo incluso aconsejable, según la Guía de la EIPD de esta Agencia realizar esta evaluación antes de adoptar decisiones que le lleven a realizar grandes inversiones en un tratamiento que pueda resultar prohibido, por no cumplir con el requisito y principio esencial.

Por tanto, este previo análisis debe realizarse antes del inicio de cualquier tratamiento de datos personales, si bien cuando existe probabilidad de que el tratamiento entrañe un alto riesgo (como es el caso de los biométricos tratados en sistemas biométricos de control de acceso mediante reconocimiento facial o detección de huella dactilar) existe obligación de documentarlo dentro de la EIPD, toda vez que ésta debe contener "*b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad",* de acuerdo con el artículo 35.7. b) del RGPD.

Ello se confirma por el considerando 39 del RGPD, que subraya la importancia de que el tratamiento sea necesario, indicando que *"Los datos personales solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios*."

En la misma línea se pronuncia el Grupo de Trabajo del artículo 29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas.

La obligación de tratar únicamente "*los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados"* prevista por el principio de minimización de datos~~/~~ del artículo 5.1.c) del RGPD, y de evaluar la necesidad y proporcionalidad del tratamiento en la EIPD según el artículo 35.7 b) del RGPD, debe interpretarse de conformidad con lo previsto por la reiterada jurisprudencia de nuestro Tribunal Constitucional respecto a la necesidad de

constatar que toda medida restrictiva de derechos fundamentales (operaciones de tratamiento que comprenden datos biométricos en este caso) supera lo que se denomina como “el triple juicio de proporcionalidad”.

Ello implica que, antes que nada, es necesario constatar si cumple los tres siguientes requisitos o condiciones a los que se refiere el Tribunal Constitucional: *«si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto*)”.

La exigencia de realizar este triple juicio de proporcionalidad previo al tratamiento se especifica en lo que respecta a datos biométricos en el apartado 72, de las Directrices 3/2019 sobre el tratamiento de datos personales mediante dispositivos de vídeo, de 29/01/2020, del CEPD, que indica*: “El uso de datos biométricos y, en particular, del reconocimiento facial conllevan elevados riesgos para los derechos de los interesados. Es fundamental que el recurso a dichas tecnologías tenga lugar respetando debidamente los principios de licitud, necesidad, proporcionalidad y minimización de datos tal y como establece el RGPD. Aunque la utilización de estas tecnologías se pueda percibir como particularmente eficaz, los responsables del tratamiento deben en primer lugar evaluar el impacto en los derechos y libertades fundamentales y considerar medios menos intrusivos de lograr su fin legítimo del tratamiento.* Es decir, habría que responder la cuestión de si esta aplicación biométrica es algo que realmente es imprescindible y necesaria, o es solo “*conveniente*”.

En el presente supuesto, se señalan a continuación los motivos por los que a la vista de la documentación aportada y manifestaciones realizadas por la reclamada y reclamantes, **se entiende que el tratamiento realizado no superaría este triple juicio de proporcionalidad**, que de acuerdo con la referida doctrina del Tribunal Constitucional exige cumplir los 3 requisitos siguientes:

1. Si el tratamiento es susceptible de conseguir el objetivo propuesto **(juicio de idoneidad).**

> De acuerdo con el Tribunal Constitucional, el requisito de la idoneidad determinar primero *“si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad)”.* Esto es, se trata de determinar si el tratamiento (cada una de las operaciones que lo conforman) es adecuado para lograr las finalidades que se persiguen. Que el tratamiento sea la respuesta a determinadas carencias, demandas, exigencias como obligaciones u oportunidades objetivas y puede conseguir los objetivos propuestos con la eficacia suficiente.
>
> Y ello implica, según la Guía de EIPD 2021 (que la reclamada dice haber consultado), que el responsable del tratamiento deberá: (i) determinar los fines últimos del tratamiento que deben ser precisos, específicos, medibles y acotados,

(ii) establecer de forma objetiva, cualitativa y basada en evidencias, cuál es el umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento; (iii) evaluar de forma objetiva, cualitativa y basada en evidencias, la efectividad del tratamiento, tal y como se ha planteado, verificando si da respuesta a las necesidades planteadas y con qué extensión.

Lo que debe ser objeto de análisis de idoneidad es si el tratamiento que se pretende implantar es eficaz para cumplir con el objetivo, entendido como finalidad real del tratamiento. Tal y como señala la Guía sobre Gestión de Riesgo y EIPD de esta Agencia,_el análisis de eficacia implica definir primeramente cuáles son los umbrales de eficacia y error que tiene cada método analizado para cumplir la misma finalidad última del tratamiento, y determinar si realmente se podrá realizar la identificación del pasajero de forma más eficaz en comparación con los métodos tradicionales que utilizan la intervención humana, o éste nuevo método puede generar un mayor número de errores que lleve a denegar el registro de la jornada de cada empleado.

A estos efectos, es cierto que la empresa reclamada no ha fijado ni analizado los umbrales de eficacia ni tasas de error de los diversos sistemas de acceso a los centros que ha estado empleando a lo largo de los años (tarjetas identificativas, huella dactilar, reconocimiento facial, y exhibición de DNI), y en concreto, no señala porque es más efectivo para verificar la identidad de los socios el fichaje biométrico por reconocimiento facial que todos los otros métodos, pues se limita a indicar, únicamente, que decidió sustituir el sistema de huella dactilar por el de reconocimiento facial, ante los fallos técnicos detectados en su aplicación, sin concretar ni justificar cuales fueron. Pero no incluye tampoco ningún análisis de eficacia-idoneidad del resto de métodos de acceso que no emplean sistemas biométricos, como el de tarjetas identificativas y el de exhibición de DNI.

No obstante, a la vista del resto de documentación aportada, se puede considerar inicialmente que todos los métodos de acceso que presuntamente fueron implantados podrían ser idóneos para servir como método eficaz de verificación de identidad (identificación unívoca fiable) de los socios al objeto de permitir su entrada/ salida del mis, y denegar la de aquellos que no tuvieran esta condición, por lo que **no se cuestiona en principio la idoneidad** de los métodos de acceso que han sido implantados, siempre que el tratamiento se configure con las medidas y garantías adecuadas.

2. Si, además, el tratamiento de datos biométricos es necesario, en el sentido de que

no exista otra medida más moderada para la consecución de tal propósito con igual eficacia **(juicio de necesidad).**

Cuando se verifica si el tratamiento realizado es necesario se trata de determinar si la finalidad perseguida no puede alcanzarse de otro modo menos lesivo o invasivo, es decir si no existe un tratamiento alternativo menos intrusivo para los derechos y libertades de los interesados que sea igualmente o más eficaz y seguro para el logro de la finalidad perseguida.

Al respecto de esta cuestión, la empresa reclamada se limita a indicar en el referido "análisis de riesgos previo a la EIPD" que: "*En definitiva, se deduce que el sistema propuesto no resulta intrusivo ni atenta contra los derechos de los usuarios de los centros deportivos al no tratar ni almacenar su imagen personal ni ningún otro dato que permita identificarlos."*

Sin embargo, esta afirmación no se acompaña de argumentos válidos que justifiquen la necesidad de implantar un método de acceso biométrico (como el reconocimiento facial, o previamente, de huella dactilar), cuando existen otros métodos de acceso menos intrusivos para los derechos y libertades de los socios que son igualmente eficaces para servir de medio de identificación y control de acceso de los mismos, como el realizado mediante tarjetas identificativas y exhibición del DNI, que no implican el tratamiento de datos personales de categoría especial, ni generan los riesgos a los que se ha hecho referencia en el Fundamento de Derecho III.

- Así pues, la mayor parte de las reclamaciones unidas al presente procedimiento indican que anteriormente a implantar el sistema de reconocimiento facial el método de acceso se realizaba a través de un torno controlado por tarjeta magnética y de un sistema biométrico de reconocimiento de huella dactilar.

- Y por otra parte, señala expresamente que en su escrito de 1-4-24 que: *"En cualquier caso, todos los centros de Supera están preparados con sistemas alternativos de acceso, como el presencial clásico de exhibición del documento de identidad que se contrasta con los datos incluidos en el sistemas de Centros Supera", y que* con posterioridad a recibir 26 reclamaciones en el centro de Entrepuentes, habilitó este método de acceso en el mismo.

En general, la empresa reclamada confunde necesidad con utilidad del sistema de reconocimiento facial, puesto que dice haber analizado varios métodos de acceso con la siguiente finalidad u objetivo: "*La sociedad SIDECU, S.A. analizó diferentes modalidades de sistemas de acceso a sus centros deportivos, en virtud de los cuales se evitase, por un lado, el acceso de personas a los centros que no tuviesen la condición de abonados y, por otro lado, que cumpliesen con la condición de evitar el tratamiento de datos adicionales e innecesarios para los que hubiera que obtener el consentimiento expreso del usuario".*

Pero la necesidad no debe confundirse con utilidad del sistema. Obviamente, un sistema de control de acceso por reconocimiento facial puede ser útil y generar ventajas o beneficios para la propia empresa y los socios como los que señala la reclamada en este párrafo o en sus carteles informativos, cuando se indica que:

" *¿Qué ventajas tienen los sistemas biométricos?*
- Garantizan la identificación y verificación del usuario de una manera rápida, fácil y fiable.
- Es una tecnología robusta ampliamente estudiada y probada.
- Al utilizar una característica intransferible, no es posible el uso fraudulento de llaves remplazando la identidad de otras personas".

No cabe duda de que pueden concurrir estas ventajas y que éstas reporten beneficios para todos, pero lo que se trata de examinar en este requisito es si estos sistemas biométricos de verificación de identidad -además de útiles e idóneos- son objetivamente necesarios para cumplir con la finalidad de identificación unívoca del empleado (siendo esto último lo que realmente debe estar presente cuando se analiza el requisito de necesidad del tratamiento). O si, por el contrario, existen otros medios alternativos menos intrusivos que cumplan esta misma finalidad.

Como establece el dictamen 3/2012 sobre la evolución de las tecnologías biométricas- del GT 29-, debe examinarse "*si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable". S*e han de analizar las opciones y alternativas antes de instaurar un sistema nuevo que supone una elevada intromisión del derecho de cada usuario, cuando pueden existir medios menos invasivos de la intimidad, y no optar por lo práctico o ágil y cómodo, cuando están en juego derechos de sus titulares.

En casos como el presente, el responsable que se plantee implantar tratamientos de alto riesgo, como el que implican los datos biométricos de las personas, debe ser escrupuloso en su labor de analizar exhaustivamente todas las opciones alternativas que sean igual de idóneas y eficaces, pero menos intrusivas disponibles. Por consiguiente, se ha de documentar junto con la EIPD el estudio de la viabilidad de otras posibles opciones alternativas disponibles que no requieran el uso de datos especiales, comparar todas las opciones y documentar las conclusiones.

En el presente supuesto, la reclamada reconoce que existen otras alternativas que podrían emplearse para la misma finalidad, y que sin duda son menos intrusivas que los métodos de acceso basados en datos biométricos como el de huella dactilar o reconocimiento facial. Pero ni existe una EIPD ni consta que se haya elaborado o documentado un análisis de estas otras alternativas que la reclamada menciona.

Esto implica que el tratamiento realizado a través del sistema de acceso mediante reconocimiento facial al que se refiere el presente expediente **no superó el previo juicio de necesidad porque** no se ha justificado porqué la alternativa biométrica era necesaria para conseguir la finalidad de identificación unívoca de los

empleados, pese a existir, al menos, otros dos métodos de identificación no biométricos igualmente eficaces para identificar a los socios, que eran menos intrusivos para los derechos y libertades de los ciudadanos por no conllevar el tratamiento de datos biométricos de categoría especial y alto riesgo (acceso mediante tarjetas identificativas, y mediante exhibición del DNI).

2. Finalmente, habrá que analizar si el tratamiento mediante huella dactilar como método de acceso es ponderado o equilibrado, por derivarse de éste más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (**juicio de proporcionalidad en sentido estricto).**

Ello se determina, entre otras, en "*STC 66/1995, de 8 de mayo, F. 5; STC 55/1996, de 28 de marzo, FF. 7, 8 y 9; STC 270/1996, de 16 de diciembre, F. 4.e; STC 37/1998, de 17 de febrero, F. 8; STC 186/2000, de 10 de julio, F. 6*)."

En este aspecto, la gravedad del riesgo para los derechos y libertades del tratamiento, y su intromisión en el derecho fundamental a la Protección de Datos de carácter personal ha de ser adecuada al objetivo perseguido y proporcionada a la urgencia y gravedad de esta. Hay que ponderar el beneficio que el tratamiento desde el punto de vista de la Protección de Datos proporciona la sociedad, manteniendo un equilibrio con el impacto que representa sobre otros derechos fundamentales. Sin embargo, aunque pueda ceder parcialmente, en ningún caso se puede asumir la negación absoluta del derecho a la Protección de Datos y vaciarle de su contenido esencial.

Debe existir un vínculo lógico entre la medida y el objetivo legítimo perseguido. Para que se respete el principio de proporcionalidad, las ventajas resultantes de la medida no deben ser superadas por las desventajas que la medida provoca con respecto al ejercicio de derechos fundamentales. Y uno de los factores que juegan en la proporcionalidad es la eficacia de las medidas de las medidas existentes, por encima de la propuesta, si en el mismo contexto ya existieran medidas para un propósito similar o idéntico, deben considerarse, si no, la evaluación de la proporcionalidad no se ha realizado debidamente.

Vistas estas manifestaciones y la documentación aportada, cabe determinar sin lugar a dudas que la empresa tampoco ha acreditado haber realizado este análisis previo de proporcionalidad, puesto que no ha elaborado una EIPD ni documento en el que se ponderen las ventajas y desventajas de utilizar el sistema biométrico como sistema "primario" escogido para controlar y registrar el acceso al centro de los socios. Únicamente consta que colocó carteles informativos en los que se

informaba a los socios de 3 ventajas del sistema biométrico, sin hacer referencia a las desventajas ni a los riesgos que conllevan este tipo de tratamientos.

No se hace mención alguna ni se aportan evidencias de que la reclamada haya evaluado ni ponderado en este juicio ninguna de las desventajas o limitaciones del sistema biométrico ante el que nos encontramos, que no se mencionan ni consideran en ningún caso, ni tampoco existe una comparación de las ventajas-desventajas que tiene este sistema frente a las otras alternativas que dice haber analizado.

En definitiva, no existen evidencias de que se haya realizado tampoco un análisis previo de proporcionalidad (balance ventajas-desventajas o riesgo-beneficio).

No parece, por tanto, necesario ni proporcional, dada la existencia de medios menos intrusivos y la relación entre ventajas y desventajas, utilizar sistemas de control de acceso de personas que se basen en tratamientos de datos personales biométricos de categoría especial, cuando existen otros posibles métodos alternativos de control de acceso igual de eficaces que permitirían cumplir con la finalidad del tratamiento, que ya se emplean en la actualidad o han sido empleados en el pasado por la reclamada, por lo que existen evidencias de que el tratamiento implantado no supera tampoco la evaluación o triple juicio de proporcionalidad al que se refiere el artículo 35.7.b) del RGPD.

En conclusión, de conformidad con las evidencias de las que se dispone en el presente momento, y sin perjuicio de lo que resulte de la instrucción, se considera que los hechos expuestos podrían vulnerar lo establecido en el artículo 35 del RGPD, al no haberse elaborado una EIPD del tratamiento ni cumplir el tratamiento realizado con los requisitos mínimos previstos en dicho artículo.

VIII. Tipificación y calificación de la infracción del artículo 35 del RGPD.

Tal y como se ha expuesto en el Fundamento de Derecho anterior, se considera que los hechos expuestos podrían vulnerar lo establecido en el artículo 35 del RGPD, lo que podría suponer la comisión de una infracción administrativa tipificada en el artículo 83.4.a) del RGPD que indica que:

"*Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:*
a) *Las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43*."

A los efectos de prescripción, la LOPDGDD establece en su artículo 73.t) que: "*En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se*

consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:

t) El tratamiento de datos personales sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible."

IX. Sanción por la infracción del artículo 35 del RGPD.

En este caso, considerando la gravedad de la infracción constatada respecto a la vulneración del artículo 35 del RGPD, de acuerdo con las previsiones normativas que se han hecho constar en el Fundamento de Derecho VI contenidas en el artículo 83 del RGPD y 76 de la LOPDGDD, y atendiendo especialmente a las consecuencias que su comisión provoca en los interesados, se entiende que procedería imponer una sanción de multa.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, la condición de gran empresa, y el volumen de negocio de la parte reclamada en el año 2023.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias de graduación de la sanción siguientes, contempladas en los preceptos antes citados:

- Art. 83.2.a) RGPD: "*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*".

  La conducta en la que se concreta la naturaleza de infracción atribuida al reclamado afecta a una obligación esencial en materia de protección de datos, que es la referida a la elaboración de una EIPD del tratamiento que cumpla con los requisitos previstos en el artículo 35 del RGPD, lo que está sancionado como se ha dicho, con multa de hasta 10 millones de euros o el 2% del volumen de negocios de la reclamada.

  Se tiene en consideración que SIDECU no realizó ninguna EIPD del tratamiento. Y se considera, así mismo, que el tratamiento implantado incumplía, así mismo, los 4 requisitos mínimos que señala el artículo 35.7 del RGPD, en el grado que se ha señalado en el Fundamento de Derecho VII de este acuerdo. Y en especial, se considera que no se ha justificado que el tratamiento mediante sistemas biométricos fuera necesario ni proporcional en este supuesto, a la vista de la existencia de otros métodos de control de acceso disponibles en el centro

que le hubieran permitido cumplir con la misma finalidad de forma menos intrusiva para los derechos y libertades de los interesados.

Así mismo, se considera para graduar la sanción inicial el número de afectados que se corresponde con el número de socios cuyos datos personales han sido objeto de tratamiento mediante el sistema de acceso basado en reconocimiento facial en los 5 centros deportivos que han sido señalados por la reclamada, sin perjuicio de que durante la instrucción se acredite un número diferente de afectados.

Por lo que respecta a la duración de la infracción, se considera que la misma se ha cometido de forma continuada, durante el periodo que ya ha sido indicado en el Fundamento de Derecho VI respecto a la infracción del artículo 9 del RGPD.

- Art. 83.2b) "*la intencionalidad o negligencia en la infracción*".

Como responsable de la implantación de un nuevo sistema de acceso de los socios que incluye el tratamiento de una categoría de datos personales cuyo tratamiento implica alto riesgo (datos biométricos de las personas), la empresa reclamada viene obligada a actuar con la especial diligencia que es exigible a este tipo de tratamientos, dados los elevados riesgos que genera su utilización.

A propósito del nivel 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, que ha sido citada anteriormente.

Aplicando esta doctrina al presente supuesto, la falta de diligencia concurrente debe calificarse de "grave", dado que se llegó a la conclusión de que no era necesaria una EIPD ni cumplir con el resto de requisitos previstos en el RGPD en base a un análisis erróneo de la naturaleza jurídica de los datos tratados por el software de ***EMPRESA.1 que no fue realizado con el rigor necesario, dejando patente su falta de diligencia al desconocer incluso cómo se realiza un análisis de riesgos previo a la EIPD y los requisitos que éste debe cumplir, así como que el análisis de necesidad, idoneidad y proporcionalidad debía ser el punto de partida, antes de tomar cualquier decisión que implicase el inicio del tratamiento.

Si bien se elaboró un documento de 2 páginas para hacer constar que no era necesario, a su juicio, elaborar una previa EIPD, este demuestra que el mismo pretendía cumplir con un requisito formal, pero no estaba sustentado por un verdadero análisis de riesgos ni de cumplimiento de la normativa, poniendo de manifiesto una actitud de incumplimiento sistémico que contradice los principios y reglas básicas de la gestión del riesgo y la evaluación de impacto a las que se refiere el nuevo RGPD. Puesto que el análisis realizado adolece de elementos esenciales y básicos que deberían haber sido examinados como parte del análisis de riesgos previo obligatorio, aunque no hubiera sido obligatorio realizar una EIPD. Y la ausencia de estos elementos esenciales dificulta el posterior cumplimiento de las obligaciones del responsable. Toda vez que existen

evidencias de haber incumplido los 4 requisitos mínimos que establece el artículo 35.7 del RGPD.

- Artículo 83.2.g) del RGPD: "La afectación a una de las categorías especiales de datos": al haber procedido a tratar datos biométricos (patrón facial extraído de la cara de los socios) cuya necesidad de protección es en esa medida superior a la de otros datos personales, de acuerdo con lo señalado por el Tribunal Constitucional en la sentencia 76/2019, de 22/05/2019, recurso 1405/2019, lo cual supone una agravante, de acuerdo con el artículo 83.2.g) del RGPD "las categorías de los datos de carácter personal afectados por la infracción".

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 35 del RGPD, permite fijar inicialmente una sanción de multa administrativa de **50.000 € (CINCUENTA MIL EUROS).**

X

Obligación incumplida del artículo 13 de RGPD. Información que deberá facilitarse cuando los datos personales se obtengan del interesado.

Una de las obligaciones del responsable de todo tratamiento de datos personales es cumplir con los deberes de información a los interesados que vienen previstos en los artículos 12 a 14 del RGPD.

De acuerdo con lo previsto en el artículo 12.1 de RGPD, se parte de un Principio de "Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado" (el subrayado es nuestro):

> "1. *El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios*"

Estos deberes de información se concretan en los artículos 13 y 14, siendo de aplicación al supuesto presente, los previstos en el artículo 13 del RGPD sobre "*Información que deberá facilitarse cuando los datos personales se obtengan del interesado" (el subrayado es nuestro):*

> 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.
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 el presente supuesto, se entiende que la empresa decidió implantar el nuevo método de acceso, como único medio obligatorio para los socios de estos 5 centros

deportivos, sin haberles informado previamente de que se iba a realizar un tratamiento de sus datos biométricos de categoría especial con la transparencia y condiciones exigidas por el artículo 12, e incluyendo todos de los aspectos exigidos por dicho artículo 13 del RGPD.

Dicha información debe prestarse, según lo previsto en los artículos 12 y 13 del RGPD "*en el momento en que se obtengan los datos personales", que en el caso presente fue* el momento de recogida de los datos personales biométricos de los socios (muestra de la cara para extraer el patrón facial), lo que significa que si la empresa informó posteriormente a esta fecha se entendería que habría incumplido igualmente con la obligación prevista en estos preceptos.

Este deber de información previa puede realizarse a través de diversas vías, siendo la reclamada la que tiene el deber de acreditar que el mismo se ha producido en cada caso, con respecto a cada persona de forma individual, con carácter previo al momento de recogida de sus datos biométricos. Por tanto, en caso de comunicaciones generales mediante carteles informativos, es preciso que el responsable del tratamiento arbitre procedimientos y garantías para asegurarse de que cada uno de los socios que accedió a que sus datos biométricos fueran recogidos, conocía que sus datos biométricos de categoría especial iban a ser tratados, con qué finalidad y riesgos, y todos los aspectos relacionados en el artículo 13 del RGPD (responsable del tratamiento, cómo y ante quien ejercer sus derechos de acceso, rectificación…etc).

En el presente supuesto, no consta que los socios hayan firmado ningún documento expreso en el que se incluyera la información del artículo 13 del RGPD en relación con el tratamiento de estos datos biométricos que iba a realizarse al emplear el sistema de reconocimiento facial, que se hubiera entregado y firmado en el momento de recogida de los mismos, previamente al primer acceso, que debió producirse entre los meses de julio-agosto de 2023, según se ha indicado. Ni que éstos recibieran una comunicación individual informando de estos aspectos en relación con el tratamiento biométrico previamente a la recogida de estos datos (mediante correo electrónico, carta,..etc).

Es más, hay evidencias de lo contrario, toda vez que consta que todas las reclamaciones y denuncias presentadas en el presente procedimiento, presentaron una reclamación previa ante la reclamada, en la que solicitaban su consentimiento para el tratamiento de datos biométricos, y que la empresa les contestaba que éste no era necesario, en los siguientes términos: *"el sistema implantado no almacenaba la imagen, ni suponían un riesgo para los datos personales de los usuarios y no era necesario recabar un consentimiento previo puesto que, dadas las características del sistema, ni se guardaba la imagen ni ningún dato que permitiese identificar al usuario, no realizando tratamiento alguno de datos"*.

Por otra parte, como ya se ha anticipado en diversas ocasiones a lo largo de este acuerdo, consta reconocido por la empresa que no recabó un consentimiento expreso para tratar datos biométricos de categoría especial, por lo que se descarta también la posibilidad de que la información previa en relación al mismo se constase en un hipotético documento de consentimiento al tratamiento de los datos biométricos.

Así pues, la empresa reclamada ha reconocido que entendió que el software empleado para el reconocimiento facial no trataba datos personales ni datos biométricos de categoría especial, por lo que no recabó de los socios ningún documento de consentimiento expreso por el que estos accedieran a que sus datos biométricos fueran recogidos a los fines de permitirles el acceso a los centros en los que eran abonados. Y así lo recogió en su documento de "análisis de riesgos previo a una EIPD" que ha sido analizado en el Fundamento de Derecho relativo al incumplimiento del artículo 35 del RGPD.

Es más, se puede ver como no recabar el consentimiento expreso de los socios fue uno de los objetivos que perseguía la empresa cuando analizó las diferentes opciones de control de acceso, puesto que en su escrito de 19-1-24, indicó expresamente que: "*La sociedad SIDECU, S.A. analizó diferentes modalidades de sistemas de acceso a sus centros deportivos, en virtud de los cuales se evitase, por un lado, el acceso de personas a los centros que no tuviesen la condición de abonados y, por otro lado, que cumpliesen con la condición de evitar el tratamiento de datos adicionales e innecesarios para los que hubiera que obtener el consentimiento expreso del usuario".*

Tampoco consta que en la documentación de alta de los usuarios se autorice a este tratamiento de datos biométricos ni que se informe de los aspectos del artículo 13 del RGPD en relación a los mismos. Como se puso de manifiesto en el informe del inspector y se ha hecho constar en el Fundamento de derecho IV al tratar el incumplimiento del artículo 9 del RGPD, consta que para poder inscribirse en los centros deportivos y acceder a los servicios contratados, los socios firmaban una hoja de inscripción, por la que aceptaban las condiciones generales y reglamento de régimen interno que fueron diligenciada por el inspector del procedimiento.

En esta documentación contractual, solamente consta una cláusula general de protección de datos personales en la que no se hace referencia al tratamiento biométrico, por lo que se descarta igualmente que al suscribir el contrato los socios fueran informados de este tipo de tratamiento biométrico. Y ello se reconoce por la reclamada expresamente, cuando indica que: ""*Si bien es cierto, que en la documentación de alta de usuario no aparece contemplada la autorización para la recogida de datos personales relativos al uso de datos biométricos o de categorías especiales, ello es debido a que, atendiendo a las características del funcionamiento del sistema de acceso, no solo no se guarda la imagen de los usuarios por parte de SIDECU, S.A. como teórico responsable del tratamiento, sino que no se conserva ningún tipo de dato personal, pues la plantilla generada por el sistema no permite la asociación a ninguna persona concreta.*

La reclamada señala que prestó información del nuevo método de acceso mediante reconocimiento facial a todos los socios, asegurándose de que en cada centro deportivo se colocaban carteles informativos, y aporta la fotografía de los carteles que la reclamada dice haber colocado en cada uno de los centros deportivos, en las que se puede comprobar que cada cartel se encabeza con el nombre de cada uno de estos 5 centros deportivos.

Así pues, en la respuesta al traslado de las 3 primeras reclamaciones, SIDECU indica que: *"Habida cuenta que los tres usuarios son abonados del centro deportivo Supera Entrepuentes de Sevilla, se ha investigado internamente cuales han podido ser las*

causas que han motivado que estos tres usuarios presentasen la referida reclamación y si ese centro estaba ofreciendo a sus usuarios la información mediante la publicación de los carteles informativos en las instalaciones y a través del personal que trabaja en las mismas con motivo del cambio en el sistema de acceso. Se ha comprobado y verificado que el centro deportivo ha incorporado en un lugar visible y accesible a todos los usuarios los carteles informativos que proporcionan a los usuarios la información necesaria acerca del uso de este sistema y en el que se les traslada que este sistema no trata ningún dato personal". Y, en cada uno de sus 3 escritos posteriores, SIDECU contesta en relación con este deber de información previa lo siguiente: *"En cualquier caso, desde SIDECU se acordó que en todos los centros deportivos se colocaría en un lugar visible un cartel informativo acerca de estos sistemas con el fin de informar a los usuarios acerca de la protección de datos de carácter personal, del funcionamiento de los lectores y de su alcance".*

En las fotografías de los 5 carteles informativos que SIDECU dice haber colocado en un lugar visible, consta que, a excepción del encabezamiento referido al nombre de cada centro, dicho cartel siempre tiene el contenido siguiente:

> *"¿Qué es un sistema de identificación biométrico?*
> *Este tipo de sistemas biométricos utilizan alguna característica física e intransferible de la persona para realizar su identificación o verificación. Los sistemas biométricos de ***EMPRESA.1, extraen los puntos de datos faciales de las imágenes sin procesar y crea una plantilla a partir de estos datos.*
>
> *¿Qué ventajas tienen los sistemas biométricos?*
> *- Garantizan la identificación y verificación del usuario de una manera rápida, fácil y fiable.*
> *- Es una tecnología robusta ampliamente estudiada y probada.*
> *- Al utilizar una característica intransferible, no es posible el uso fraudulento de llaves remplazando la identidad de otras personas.*
>
> *¿Privacidad y protección del usuario?*
> *Los sistemas biométricos de ***EMPRESA.1 no guardan la imagen procesada, crea una plantilla con el algoritmo NIR patentado por ***EMPRESA.1. Mediante complejos algoritmos matemáticos se genera la plantilla numérica utilizando la información de algunos puntos de la captura. En ningún se puede deducir a partir de la plantilla características físicas, el algoritmo de extracción sólo es conocido por el fabricante.*
>
> *Funcionamiento*
> *La plantilla de la cara no es una imagen en bruto. Se crea utilizando la tecnología y el algoritmo NIR patentados de ***EMPRESA.1, y la plantilla es un conjunto de datos que es una fusión de características 2D y 3D de la cara de un usuario la cual es adquirida por una cámara visual y una cámara NIR. Para proteger esta plantilla, se utilizan herramientas criptográficas y métodos de encriptación, como la encriptación AES de 256 bits."*

No obstante, **dicho cartel informativo no acredita que la reclamada cumpliera con este deber de informar previamente a cada uno de los socios** que accedieron a

través del sistema de reconocimiento facial de todos los aspectos del tratamiento a los que hace referencia el artículo 13 del RGPD, toda vez que:

1. No consta fecha de colocación del cartel, sin que se haya aportado por la reclamada documentación alguna que pueda acreditar en qué fecha se colocaron los mismos, por lo que no consta acreditado que dichos carteles fueran colocados con carácter previo o en el mismo momento de recogida del primero de los datos biométricos que eran precisos para poner en marcha el sistema de reconocimiento facial, tal y como exigen los artículos 12 y 13 del RGPD.

2. No es visible el lugar de colocación, a los efectos de asegurar que estuvo a la vista y era accesible a los socios previamente a acceder a la recogida de sus datos biométricos.

3. A la vista del contenido del cartel, se observa que la empresa no informó a los socios de que el nuevo método de acceso a los centros mediante reconocimiento facial implicaba un tratamiento de sus datos personales biométricos, ya que les proporcionó información incorrecta sobre el funcionamiento del sistema, en base a la interpretación errónea que realizaron de los certificados del fabricante, sin consultar ni analizar debidamente la naturaleza jurídica del patrón facial que generaba, almacenaba y explotaba el software de ***EMPRESA.1.

   Y, lo que es más grave, no solo no se cumplió con el deber de informar que el nuevo método de acceso por reconocimiento facial -que era único y obligatorio-precisaba recabar sus datos biométricos personales y que ello era de alto riesgo, e implicaba el tratamiento de datos personales de categoría especial. Sino que la empresa fue más allá, señalando que ni siquiera se iban a tratar datos personales a través de este nuevo método.

   Y en consecuencia, al entender que no había tratamiento de datos personales, no se ofreció ninguna información acerca de los aspectos exigidos en el artículo 13 del RGPD (identidad y datos del responsable del tratamiento, del DPD en su caso, base jurídica y finalidad del tratamiento, destinatarios de los datos, el plazo de conservación de los datos, la posibilidad de ejercer los derechos de acceso, rectificación, supresión, limitación u oposición, derecho a presentar una reclamación ante esta Agencia…etc).

En definitiva, de los documentos obrantes en el expediente y sin perjuicio de aquellos que se aporten durante la instrucción, en el presente momento se deducen evidencias suficientes de que SIDECU ha estado recogiendo datos personales biométricos (patrón facial), almacenándolos y explotándolos con la finalidad de controlar el acceso de los socios que accedieron mediante este sistema de reconocimiento facial a estos 5 centros deportivos, sin informarles adecuadamente de todos los aspectos exigidos a efectos de protección de datos, por lo que cabría imputarle asimismo una infracción por incumplimiento del deber del artículo 13 del RGPD.

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción del artículo 13 del RGPD, imputable a ***SIDECU***, por vulneración del artículo transcrito anteriormente.

X. Tipificación de la infracción del artículo 13 del RGPD y calificación a efectos de prescripción.

El artículo 83.4 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

"a) las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43;
b) las obligaciones de los organismos de certificación a tenor de los artículos 42 y 43;
c) las obligaciones de la autoridad de control a tenor del artículo 41, apartado 4."

Por su parte, la LOPDGDD, a los solos efectos del plazo de prescripción en su artículo 72.1, establece lo siguiente:

> *"Artículo 72. Infracciones consideradas muy graves.*
>
> *1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran 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: (..)*
> *h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica"*

XI. Sanción por la infracción del artículo 13 del RGPD.

En este caso, considerando la gravedad de la infracción constatada respecto a la vulneración del artículo 35 del RGPD, de acuerdo con las previsiones normativas que se han hecho constar en el Fundamento de Derecho VI contenidas en el artículo 83 del RGPD y 76 de la LOPDGDD, y atendiendo especialmente a las consecuencias que su comisión provoca en los interesados, se entiende que procedería imponer una sanción de multa.

La multa que se imponga deberá ser, en cada caso individual, efectiva, proporcionada y disuasoria, conforme a lo establecido en el artículo 83.1 del RGPD. Para garantizar estos principios, se considera, con carácter previo, el volumen de negocio de ***SIDECU*** que se ha hecho constar en el hecho octavo de **16.154.950 euros** en el año 2023.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de

acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que procede graduar la sanción a imponer de acuerdo con las circunstancias siguientes, contempladas en los preceptos antes citados:

- Art. 83.2.a) RGPD: "*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*".

  La conducta en la que se concreta la naturaleza de infracción atribuida al reclamado afecta a una obligación esencial en materia de protección de datos, que es la referida al deber de informar al afectado por el tratamiento sobre los aspectos señalados en el artículo 13 del RGPD, lo que está sancionado como se ha dicho, con multa de hasta 20 millones de euros o el 4% del volumen de negocios de la reclamada.

  Se tiene en consideración que SIDECU no informó de ninguno de los aspectos del artículo 13 del RGPD, y que, además, colocó carteles informativos y respondió a las reclamaciones presentadas por los socios señalando que el nuevo sistema de reconocimiento facial de ***EMPRESA.1 no implica el tratamiento de ningún dato personal.

  Así mismo, se considera para graduar la sanción inicial el número de afectados que se corresponde con el número de socios cuyos datos personales han sido objeto de tratamiento mediante el sistema de acceso basado en reconocimiento facial en los 5 centros deportivos, partiendo del número que ha sido señalado por la reclamada, sin perjuicio de que durante la instrucción se acredite un número diferente de afectados.

  Por lo que respecta a la duración de la infracción, se considera que la misma se ha cometido de forma continuada, durante el periodo que ya ha sido indicado en el Fundamento de Derecho VI respecto a la infracción del artículo 9 del RGPD.

- Art. 83.2b) "*la intencionalidad o negligencia en la infracción*".

  Como responsable de la implantación de un nuevo sistema de acceso de los socios que incluye el tratamiento de una categoría de datos personales cuyo tratamiento implica alto riesgo (datos biométricos de las personas), la empresa reclamada viene obligada a actuar con la especial diligencia que es exigible a este tipo de tratamientos, dados los elevados riesgos que genera su utilización, que incluye el deber de informar debidamente de éstos en el momento de recogida de los datos personales, además de los aspectos generales que prevé el artículo 13 del RGPD.

  A propósito del nivel 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, que ha sido citada anteriormente.

Aplicando esta doctrina al presente supuesto, la falta de diligencia concurrente debe calificarse de “grave”, no solo porque se colocaron carteles informativos en los que no se daba a conocer que se tratasen datos biométricos, ni datos personales de ningún tipo, y la reclamada podía haber sido consciente de ello de haber actuado con la diligencia exigible a un responsable para determinar la naturaleza jurídica del tratamiento, antes de llegar a la conclusión de considerar que no existía tratamiento de datos personales en este supuesto, y omitir en consecuencia el cumplimiento de obligaciones tan esenciales como la de informar del tratamiento, sus finalidades, categorías de datos, bases de licitud, riesgos así como todos los aspectos previstos en el artículo 13 del RGPD. Todo a ello, pese a que los socios le advirtieron de que ello suponía un tratamiento de datos biométricos de categoría especial, sin que conste que la responsable actuase con la debida diligencia para analizar profundamente la normativa, guías y directrices que estaban aprobadas acerca de esta cuestión Es más, consta que los socios plantearon dudas acerca de si el nuevo método implicaba un tratamiento de datos personales biométricos, y la empresa reclamada persistió en su versión inicial, y pese a ello, no analizó exhaustivamente esta cuestión, examinando las guías y directrices sobre tratamiento de datos biométricos que le hubieran permitido deducir fácilmente que un patrón facial si es un dato biométrico, ni recabó la ayuda de expertos, ni formuló una consulta previa.

- Artículo 83.2 g) “*las categorías de los datos de carácter personal afectados por la infracción*”. En el presente caso, el tratamiento realizado sobre el que no se han cumplido los deberes de información previa afecta a una de las categorías especiales de datos, los datos biométricos, cuya necesidad de protección es superior a la de otros datos personales, de acuerdo con lo señalado por el Tribunal Constitucional en la sentencia 76/2019, de 22/05/2019, recurso 1405/2019.

- Artículo 76.2.f) de la LOPDGDD. *La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.* A este respecto, como ya se ha indicado anteriormente, por la actividad a la que se dedica SIDECU, se entiende que trata numerosos datos personales y de forma continua de los socios inscritos en los 33 centros que gestiona.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 13 del RGPD, permite fijar inicialmente una sanción de multa administrativa de **30.000 € (TREINTA MIL EUROS).**

XII. Medidas correctivas.

De confirmarse la infracción, la resolución que se dicte podrá establecer las medidas correctivas que la entidad infractora deberá adoptar para poner fin al incumplimiento de la legislación de protección de datos personales, en este caso del Artículo 9 del RGPD y Artículo 13 del RGPD, de acuerdo con lo establecido en el citado artículo 58.2.d) del RGPD, según el cual cada autoridad de control podrá “*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…”*

Así, se podrá requerir a la entidad responsable para que adecúe su actuación a la normativa de protección de datos personales, con el alcance expresado en los anteriores Fundamentos de Derecho.

En el presente acto se establece cuáles son las presuntas infracciones cometidas y los hechos que podrían dar lugar a esa posible vulneración de 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.

No obstante, en este caso, con independencia de lo anterior, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, en la resolución que se adopte se podrá requerir a SIDECU para que adopte las medidas siguientes:

- **En el plazo de 7 meses**, acredite haber realizado y superado una EIPD del tratamiento de control de acceso de sus socios a los centros gestionados por la misma, que contenga un previo análisis de riesgos, y la evaluación del triple juicio de idoneidad, necesidad y proporcionalidad del tratamiento llevado a cabo, determine si concurre alguna de las excepciones del artículo 9.2.del RGPD, así como las medidas de protección adecuadas, y el resto de obligaciones requeridas por la normativa de protección de datos personales.

  En caso de que alguna de las operaciones de tratamiento en que se concretan los métodos de acceso que se pretenden implantar no supere el triple juicio señalado, y/o no concurra la excepción que permita tratar datos biométricos, o no sea posible cumplir con alguna de las obligaciones previstas en la normativa de protección de datos, SIDECU no podrá llevar a cabo la operación/es de tratamiento de que se trate, debiendo acreditar tal circunstancia ante esta Agencia.

- En el plazo de **1 mes**, a contar desde la fecha de ejecutividad de la resolución finalizadora de este procedimiento, acrediten la puesta a disposición a los afectados de la información a la que se refieren el artículo 13 RGPD respecto al tratamiento de los datos biométricos personales realizados, previamente a implantarlos, en caso de que se cumpla con los requisitos anteriores.

La imposición de estas medidas es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

Se advierte que no atender la posible orden de adopción de medidas impuestas por este organismo en la resolución del presente procedimiento sancionador podrá ser considerado como una infracción administrativa conforme a lo dispuesto en el RGPD, tipificada como infracción en su artículo 83.5 y 83.6, pudiendo motivar tal conducta la apertura de un ulterior procedimiento administrativo sancionador.

Asimismo, se recuerda que ni el reconocimiento de la infracción cometida ni, en su caso, el pago voluntario de las cuantías propuestas, eximen de la obligación de adoptar las medidas pertinentes para que cese la conducta o se corrijan los efectos de la infracción cometida y la de acreditar ante esta AEPD el cumplimiento de esa obligación.

XIII. Suspensión provisional del tratamiento

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 estas medidas es compatible entre sí.

En especial, cabe referenciar el artículo 69.1 y 2 de la LOPDGDD dispone lo siguiente:

> **"***1. Durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, la Agencia Española de Protección de Datos podrá acordar motivadamente las medidas provisionales necesarias y proporcionadas para salvaguardar el derecho fundamental a la protección de datos y, en especial, las previstas en el artículo 66.1 del Reglamento (UE) 2016/679, el bloqueo cautelar de los datos y la obligación inmediata de atender el derecho solicitado.*
> *2. En los casos en que la Agencia Española de Protección de Datos considere que la continuación del tratamiento de los datos personales, su comunicación o transferencia internacional comportará un menoscabo grave del derecho a la protección de datos personales podrá ordenar a los responsables o encargados de los tratamientos el bloqueo de los datos y la cesación de su tratamiento y, en caso de incumplirse por estos dichos mandatos, proceder a su inmovilización."*

En el supuesto presente, tal y como ha sido indicado, cabe considerar al tratamiento consistente en el control de acceso (entrada y salida) de los socios implantado por SIDECU como un solo tratamiento de datos personales al menos a 5 de sus 33 centros deportivos, se realiza, al menos, desde los meses de julio-agosto de 2023 mediante un sistema de identificación a través de reconocimiento facial. Y que, anteriormente, se empleaba un sistema de acceso mediante tarjetas magnéticas o identificación biométrica a través de huella dactilar. Y actualmente, a raíz de las reclamaciones presentadas, ha habilitado un nuevo método de acceso a través de exhibición de DNI en el centro de Entrepuentes.

En principio, no existen evidencias de que el método de acceso a través de tarjetas magnéticas ni el referido a la exhibición del DNI incumplan la normativa de protección de datos personales. Sin embargo, este no es el caso de los métodos de acceso biométricos, puesto que de las actuaciones de investigación practicadas se deducen evidencias que, de confirmarse durante la fase de instrucción, podrían suponer la comisión de tres infracciones administrativas por incumplimiento de los artículos 9, 35 y 13 del RGPD, tal y como se ha expuesto en el presente Acuerdo de Inicio.

A fecha del presente Acuerdo de Inicio, no consta que la empresa reclamada haya cesado en el tratamiento de datos biométricos de categoría especial, sin que ésta ni los reclamantes hayan comunicado a esta Agencia que se hallan deshabilitado los métodos de acceso a través de sistemas biométricos actualmente empleados en estos centros deportivos (reconocimiento facial). Y tampoco se ha acreditado que se haya habilitado el método de acceso a través de exhibición del DNI en el centro de Entrepuentes. Y pese a haberse señalado que el método basado en reconocimiento facial ha sustituido al anterior de huella dactilar, no se ha concretado ni acreditado que el sistema de huella dactilar se haya deshabilitado en la totalidad de los centros gestionados por la reclamada (33 según la diligencia de 2 de abril de 2025).

Tal y como ha sido expuesto a lo largo del presente acuerdo de inicio, hay indicios y evidencias constatadas que recomiendan no continuar con el tratamiento de los datos personales biométricos que implican a categorías especiales de datos personales y entrañan un alto riesgo de carácter muy significativo.

La continuación del tratamiento de las operaciones de tratamiento correspondientes a ambos sistemas biométricos mencionadas podría comportar un menoscabo muy grave e irreparable para los derechos de esos usuarios. Por tanto, la suspensión temporal de los mismos es la única medida susceptible de ser adoptada para salvaguardar el Derecho Fundamental a la Protección de Datos, resultando ser, además, la menos lesiva, onerosa, proporcional y efectiva, así como la más proporcional y efectiva para el denunciado.

Desde estas premisas y a fin de garantizar los derechos y libertades de los afectados, se estima procedente imponer una medida provisional que evite lo antes posible la continuación del tratamiento de los datos personales a través de las operaciones de tratamiento que la parte reclamada, por lo que la empresa **deberá acreditar que ha suspendido temporalmente en todos sus centros el uso del método de acceso a través de sistemas biométricos**, medida que podrá levantarse o confirmarse, dictando la correspondiente medida de suspensión o cese definitivo de estos sistemas de fichaje.

Esta medida no impediría a la empresa reclamada el seguir controlando el acceso de las personas autorizadas a sus centros, de forma correcta y legal con los otros sistemas que ya está utilizando, como el de exhibición de DNI al personal que dice haber habilitado tras recibir 26 reclamaciones en el centro de Entrepuentes, o como el que ha utilizado en el pasado según manifiestan los reclamantes, como el acceso mediante tornos con tarjetas magnéticas, por lo que la suspensión de los sistemas de acceso biométricos no le supone un coste o esfuerzo desproporcionado ni le impide continuar cumpliendo con su obligación legal de vigilar y controlar el acceso de sus socios a sus centros.

En consecuencia, conforme dispone el art 83.2 del RGPD y el artículo 76.3 de la LOPDGDD arriba transcritos, cabe imponer mediante el presente Acuerdo de Inicio de expediente sancionador la medida provisional de ordenar, de acuerdo con lo dispuesto en el art. 69 de la LOPDGDD, la suspensión temporal de todo tratamiento de datos personales biométricos -y en especial de los referidos al sistema de reconocimiento facial, y si existiera, de detección de huella dactilar- como método de control de entrada y salida a sus centros. Toda vez que la suspensión provisional del tratamiento se considera necesaria, proporcional, efectiva para garantizar los derechos y libertades en liza de los afectados y de menor onerosidad para el denunciado.

La medida provisional deberá llevarse a cabo desde la notificación del presente acuerdo de inicio de procedimiento sancionador hasta su resolución final, en que deberá ser confirmada, modificada o levantada.

Por lo tanto, a tenor de lo anteriormente expuesto, por la Presidencia de la Agencia Española de Protección de Datos

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ***SIDECU, S.A.***, con NIF ***A15435092***, por la presunta comisión de tres infracciones administrativas:

- Por la presunta infracción del artículo 9 del RGPD, tipificada en el artículo 83.5.a) del RGPD.
- Por la presunta infracción del artículo 35 del RGPD, tipificada en el artículo 83.4.a) del RGPD
- Por la presunta infracción del artículo 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD.

SEGUNDO: ORDENAR como medida provisional a **SIDECU, S.A** , con NIF ***A15435092***, de acuerdo con lo dispuesto en el artículo 69 de la LOPDGDD, la suspensión temporal de todo tratamiento de datos personales biométricos de categoría especial como método de control de acceso (entrada y salida) a sus centros deportivos. La medida provisional deberá llevarse a cabo en el plazo de diez días hábiles, contados desde la notificación de este acuerdo de apertura del procedimiento, y permanecerá hasta su resolución final, en que deberá ser confirmada, modificada o levantada. A tal fin, deberá justificar ante esta Agencia Española de Protección de Datos la atención del presente requerimiento.

TERCERO: NOMBRAR como instructora a ***S.S.S.*** y, como secretaria, a ***R.R.R.***, indicando que podrán ser recusadas, en su caso, conforme a lo establecido en los artículos 23 y 24 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (LRJSP).

CUARTO: INCORPORAR al expediente, a efectos probatorios, la reclamación interpuesta por la parte reclamante y su documentación, así como, así como los documentos obtenidos y generados por la Subdirección General de Inspección de Datos en las actuaciones previas al inicio del presente procedimiento sancionador.

QUINTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la

sanción que pudiera corresponder sería de multa administrativa de las siguientes cuantías, sin perjuicio de lo que resulte de la instrucción:

- Por la presunta infracción del artículo 9 del RGPD, una sanción de multa de 80.000 euros.
- Por la presunta infracción del artículo 35 del RGPD, una sanción de multa de 50.000 euros.
- Por la presunta infracción del artículo 13 del RGPD, una sanción de multa de 30.000 euros.

Todo lo cual, asciende a una cantidad total de **160.000 euros** (CIENTO SESENTA MIL EUROS).

SEXTO: NOTIFICAR el presente acuerdo a ***SIDECU, S.A.***, con NIF ***A15435092***, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en **128.000** euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en **128.000** euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **96.000 euros**.

En todo caso, la efectividad de cualquiera de las dos reducciones mencionadas estará condicionada al desistimiento o renuncia expresos de cualquier acción o recurso en vía administrativa contra la sanción.

A estos efectos, en caso de acogerse a alguna de ellas, deberá remitir a la Subdirección General de Inspección de datos comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción indicando a cuál de las dos reducciones se acoge o si es a las dos.

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente **(128.000** euros o **96.000 euros**), deberá hacerlo efectivo

mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

Asimismo, deberá enviar el justificante del ingreso a la Subdirección General de Inspección junto con la comunicación expresa del desistimiento o renuncia a cualquier acción o recurso en vía administrativa contra la sanción para continuar con el procedimiento en concordancia con la cantidad ingresada.

Por último, se señala que conforme a lo establecido en el artículo 112.1 de la LPACAP, contra el presente acto no cabe recurso administrativo alguno.

Contra el acuerdo de adopción de medidas provisionales, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDPGDD, y de acuerdo con lo establecido en el artículo 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (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 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.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente el acuerdo de adopción de medidas provisionales firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formal-mente 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. Esta suspensión cautelar se daría por finalizada 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 del presente acuerdo de adopción de medidas provisionales, o si interpuesto dicho recurso no se solicitará en el mismo trámite su suspensión cautelar al órgano judicial.

1479-290125

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

>>

SEGUNDO**:** En fecha 20 de mayo de 2025, ***SIDECU*** ha procedido al pago de la sanción en la cuantía de **96.000,00 euros** haciendo uso de las dos reducciones previstas en el acuerdo de inicio transcrito anteriormente, por pronto pago y por reconocimiento de la responsabilidad en relación con los hechos a los que se refiere el acuerdo de inicio y su calificación jurídica.

TERCERO: En el acuerdo de inicio transcrito anteriormente se señalaba que, de confirmarse la infracción, podría acordarse imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá *"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…".*

Habiéndose reconocido la responsabilidad de la infracción, procede la imposición de las medidas incluidas en el acuerdo de inicio.

CUARTO: Asimismo, en el transcrito acuerdo de inicio, se ordenaba a ***SIDECU***, como medida provisional, la suspensión temporal de todo tratamiento de datos personales biométricos de categoría especial como método de control de acceso (entrada y salida) a sus centros deportivos, de acuerdo con lo dispuesto en el artículo 69 de la LOPDGDD.

QUINTO: En el escrito de 20 de mayo de 2025, ***SIDECU*** reconoce la responsabilidad, renuncia al ejercicio de acciones y solicita *"**un aplazamiento y ampliación de plazo para acreditar y justificar a esa Agencia el cese del uso del método de acceso que ha dado origen al presente expediente y su sustitución por el nuevo método de acceso, hasta el próximo 1 de julio de 2025**, con el fin de poder disponer de todos los medios oportunos para su uso".*

FUNDAMENTOS DE DERECHO

I
Competencia

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 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para

resolver este procedimiento 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
Terminación del procedimiento

El artículo 85 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo, LPACAP), bajo la rúbrica "*Terminación en los procedimientos sancionadores*" dispone lo siguiente:

"1. Iniciado un procedimiento sancionador, si el infractor reconoce su responsabilidad, se podrá resolver el procedimiento con la imposición de la sanción que proceda.

2. Cuando la sanción tenga únicamente carácter pecuniario o bien quepa imponer una sanción pecuniaria y otra de carácter no pecuniario pero se ha justificado la improcedencia de la segunda, el pago voluntario por el presunto responsable, en cualquier momento anterior a la resolución, implicará la terminación del procedimiento, salvo en lo relativo a la reposición de la situación alterada o a la determinación de la indemnización por los daños y perjuicios causados por la comisión de la infracción.

3. En ambos casos, cuando la sanción tenga únicamente carácter pecuniario, el órgano competente para resolver el procedimiento aplicará reducciones de, al menos, el 20 % sobre el importe de la sanción propuesta, siendo éstos acumulables entre sí. Las citadas reducciones, deberán estar determinadas en la notificación de iniciación del procedimiento y su efectividad estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

El porcentaje de reducción previsto en este apartado podrá ser incrementado reglamentariamente."

III
Pago voluntario y reconocimiento de responsabilidad

De conformidad con lo dispuesto en el citado artículo 85 de la LPACAP, en el acuerdo de inicio notificado se informaba sobre la posibilidad de reconocer la responsabilidad y de realizar el pago voluntario de la sanción propuesta, lo que supondría dos reducciones acumulables de un 20% cada una. Con la aplicación de estas dos reducciones, la sanción quedaría establecida en **96.000,00 euros** y su pago implicaría la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

Tras la notificación del citado acuerdo de inicio, ***SIDECU*** ha procedido al reconocimiento de la responsabilidad y al pago voluntario de la sanción, acogiéndose a las dos reducciones previstas. De conformidad con el apartado 3 del artículo 85

LPACAP, la efectividad de las citadas reducciones estará condicionada al desistimiento o renuncia de cualquier acción o recurso en vía administrativa contra la sanción.

Debe tenerse en cuenta que, de acuerdo con los preceptos de la LPACAP, así como de la jurisprudencia del Tribunal Supremo en esta materia, el ejercicio del pago voluntario por el presunto responsable no exime a la administración de la obligación de resolver y notificar todos los procedimientos, cualquiera que sea su forma de iniciación. De igual forma, el artículo 88 de la citada norma establece que la resolución que ponga fin al procedimiento decidirá todas las cuestiones planteadas por los interesados y aquellas otras derivadas del mismo.

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones, la Presidencia de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la comisión de las infracciones y CONFIRMAR las sanciones determinadas en la parte dispositiva del acuerdo de inicio transcrito en la presente resolución.

La suma de las citadas cuantías arroja una cantidad total **160.000,00 euros.**

Tras haber procedido ***SIDECU, S.A.*** al pronto pago y reconocimiento de responsabilidad, se procede, en virtud del artículo 85 de la LPACAP, a la reducción de un 40% del total mencionado, lo cual supone la cantidad definitiva de **96.000,00 euros**.

La efectividad de las citadas reducciones está condicionada, en todo caso, al desistimiento o renuncia de cualquier acción o recurso en vía administrativa.

SEGUNDO: DECLARAR la terminación del procedimiento **EXP202313347**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

TERCERO: ORDENAR a ***SIDECU, S.A.*** acredite ante esta Agencia que ha adoptado las medidas correctivas que se describen en los fundamentos de derecho del acuerdo de inicio transcrito en la presente resolución en los plazos fijados de 7 meses y 1 mes desde la notificación de la Resolución en el supuesto de que el nuevo método de acceso implementado implique el tratamiento de datos biométricos. En el caso de que se opte por implantar un nuevo método de acceso a los centros que no sea considerado de alto riesgo ni trate datos biométricos, debiendo en todo caso acreditar cual ha sido el nuevo método de acceso implantado y haber cumplido con los requisitos previstos en el RGPD en el caso de que este implique el tratamiento de datos personales.

CUARTO: CONFIRMAR, elevándola a definitiva, la medida provisional impuesta a ***SIDECU, S.A.*** cuyo cumplimiento deberá acreditarse a partir del día siguiente de la notificación de la presente resolución de procedimiento sancionador y hasta el 1 de julio de 2025 como plazo máximo:

- suspensión de todo tratamiento de datos personales biométricos de categoría especial como método de control de acceso (entrada y salida) a sus centros deportivos.

QUINTO: NOTIFICAR la presente resolución a ***SIDECU, S.A.***.

SEXTO: De acuerdo con lo previsto en el artículo 85 de la LPACAP que condiciona la reducción por pago voluntario y reconocimiento de la responsabilidad al desistimiento o renuncia de cualquier acción o recurso en vía administrativa, la presente resolución será firme en vía administrativa y plenamente ejecutiva a partir de su notificación.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, los interesados podrán interponer 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.

No obstante, conforme a lo previsto en el artículo 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://sedeaepd.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.

1259-260325

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