DECLARACIÓN RESPONSABLE DE CUMPLIMIENTO DEL RGPD Y LOPD-GDD EN CUANTO A LA REALIZACIÓN DE LA EIPD PARA EL TRATAMIENTO DE DATOS PARA EL ACCESO POR SISTEMAS DE RECONOCIMIENTO FACIAL

CONSULTING & STRATEGY GFM S.L. (GFM SERVICIOS) con CIF B71198543, en calidad de representante legal de **AGRUPACIÓN DEPORTIVA SAN JUAN – DONIBANE KIROL ELKARTEA**, con domicilio en Avenida Sancho el Fuerte S/N , 31011 de Pamplona (Navarra) y CIF G31063548.

DECLARA

Que dicha entidad ha implantado los requisitos y medidas que exige al REGLAMENTO (UE) 2016/679, de 27 de abril de 2016 del Parlamento Europeo y del Consejo relativo a la Protección de personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismo, en adelante (el RGPD) y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, en adelante (la LOPDPGDD), en relación con la obligación que establece el artículo 35, RGPD UE 2016/679, de realizar una Evaluación de Impacto en la Protección de Datos (EIPD) en cuanto al tratamiento de datos biométricos, en este caso, tratamientos de datos para acceso mediante reconocimiento facial.

Artículo 35. Evaluación de impacto relativa a la protección de datos

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

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

En concreto, en la elaboración de la EIPD se han desarrollado los siguientes apartados:

En PAMPLONA, a 6 de febrero de 2025

Consulting & Strategy GFM S.L.

Gonzalo Fdez.-Micheltorena

dpo@gfmservicios.com

29148475T GONZALO FERNANDEZ MICHELTORENA (R: B71198543)

Firmado digitalmente por 29148475T GONZALO FERNANDEZ MICHELTORENA (R: B71198543)
Nombre de reconocimiento (DN): 2.5.4.13=Reg:31015 /Hoja:NA-34347 / Tomo:1732 /Folio:35 / Fecha:27/08/2014 /Inscripción:1, serialNumber=IDCES-29148475T, givenName=GONZALO, sn=FERNANDEZ MICHELTORENA ARAMENDIA, cn=29148475T GONZALO FERNANDEZ MICHELTORENA (R: B71198543), 2.5.4.97=VATES-B71198543, o=CONSULTING & STRATEGY GFM SL, c=ES
Fecha: 2025.02.06 13:45:39 +01'00'

RESUMEN DEL INFORME DE EVALUACIÓN DE IMPACTO RELATIVA A LA PROTECCIÓN DE DATOS

CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL

AGRUPACIÓN DEPORTIVA SAN JUAN DONIBANE KIROL ELKARTEA

DATOS DEL RESPONSABLE

Datos de contacto del responsable

AGRUPACIÓN DEPORTIVA SAN JUAN – DONIBANE KIROL ELKARTEA

G31063548

AVDA. SANCHO EL FUERTE S/N. - 31011 - PAMPLONA - NAVARRA

948172255

gerencia@adsj-dke.com

Delegado de Protección de Datos

CONSULTING & STRATEGY GFM SERVICIOS

B71198543

Polígono Ind. Noáin-Esquíroz, Calle 0, Num. 2 (Edif. Portal de Navarra), Planta 2, Oficina 7 – 31110 Noáin (Navarra)

dpo@gfmservicios.com

1. DATOS DE LA EIPD

1.1. NOMBRE DE LA EIPD

CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL

1.2. NOMBRE DEL TRATAMIENTO SOBRE EL QUE SE HA REALIZADO

CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL

1.3. FECHA DE REALIZACIÓN Y VERSIÓN

Fecha de realización: 06/02/2025

Versión: v2

Estado: Finalizada

2. DESCRIPCIÓN DEL TRATAMIENTO

2.1. DATOS GENERALES

DATOS GENERALES DEL TRATAMIENTO

Nombre: CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL

Finalidad: CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL, TRATAMIENTO DE IMAGENES GENERANDO VECTOR PARA IDENTIFICAR AL USUARIO

Descripción detallada del tratamiento: La finalidad orientada a la verificación o autentificación de la identidad del usuario y no a su identificación. a traves de un sistema de reconocimiento facial en el cual se crea un algoritmo de la imagen , algoritmo que se almacena y que sirve como base para la posterior verificación o autentificación de la identidad del usuario al buscar dicho algoritmo sobre el generado por el usuario en el momento.

BASE JURÍDICA

- **Interés legítimo del Responsable**: Control de entradas y salidas a las instalaciones del responsble por motivos de seguridad y trazabilidad de visitas. (RGPD art. 6.1.f).
- **Consentimiento del interesado**: Art. 6.1.a) RGPD UE 2016/679, tratamiento de imágenes y generación de vector para la identificación del Usuario

CATEGORÍAS DE INTERESADOS

Personas que visitan las instalaciones.

Categorías: Empleados; Asociados y miembros.

Otras categorías de interesados: Socios/as; Monitores/as.

CATEGORÍAS DE DATOS PERSONALES

Identificación: Imagen.

Otros: ID y número de usuario/a, vector de la imagen del usuario/a.

CATEGORÍAS DE DESTINATARIOS

Organizaciones o personas relacionadas directamente con el Responsable del tratamiento.

Otros destinatarios: Das-Nano S.L, empresa proveedora servicios reconocimiento facial

TRANSFERENCIAS DE DATOS A TERCEROS PAÍSES U ORGANIZACIONES INTERNACIONALES

No existen transferencias de datos a terceros países.

PLAZOS PREVISTOS PARA LA SUPRESIÓN

Los datos se suprimirán siempre que lo solicite el interesado (vector irreversible) o, en su defecto, cuando la legislación específica así lo establezca. En cuanto a las imágenes de socios utilizadas en el tratamiento, se eliminarán en el momento en que se ha validado la misma y se genera el vector irreversible.

ENCARGADOS DEL TRATAMIENTO

A continuación, se indican los encargados del tratamiento que tienen, o pueden tener, acceso a los datos personales incluidos en este tratamiento:

- **DAS-NANO S.L. (B71092696).**

Los servicios que cada uno de estos encargados del tratamiento prestan al responsable, así como las condiciones que regulan la prestación de dichos servicios, las categorías de datos involucradas, las categorías de interesados, sus implicaciones y demás detalles de la prestación de dichos servicios se encuentran especificadas en el contrato de acceso a datos por cuenta de terceros que se ha suscrito con cada uno de los encargados del tratamiento correspondientes.

2.2. VOLUMEN Y EXTENSIÓN DEL TRATAMIENTO

El volumen de interesados objeto del tratamiento, así como la extensión del mismo, se indican en la siguiente tabla:

Interesados objeto del tratamiento	Usuarios/as de las instalaciones de la ADSJ- DKE
Duración del tratamiento	Años
Extensión geográfica del tratamiento	Regional

3. ANÁLISIS DE LA NECESIDAD DE REALIZAR UNA EIPD

A continuación, se muestra el análisis que se ha realizado sobre cada uno de los tratamientos para valorar si es necesario, o no, realizar una evaluación de impacto relativa a la protección de datos.

CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL
ANÁLISIS
• El tratamiento está incluido en la lista de actividades de tratamiento publicada por la AEPD que SÍ requieren de EIPD • Uso innovador o aplicación de nuevas soluciones tecnológicas u organizativas: como combinar el uso de huella dactilar y reconocimiento facial para mejorar el control físico de acceso, etc. Esto es debido a que el uso de dicha tecnología puede implicar nuevas formas de recogida y utilización de datos, posiblemente con un alto riesgo para los derechos y libertades de las personas. De hecho, las consecuencias personales y sociales del despliegue de una nueva tecnología pueden ser desconocidas. Por ejemplo, algunas aplicaciones del «Internet de las cosas» podrían tener un impacto significativo sobre la vida diaria y la privacidad de las personas y, por tanto, requieren una EIPD • La finalidad orientada a la verificación o autentificación de la identidad del usuario y no a su identificación. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física a través de sistema de reconocimiento facial, utilizado el mismo como un sistema alternativo de control de accesos a las instalaciones, mejorando siempre los servicios al socio y siempre con la legitimación del consentimiento expreso, libre, informado y demostrable del interesado.
CONCLUSIÓN
Se requiere EIPD, pues es un tratamiento que se va a llevar a cabo y se considera que es probable que exista un alto riesgo para los derechos y las libertades de los interesados

4. METODOLOGÍA DE LA EIPD

4.1. DOCUMENTACIÓN DE REFERENCIA

Para llevar a cabo esta Evaluación de Impacto relativa a la Protección de Datos (EIPD) se ha utilizado la siguiente documentación de referencia:

- Guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD de la Agencia Española de Protección de Datos.
- Norma ISO/IEC 29134:2017. *Guidelines for privacy impact assessment*.
- Norma ISO/IEC 27005:2018. *Information security risk management*.
- Norma UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información.
- Norma UNE-EN ISO/IEC 27002:2017. Código de prácticas para los controles de seguridad de la información.
- Norma ISO/IEC 27701:2019. *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -Requirements and guidelines-.*
- Norma ISO/IEC 29151:2017. *Code of practice for personally identifiable information protection.*

4.2. METODOLOGÍA EMPLEADA

La presente EIPD se ha realizado siguiendo esta metodología:

1. **Determinar si es necesario realizar una EIPD:** en esta fase previa, se realiza un análisis preliminar de la necesidad de realizar una EIPD. Si no se necesita, se justifica y documenta por qué no es necesario realizar una EIPD y el proceso finaliza en este punto; en cambio, si el análisis revela que hay que realizar una EIPD, se justifica y documenta la necesidad de realizarla y se continua en el siguiente punto.
2. **Preparación de la EIPD:** se establece un equipo de trabajo y se le facilitan los recursos necesarios para su desempeño.

3. **Participación de los interesados:** si es necesaria la participación de los interesados en la EIPD, se identifican los interesados a los que se va a consultar y se establece un plan de consulta y comunicación, registrándose las respuestas y comentarios de los mismos.

4. **Análisis detallado del tratamiento:** en esta fase se describe todo el ciclo de vida de los datos personales (captura de datos, clasificación/almacenamiento, uso/tratamiento, cesión/transferencia de datos a un tercero y destrucción), incluyendo los siguientes aspectos:

    a. Datos tratados: se detallan las categorías de datos involucradas en cada fase del ciclo de vida de los datos.

    b. Actividades u operaciones: se detallan las distintas actividades u operaciones que se llevan a cabo sobre los datos personales, con el objetivo de comprender los posibles riesgos a los que se pueden ver expuestos los datos.

    c. Intervinientes: se detallan las personas físicas o jurídicas que, de manera individual o colectiva, están implicadas en el desarrollo de las actividades de tratamiento (responsables, áreas o empleados, encargados del tratamiento, etc.)

    d. Tecnología: se detallan, a un alto nivel, aquellos elementos tecnológicos que intervienen en las actividades de tratamiento de los datos. Se identifica la tecnología (Cloud, BBDD, servidores), aplicaciones, dispositivos y técnicas empleadas en el procesamiento de los datos.

5. **Análisis de la necesidad y proporcionalidad del tratamiento:** se realiza un análisis para justificar, adecuadamente, la necesidad y proporcionalidad de las actividades de tratamiento en relación a las finalidades del mismo.

6. **Análisis y gestión de riesgos:** se realiza un análisis de los riesgos de privacidad y cómo se van a tratar dichos riesgos para reducirlos hasta un umbral aceptable. Esto comprende las siguientes actividades:

    - Identificar amenazas, vulnerabilidades y riesgos.

    - Evaluar los riesgos identificados.

- Tratar los riesgos.

7. **Medidas de seguridad:** se documentan detalladamente las medidas de seguridad que se aplicarán al tratamiento para reducir el riesgo hasta un umbral aceptable.

8. **Conclusión:** basándose en el riesgo residual obtenido durante la fase de análisis y gestión de riesgos, debe valorarse si éste es elevado o se considera aceptable y dentro de unos límites razonables.

9. **Comunicación y consulta a la autoridad de control:** en caso de que el riesgo residual del tratamiento sea alto o muy alto, debe realizarse una consulta a la Autoridad de Control mediante los canales de comunicación establecidos.

10. **Supervisión y revisión de la implantación:** como último paso de la EIPD, debe realizarse una adecuada supervisión y una posterior revisión de la implantación de las medidas de seguridad y control definidas en el punto 7 para reducir el riesgo inherente hasta un riesgo residual que permite llevar a cabo el tratamiento garantizando los derechos y libertades de las personas físicas.

5. ANÁLISIS DETALLADO DEL TRATAMIENTO

A continuación, se detalla todo el ciclo de vida de los datos, así como los elementos involucrados en cada una de esas etapas.

6.1. CAPTURA DE DATOS

En esta etapa se han tenido en cuentas las actividades que se van a llevar a cabo para la recogida de imágenes de socios/as, trabajadores/as y monitores/as del Agrupación Deportiva San Juan – Donibane Kirol Elkartea, para su posterior validación y vectorización. Haciendo especial hincapié en las imágenes de los/as menores de edad, por su especial sensibilidad, así como en las imágenes de nuevos/as socios/as.

Para la activación de los lectores faciales utilizados en la captura de datos se han instalado sensores de proximidad con el objetivo de activar los lectores faciales; de esta forma se consigue cumplir con los requisitos establecidos en el Reglamento de Inteligencia Artificial que estable que los sistemas de datos biométricos y control de acceso no deben permitir la identificación remota y deben contar con una acción proactiva del interesado.

DATOS TRATADOS

Datos de identificación: Imagen.

Otros: ID y número de socio/a, trabajador/a, monitor/a.

Categorías especiales de datos: Datos biométricos.

6.2. CLASIFICACIÓN / ALMACENAMIENTO

En esta etapa del proceso se ha procedido a describir y analizar la actividad de la validación de las imágenes de los usuarios/as de las instalaciones de la ADSJ-DKE, así como a la de vectorización posterior de las mismas (generación de un vector irreversible). También se ha procedido a describir la actividad de almacenamiento de dichos vectores irreversibles generados para cada socio/a en las bases de datos oportunas para permitir el acceso mediante reconocimiento facial.

DATOS TRATADOS

Datos de identificación: Imagen.

Categorías especiales de datos: Datos biométricos.

6.3. USO / TRATAMIENTO

En esta etapa del proceso de tratamiento de datos personales, se han descrito y analizado dos actividades distintas. En primer lugar, el envío de la base de datos que almacena los vectores irreversibles al motor facial correspondiente (lector facial). En segundo lugar, el tratamiento relativo a la imagen tomada por los lectores faciales en el momento en que el usuario/a pretende acceder a las instalaciones de la ADSJ-DKE.

DATOS TRATADOS

Datos de identificación: Imagen.

Categorías especiales de datos: Datos biométricos.

6.4. CESIÓN O TRANSFERENCIA DE DATOS A UN TERCERO

En esta etapa del tratamiento de datos personales se hace referencia a aquellas cesiones de datos que se puedan dar a lo largo del mismo. En concreto se producen dos cesiones, en las que se han analizado los riesgos inherentes a las mismas: en primer lugar, cesión de imágenes y número de socio/a para validación y generación de los vectores irreversibles; en segundo lugar, cesión de vectores irreversibles a base de datos de almacenamiento.

DATOS TRATADOS

Datos de identificación: Imagen.

Otros: Vectores irreversibles.

Categorías especiales de datos: Datos biométricos.

6.5. DESTRUCCIÓN

Última etapa del tratamiento de datos personales, en la cual se procede a la destrucción de la imagen y número de usuario/a, una vez generados los vectores correspondientes que permiten el acceso a las instalaciones.

DATOS TRATADOS

Datos de identificación: Imagen.

Otros: ID Socios/as, trabajadores/as y monitores/as

Categorías especiales de datos: Datos biométricos.

6. NECESIDAD Y PROPORCIONALIDAD DEL TRATAMIENTO

El tratamiento que aquí se analiza no es de los calificados como exentos.

Análisis de la inclusión del tratamiento en los casos de tratamientos obligados

De acuerdo con la lista aprobada por el Comité Europeo de Protección de Datos, son tratamientos que precisan EIPD, los tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos. Por otro lado, la AEPD señala en el documento “Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos (art 35.4)”, el tratamiento de datos biométricos como un tratamiento que precisa EIPD.

Además, es decisión del responsable, en línea con su política de respeto y tutela de los derechos de sus empleados y, más específicamente del derecho a la protección de datos, el adoptar las mayores garantías para la protección de tal derecho y, por ello, se decide realizar la EIPD, para asegurar la licitud del tratamiento que se pretende adoptar.

8. ANÁLISIS Y GESTIÓN DE RIESGOS

8.1. OBJETO DEL ANÁLISIS DE RIESGOS

La gestión de riesgos, es el proceso de identificar, analizar y valorar la probabilidad e impacto derivados de la posibilidad de que se materialicen las distintas amenazas que acechan a la seguridad de los datos personales, para establecer las acciones correctivas que permitan minimizar la exposición al riesgo.

Para ello, se ha realizado un análisis de riesgos en el que se han identificado, de forma metódica, las amenazas a las que los datos personales están expuestos, así como las vulnerabilidades que pueden aprovechar dichas amenazas para tener éxito.

Se ha estimado también el daño que podrían producir las distintas amenazas en caso de que se materializasen, así como la probabilidad de su ocurrencia.

Con estos datos, se ha realizado una estimación del nivel de riesgo y se han tomado las decisiones pertinentes para gestionar estos riesgos, identificando las medidas de seguridad necesarias para eliminar o reducir aquellos riesgos que se ha decidido gestionar.

8.2. METODOLOGÍA DEL ANÁLISIS Y GESTIÓN DE RIESGOS

Para realizar un análisis de riesgos, es preciso, en primer lugar, definir la metodología para evaluar y gestionar los riesgos a que están expuestos los tratamientos de datos personales.

La evaluación y gestión de los riesgos se aplica a todos los tratamientos de datos personales que la entidad realice y sobre todos los activos que están involucrados en los mencionados tratamientos de datos personales.

A continuación, se detalla la metodología utilizada para el análisis y gestión de los riesgos.

Para la elaboración de la metodología se han tenido en cuenta los siguientes documentos:

- Norma UNE 71504:2008. Metodología de análisis y gestión de riesgos para los sistemas de información.
- Norma ISO/IEC 27005:2018. *Information security risk management*.
- Guía práctica de análisis de riesgos en los tratamientos de datos personales sujetos al RGPD de la AEPD.
- Norma UNE-EN ISO/IEC 27002:2017. Código de prácticas para los controles de seguridad de la información.
- Norma ISO/IEC 27701:2019. *Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management -Requirements and guidelines-.*
- Norma ISO/IEC 29151:2017. *Code of practice for personally identifiable information protection.*

8.2.1. PROCESO

El análisis de riesgos se ha realizado a través de un proceso metódico que sigue los siguientes pasos:

1. Se identifican todos los activos primarios de información involucrados en el tratamiento de los datos personales.
2. Se identifica y valora el impacto que podría suponer para los interesados, en las distintas dimensiones de la seguridad de la información (confidencialidad, integridad y disponibilidad) si a consecuencia de la materialización de alguna amenaza, resultasen dañadas.
3. Se identifican los distintos activos que dan soporte a los activos primarios de información (hardware, software, soportes, etc.) y se vinculan a los activos primarios de información concretos a los que prestan soporte.
4. Se identifican las distintas amenazas a que están expuestos esos activos que podrían comprometer la confidencialidad, integridad o disponibilidad de la información.

5. Se identifican las distintas vulnerabilidades de los activos que pueden aprovechar las mencionadas amenazas para causar su daño.
6. Se estima la frecuencia con que se presenta cada una de las amenazas, así como el grado de vulnerabilidad de los distintos activos para calcular la probabilidad de que las distintas amenazas se materialicen aprovechando las vulnerabilidades identificadas.
7. Se calcula el nivel de riesgo para cada par de amenaza-vulnerabilidad. Este nivel de riesgo se calcula en base al impacto y la probabilidad que se ha analizado en los pasos previos.
8. Se evalúa y decide cuáles son los riesgos que se van a gestionar en base a los criterios establecidos en la metodología.
9. Se identifican los controles necesarios para gestionar los riesgos.
10. Se vuelve a calcular el nivel de riesgo considerando los controles seleccionados para calcular el nivel de riesgo residual.
11. Si el nivel de riesgo residual no es aceptable, se repite de nuevo el proceso desde el punto 8.
12. Si no es posible bajar más el riesgo a un umbral aceptable, no se podría llevar a cabo el tratamiento y sería necesario activar el procedimiento de consulta previa a la Autoridad de Control.
13. Se deben describir en detalle las medidas de seguridad que se van a aplicar para una implantación efectiva de las mismas en la organización.
14. Se debe documentar todo el proceso, así como la conclusión del mismo.

A continuación, veremos detalladamente cómo se recopila la información necesaria en cada uno de estos ámbitos y cómo se realizan los cálculos indicados anteriormente.

8.2.2. IDENTIFICACIÓN DE LOS ACTIVOS PRIMARIOS DE INFORMACIÓN

El primer paso que se debe dar en el análisis de riesgos es identificar todos los activos que están involucrados en el tratamiento de los datos personales.

Los activos pueden distinguirse en:

- Activos primarios:
  - Procesos de negocio y actividades.
  - Información.
- Activos de soporte (en los que se apoyan los activos primarios):
  - Hardware.
  - Software.
  - Comunicaciones.
  - Personal.
  - Instalaciones.

9. MEDIDAS DE SEGURIDAD Y CONTROL

Como resultado del Análisis de Riesgos realizado, las medidas de seguridad y control que deben implantarse en la organización para mantener los riesgos en un umbral aceptable, son las que a continuación se enumeran.

10. CONCLUSIÓN

La realización de una Evaluación de Impacto para la Protección de Datos Personales (EIPD) supone la determinación previa de las amenazas y vulnerabilidades, a través de un análisis de riesgos, con el objetivo de implantar una serie de medidas de seguridad que garanticen un riesgo residual aceptable para el tratamiento, de acuerdo con lo previsto en el Reglamento UE 2016/679 y la Ley Orgánica 3/2018, de Protección de Datos Personales y Garantía de los Derechos Digitales.

En el caso de la EIPD relativa al tratamiento de datos para el acceso mediante reconocimiento facial a las instalaciones de la Agrupación Deportiva San Juan - Donibane Kirol Elkartea, se ha realizado un análisis de riesgo de todas las etapas del proceso; desde la utilización de la imagen de los/as socios/as, trabajadores/as y monitores/as, para la generación de un vector irreversible único que se almacenará en la base de datos de AWS y que estará conectada a los motores faciales del club, hasta la obtención de la imagen de la persona que quiera acceder a la Agrupación mediante lectores faciales que, a través del motor facial, asociarán ese nuevo vector creado al correspondiente vector irreversible.

Analizados los riesgos, tanto para la confidencialidad como para la integridad y la disponibilidad de los datos personales de los socios/as, se han implantado una serie de medidas de seguridad, tanto técnicas como organizativas, que permiten garantizar el respeto a los derechos de las personas y que, a su vez, reducen los riesgos inherentes al tratamiento.

Por todo ello, en cumplimiento del artículo 35 del Reglamento UE 2016/679, se establece que la Evaluación de Impacto en materia de Protección de Datos (EIPD) es favorable en relación con el tratamiento de los datos personales necesarios para el acceso mediante reconocimiento facial a las instalaciones del Club, determinando que el riesgo residual existente en este tratamiento es bajo o muy bajo para los derechos de las personas.