INFORME DE EVALUACIÓN DE IMPACTO EN LA PROTECCION DE DATOS (CONTROL DE ACCESO POR RECONOCIMIENTO FACIAL)

(Cumplimiento con los establecido en el art. 35.1 del Reglamento (UE) 2016/679 (RGPD)

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 sistema de reconocimiento facial.

El Club Natación Almería con CIF G04050985, con domicilio en Camino Jaul Bajo Finca 3, 04007 Almería.

DECLARA:

Que dicha entidad ha implantado los requisitos y medidas que exige el REGLAMENTO (UE) 2016/679, de 27 de abril de 2016 del Parlamento Europeo y del Consejo relative a la Protección de personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de los mismos, en adelante "el RGPD" y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos, en adelante "la LOPDPGDD, en relación con la obligación que establece el artícular 35, RGPD UE 2016/679m 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 relative a la protección de datos:

1.- Cuando sea probable que un tipo de tratamiento, en particular si utilize nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsible 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 similiares 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 relative a la protección de datos.

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

I N D I C E

1.- INTRODUCCION:

De conformidad con lo señalado en el considerado 84 del Reglamento General de Protección de Datos, en aquellos casos en los sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, debe incumbir al responsible del tratamento la realización de una evaluación de impacto relative a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostar que el tratamiento de los datos personales es conforme con el citado Reglamento.

En su consecuencia, la entidad CLUB NATACIÓN ALMERIA, ha realizado con fecha 01/02/2022, una evaluación de impacto relative a la protección de datos, con la finalidad de dar cumplimiento con lo establecido en el artículo 35, apartado 1, del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relative a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos) (DOUE L 119/1, 04/05/2016) (RGPD):

Cuando sea probable que un tipo de tratamento, en particular si utilize nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsible del tratamiento realizará antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales.

De acuerdo a lo señalado en las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sob re la evaluación de impacto relative a la protección de datos (EIPD), la EIPD es un proceso continuo, especialmente cuando una operación de tratamiento es dinámica y está sujeta a cambios permanents.

En tal sentido, la actualización de la EIPD a lo largo del ciclo de vida del proyecto o de las operaciones de tratamiento garantizará que se tenga en cuenta la protección de datos y la intimidad y propiciará la creación de soluciones que fomenten el cumplimiento.

También puede resultar necesario repertir pasos concretos de la evaluación a medida que avance el proceso de desarrollo del proyecto o de las operaciones de tratamiento debido a que la selección de determinadas medidas técnicas u organizativas puede afectar a la gravedad o probabilidad de los riesgos que suponga el tratamento.

La gestión de riesgos en el ámbito de protección de datos está regulada en el artículo 35 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016, relative a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a

la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamenteo general de protección de datos), en adelante RGPD.

La Evaluación de Impacto sobre Protección de Datos (EIPD) permite identificar riesgos y establecer una respuesta a éstos, adoptando las salvaguardas necesarias para reducer dichos riesgos hasta un nivel considerado acceptable. La EIPD pretende también dar respuesta al principio de responsabilidad proactive (accountability) de quienes tartan datos personales para determiner qué medidas son adecuadas para cumplir con el RGPD.

La EIPD es necesaria cuando exista una probalidad de que un tipo de tratamiento, y de manera particular si se utilizan nuevas tecnologías, entrañe un alto riesgo para los derechos y libertades de las personas físicas teniendo en cuenta la naturaleza, alcance, context y fines de dicho tratamiento de datos.

La presente EIPD realizada sobre el nuevo sistema de control (con tecnología biométrica facial) de acceso implantado en el Club Natación Almeria, con el fin de proporcionar a sus socios/a información sobre la adecuación del Nuevo sistema a la normative vigente en el ámbito de protección de datos personales.

Esta evaluación de impacto está orientada a cumplir con las previsiones del Reglamento General de Protección de datos que incluye, entre las obligaciones del responsable del tratamiento, la necesidad de evaluar el impacto de las actividades de tratamiento en la protección de datos personales cuando resulte probable que el tratamiento suponga un riesgo significativo para los derechos y libertades de las personas.

Aunque no está orientado a los tratamientos de bajo riesgo, en aquellos en los que no es obligatoria la realización de una EIPD puede tenerse en cuenta la posibilidad de llevar a cabo este análisis con el objeto de estudiar en profundidad un tratamiento y sus procesos asociados necesarios para la consecución de los objetivos de una organización.

Este modelo está basado en las siguientes guías y normas:

- La guía práctica para las evaluaciones de impacto en la protección de datos sujetas al RGPD de la AEPD.
- Nomas ISO-29134 “Directrices para la evaluación de impacto sobre la privacidad”.
- Normas ISO 31000 “Gestión del riesgo. Principios y directrices”
- Normas ISO 31010 “Gestión del riesgo. Técnicas de evaluación de riesgos”.

¿Que es una evaluación de impacto relativo a la protección de datos (EIAP)?

El Reglamento (UE) 2016/679 establece la obligación para el responsible del tratamiento de datos de aplicar ***“medidas técnicas y organizativas apropiadas”,*** a fin de garantizar y poder demostrar que el tratamiento es conforme con el citado Reglamento, teniendo en cuenta ***“la naturaleza, el ámbito, el context y los fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas”*** (art. 24.1 RGPD).

En su consecuencia, y atendiendo al principio de la "protección de datos desde el diseño", el responsible del tratamiento debe aplicar, tanto en el momento de determiner los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisites del Reglamento (UE) 2016/679 y proteger los derechos de los interesados. Por ello, deberá tener en cuenta ***"el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, context y fines del tratamiento, así como los riesgos de diversas probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas"***

Así mismo, dichas medidas deberán ser revisadas y actualizadas cuando sean necesarias (art. 24.1 RGPD in fine)

En una misma línea, el artículo 35 del Reglamento (UE) 2016/679 establece, en su apartado primero, que cuando sea probable que un tipo de tratamiento, en particular si utilize nuevas tecnologías, por su naturaleza, alcance, context o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsible del tratamiento deberá realizar, antes del tratamiento, una evaluacíón de impacto de las operaciones de tratamiento en la protección de datos personales.

En tal sentido, una EIPD o evaluación de impacto relative a la protección de datos es, en esencia, un ejercicio de análisis de los riesgos que un determinado sistema de información, product o servicio puede entrañar para el derecho fundamental a la protección de datos de los interesados y, tras ese análisis, afrontar la gestión eficaz de los riesgos identificados mediante la adopción de las medidas necesarias para eliminarlos o mitigarlos.

No en vano, las propias Directrices sobre la evaluación de impacto relative a la protección de datos, del Grupo de Trabajo sobre protección de datos del artículo 29, señalan que una EIPD es ***"un proceso concebido para describer el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivadas del tratamiento de datos personales, evaluándolos y determinando las medidas para abordarlos."***

De conformidad con lo establecido en el artículo, apartado 7, del RGPD, 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 responsible del tratamiento.

b) Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respect a su finalidad.

c) Una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1.

d) Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismo 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.

Siguiendo el esquema publicado por la Agencia Española de Protección de Datos en su "Guía práctica par alas evaluaciones de impacto en la protección de los datos sujetas al RGPD", las

diferentes fases de una evaluacón de impacto relative a la protección de datos y el flujo a seguir en la ejecución de la misma sería el siguiente:

2.- NORMATIVA APLICABLE:

- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relative a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) (DOUE L 119/1 de 04-05-20146 (RGPD).

- Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relative a la protección de datos (EIPD) y para determiner si el tratamiento "entraña probablemente un alto riesgo" a efectos del Reglamento (UE) 2016/679. Adoptadas el 4 de abril de 2017. Revisada por última vez y adoptadas el 4 de octubre de 2017.

- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (BOE núm. 294, de 06-12-2018) (LOPDGDD).

3.- RESUMEN EJECUTIVO.-

El responsable RGPD del tratamiento será en todo momento CLUB DE NATACIÓN DE ALMERIA (G04050895) sito en CAMINO JAUL BAJO, FINCA 003 04007 ALMERIA, Teléfono 950222579, Correo electrónico info@cnalmeria.com y pagina web (URL) www.cnalmeria.com, así como se incluirá a aquellas entidades gestores de los datos que intervienen en alguna de las fases del tratamiento, encargados y subencargados del tratamiento y cesiones de datos previstas.

4.- DATOS DE LA EIPD.-

4.1 Nombre de la EIPD:

Control de accesos a las instalaciones deportivas en el CLUB NATACION ALMERIA, por reconocimiento facial.

4.2- Fecha de realización de la EIPD:

Concluida el 3 de febrero de 2021. Elaborada por Luis Carretero Torres y asesorada por Alicia Pastor. (protección de datos)

4.3 Nombre y descripción del Tratamiento:

Evaluación de impacto por la instalación de un sistema biométrico de reconocimiento facial para el acceso a las instalaciones deportivas del Club Natación Almería.

El Registro de Datos de tratamiento puede encontrarse en https://cnalmeria.com/aviso-legal-reconocimiento-facial/.

Los datos personales tratados (previo consentimiento en la hoja de solicitud) tienen las finalidades que se detallan a continuación:

a) La recopilación de datos de los socios/as y su posterior tramitación para dar de alta en el sistema informático, con el fin de poder accede a las instalaciones.
b) Gestión de cobro y remesa de los asistentes a las instalaciones y cursos que realicen.
c) Envío de datos personales necesarios a los bancos de cada cliente para el cobro de los recibos o servicios correspondientes.
d) Utilización de datos para informar a los socios/as de las actividades que se realicen en el Club Natación Almeria, solicitando su participación en los mismo, exclusivamente en caso de haber consentido.

5.- OBJETO DEL INFORME:

La protección de las personas físicas en relación con el tratamiento de datos personales es un derecho fundamental. El artículo 8, apartado 1, de la Carta de los Derechos Fundamentales de la Unión Europe y el artículo 16, apartado 1, del Tratado de Funcionamiento de la Unión Europea (TFUE) establecen que toda persona tiene derecho a la protección de los datos de character personal que le conciernan.

En este sentido, el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relative a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46 CE, establece un marco sólido y coherente para la protección de datos en la Unión Europea, reforzando la seguridad juridical y práctica par alas personas físicas, los operadores económicos y las Autoridad Pública.

Como consecuencia de lo anterior, la Junta Directiva del Club Natación America (el responsabel del tratamiento) ha asumido la maxima responsabilidad y compromise con el establecimiento, implementación y mantenimiento de una Política de Protección de Datos en dicha entidad, garantizando la mejora continua con el objetivo de alcanzar la excelencia en relación con el cumplimiento del Reglamento (UE) 2016/679 y de la normative española de protección de datos de carácter personal (Ley Orgánica, legislación sectorial especifica y sus normas de desarrollo)

La Política de Protección de Datos del CLUB NATACION ALMERIA, descansa en el principio de responsabilidad proactive, según el cual el responsale del tratamiento es responsible del cumplimiento del marco normative y jurisprudencial que gobierna dicha política, y es capaz de demostrarlo ante las autoridades de control competente.

No en vano, tal y como señala el considerado 74 del propio Reglamento (UE) 2016/679, los responsables del tratamiento están obligados a aplicar medidas oportunas y eficaces y han de poder demostar la conformidad de las actividades de tratamiento con el referido Reglamento, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito, el context y los fines del tratamiento, así como el riesgo para los derechos y libertades de las personas físicas.

Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materials o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdida financieras, reversion no autorizada de la seudonimización o cualquier otro perjuicio economic o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opinions políticas, la religion o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos datos relatives a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales, en los casos en los que se traten datos personales de personas vulnerable, en particular niños, o en los caso en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de socios/as.

De tal modo, la probabilidad y la gravedad del riesgo para los derechos y libertades de lo socios/as debe determinarse con referencia a la naturaleza, el alcance, el context y los fines del tratamiento de datos. El riesgo debe ponderarse sobre la base de una evaluación objetiva mediante la cual se determine si las operaciones de tratamiento de datos suponen un riesgo o si el riesgo es alto.

A fin de mejorar el cumplimiento del Reglamento (UE) 2016/679, en aquellos casos en los que sea probable que las operaciones de tratamiento entrañen un alto riesgo para los derechos y libertades de las personas físicas, deben incumbir al responsible del tratamiento la realización de una evaluación de impacto relative a la protección de datos, que evalúe, en particular, el origen, la naturaleza, la particularidad y la gravedad de dicho riesgo. El resultado de la evaluación debe tenerse en cuenta cuando se decidan las medidas adecuadas que deban tomarse con el fin de demostrar que el tratamiento de los datos personales es conforme con el presente Reglamento. Si una evaluación de impacto relative a la protección de datos muestra que las operaciones de tratamiento entrañan un alto riesgo que el responsible no puede mitigar con medidas adecuadas en terminus de tecnología disponible y costes de aplicación, deben consultarse a la autoridad de control antes del tratamiento.

Como corolario de lo hasta aquí expuesto, el presente informe tiene como objeto dar cumplimiento a lo establecido en el artículo 35, apartado 1, del Reglamento (UE) 2016/679, según el cual ***"cuando sea probable que un tipo de tratamient, en particular si utilize nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsible del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales."***

En el tocante a este particular, la publicación de la evaluación de impacto relativa a la protección de datos no representa un requisito jurídico del RGPD, ya que es una decision que corresponde al responsable del tratamiento.

No obstante lo anterior, las Directrices del Grupo de Trabajo sobre protección de datos del artículo 29 (GT29) sobre la evaluación de impacto relative a la protección de datos (EIAP), subrayan expresamente que ***los responsables del tratamiento deben considerer al menos la publicación de alguna parte de su EIPD, como un resumen o una conclusion de la misma.***

El fin de dicho proceso es ayudar a fomenter la confianza en las operaciones de tratamiento del responsable, y demostrar responsabilidad proactive y transparencia. Cuando las personas se ven afectadas por las operaciones de tratamiento, la publicación de una EIPD supone una práctica particularmente positiva.

6.- DESCRIPCION DEL TRATAMIENTO:

La evaluación de impacto se elabora en el mes de enero de 2022, siendo su responsable la dirección del Club Natación de Almería, Es la primera version, y aún no se han dado por tanto ningún tipo de cambios ni modificaciones alguna.

6.1 REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE USUARIOS:

-- **Tratamiento:**
***** Los usuario.

-- **Finalidad del tratamiento**:
* Gestión de la relación con los usuarios

-- **Descripción de las categorias de usuarios:**
*****Personas que hacen uso del centro del responsable del tratamiento.

--Descripción de las categorias de datos personales:
* Los necesarios para gestionar la identificación tales como nombre, apellidos, dirección postal, telefonos, e-mail, dni, y las características personales de tales como fecha de nacimiento, sexo y datos financieros para remesar las cuotas. **Se excluyen datos de raza, salud o afiliación política o sindical.**

--**Las categorias de destinatarios a quienes se comunicaron o comunicaran los datos personales:**
*****No se han previsto.

--Plazos previstos para la supresion de las diferentes categorías de datos:
***** Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades y atendiendo al principio limitación del plazo de conservación y según establece ell RGPD, en su artículo 5.1 e), recoge el **principio** de "**Limitación del Plazo de Conservación**". Podríamos resumirlo con que –salvo si concurren ciertas excepciones- el tratamiento de datos personales no debe durar más tiempo del necesario para el cumplimiento de las finalidades pertinentescuando sea posible estando en nuestro poder el minimo de tiempo imprescindible.

Cuando se posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.1 del RGPD.

6.2 REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE CORREO ELECTRONICO:

-- **Tratamiento:**
***** Correo electrónico.

-- **Finalidad del tratamiento**:
* Gestión de clientes contrable, fiscal y administrativa.
* Guías-repertorios de servicios de comunicaciones electrónicas.

-- **Descripción de las categorias de correo electronico y de las categorías de datos personales:**
*****Correo electronic, aplicación paa la gestión del correo electronic, así como la agenda de contactos.

--Descripción de las categorias de datos personales:
* Nif, nombre y apellidos, dirección, teléfono, firma/huella, económicos, financieros y de seguros, transacciones de bienes y servicios, dirección electronic.

--**Las categorias de destinatarios a quienes se comunicaron o comunicaran los datos personales:**
*****No se han previsto.

--Plazos previstos para la supresion de las diferentes categorías de datos:
***** Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades y atendiendo al principio limitación del plazo de conservación y según establece ell RGPD, en su artículo 5.1 e), recoge el **principio** de "**Limitación del Plazo de Conservación**". Podríamos resumirlo con que –salvo si concurren ciertas excepciones- el tratamiento de datos personales no debe durar más tiempo del necesario para el cumplimiento de las finalidades pertinentescuando sea posible estando en nuestro poder el minimo de tiempo imprescindible.

Cuando se posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.1 del RGPD.

6.3 REGISTRO DE ACTIVIDADES DE EMPLEADOS:

-- Tratamiento:
***** Empleados.

-- **Finalidad del tratamiento**:
* Gestión de la relación laboral con los empleados.

-- **Descripción de las categorias de empleados y de las categorías de datos:**
***** Empleados, personas que trabajan para el responsible del tratamiento

--Descripción de las categorias de datos personales:
* Los necesarios para el mantenimiento de la relación comercial, gestionar la nomina, formación y identificación: Nif, nombre y apellidos, número de la seguridad social, dirección, teléfono, e-mail, además de los datos personales tales como estado civil, fecha y lugar de nacimiento, edad, sexo, nacionaldad, porcentaje de minusvalia, datos académicos y datos bancarios para la domiciliación del pago de las nominas.

--**Las categorias de destinatarios a quienes se comunicaron o comunicaran los datos personales:**
*****Organismos de la seguridad social, de la administración pública con competencia en la material, cualquier organism relacionado con el responsible de los ficheros, la gestión laboral.

--Plazos previstos para la supresion de las diferentes categorías de datos:
***** Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades y atendiendo al principio limitación del plazo de conservación y según establece ell RGPD, en su artículo 5.1 e), recoge el **principio** de "**Limitación del Plazo de Conservación**". Podríamos resumirlo con que –

salvo si concurren ciertas excepciones- el tratamiento de datos personales no debe durar más tiempo del necesario para el cumplimiento de las finalidades pertinentescuando sea posible estando en nuestro poder el minimo de tiempo imprescindible.

Cuando se posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.1 del RGPD.

6.4 CONTROL DE ACCESOS POR RECONOCIMIENTO FACIAL:

-- Tratamiento:
***** Usuarios.

-- **Finalidad del tratamiento**:
* Registro y gestión de los accesos a las instalaciones del Club Natación Almería, mediante sistema de reconocimiento facial.

-- **Descripción de las categorias de de acceso por reconocimiento facil y de las categorías de datos:**
***** Registro y gestión de los accesos a las instalaciones mediante sistema de reconocimiento facial.

- En la fase de registro:
  -Captura de una o varias imágenes faciales.
  -Comparación de imágenes faciales capturadas en el proceso mediante técnicas de biometría facial para realizar mediciones de la coincidencia de identidad.
  -Cotejo de los gestos del usuario (sin grabación de video) para la prueba de vida.

- En la fase de verificación:
  -Comparación de las imágenes faciales capturadas por la cámara de la puerta de acceso y los vectores biométricos encriptados obtenidos en el registro almacenados en la base de datos del sistema, mediante técnicas de biometría facial para realizar mediciones de la coincidencia de identidad. En el caso de que no facilite sus datos personales, no podremos cumplir con las funcionalidades descritas anteriormente.

--Descripción de las categorias de datos personales:
* Los necesarios para el acceso a las instalaciones del club, se require una fotografía actualizada.

--**Las categorias de destinatarios a quienes se comunicaron o comunicaran los datos personales:**
*****Das-Gate.

--Plazos previstos para la supresion de las diferentes categorías de datos:
***** Los previstos por la legislación fiscal respecto a la prescripción de responsabilidades y atendiendo al principio limitación del plazo de conservación y según establece ell RGPD, en su artículo 5.1 e), recoge el **principio** de "**Limitación del Plazo de Conservación**". Podríamos resumirlo con que –salvo si concurren ciertas excepciones- el tratamiento de datos personales no debe durar más tiempo del necesario para el cumplimiento de las finalidades pertinentescuando sea posible estando en nuestro poder el minimo de tiempo imprescindible.

Cuando se posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32.1 del RGPD.

7.- CATEGORIA DE DATOS (concepto y definiciones):

7.1.- A efectos del presente informe se entenderán por:

7.1.1 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.

7.1.2 Tratamiento: 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.

7.1.3 Responsable del tratamiento o responsable: La persona física o juridical, autoridad pública, servicio u otro organism que, solo o juntos con otros, determinen los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determinan los fines y medios del tratamiento, el responsible del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

7.1.4 Limitacion del tratamiento: El marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el future.

7.1.5 Elaboración de perfiles: Toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

7.1.6 Seudonimización: El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

7.1.7 Fichero: Todo conjunto estructurado de datos personales, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

7.1.8 Encargado del tratamiento o encargado: La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

7.1.9 Responsible del tratamiento o responsable: La persona física o juridical, autoridad pública, servicio u otro organism que, solo o junto con otros, determne los fines y medios del tratamiento; si el

Derecho de la Unión o de los Estados miembros determinan los fines y medios del tratamiento, el esponsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.

7.1.10 Destinatario: La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que 4.5.2016 L 119/33 Diario Oficial de la Unión Europea ES puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento;

7.1.11 Tercero: Persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado;

7.1.12 Consentimiento del interesado: 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;

7.1.13 Violación de la seguridad de los datos personales: Toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

7.1.14 Datos genéticos: Datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona;

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

7.1.16 Datos relativos a la salud: Datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

7.1.17 Establecimiento principal: a) En lo que se refiere a un responsable del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión, salvo que las decisiones sobre los fines y los medios del tratamiento se tomen en otro establecimiento del responsable en la Unión y este último establecimiento tenga el poder de hacer aplicar tales decisiones, en cuyo caso el establecimiento que haya adoptado tales decisiones se considerará establecimiento principal; b) en lo que se refiere a un encargado del tratamiento con establecimientos en más de un Estado miembro, el lugar de su administración central en la Unión o, si careciera de esta, el establecimiento del encargado en la Unión en el que se realicen las principales actividades de tratamiento en el contexto de las actividades de un establecimiento del encargado en la medida en que el encargado esté sujeto a obligaciones específicas con arreglo al presente Reglamento.

7.1.18 Representante: Persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.

7.1.19 Empresa: Persona física o jurídica dedicada a una actividad económica, independientemente de su forma jurídica, incluidas las sociedades o asociaciones que desempeñen regularmente una actividad económica;

7.1.20 Grupo empresarial: Grupo constituido por una empresa que ejerce el control y sus empresas controladas.

7.1.21 Normas corporativas vinculantes: Las políticas de protección de datos personales asumidas por un responsable o encargado del tratamiento establecido en el territorio de un Estado miembro para transferencias o un conjunto de transferencias de datos personales a un responsable o encargado en uno o más países terceros, dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta;

7.1.22 Autoridad de control: La autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51; 4.5.2016 L
119/34 Diario Oficial de la Unión Europea ES

7.1.23 Autoridad de control interesada: La autoridad de control a la que afecta el tratamiento de datos personales debido a que: a) el responsable o el encargado del tratamiento está establecido en el territorio del Estado miembro de esa autoridad de control; b) los interesados que residen en el Estado miembro de esa autoridad de control se ven sustancialmente afectados o es probable que se vean sustancialmente afectados por el tratamiento, o c) se ha presentado una reclamación ante esa autoridad de control;

7.1.24 Tratamiento transfronterizo: a) El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro, o b) el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro;

7.1.25 Objeción pertinente y motivada: La objeción a una propuesta de decisión sobre la existencia o no de infracción del presente Reglamento, o sobre la conformidad con el presente Reglamento de acciones previstas en relación con el responsable o el encargado del tratamiento, que demuestre claramente la importancia de los riesgos que entraña el proyecto de decisión para los derechos y libertades fundamentales de los interesados y, en su caso, para la libre circulación de datos personales dentro de la Unión;

7.1.26 Servicio de la sociedad de la información: Todo servicio conforme a la definición del artículo 1, apartado 1, letra b), de la Directiva (UE) 2015/1535 del Parlamento Europeo y del Consejo (1);

7.1.27 Organización internacional: Una organización internacional y sus entes subordinados de Derecho internacional público o cualquier otro organismo creado mediante un acuerdo entre dos o más países o en virtud de tal acuerdo.

7.1.28 Evaluación del impacto relative a la protección de datos: proceso concebido para describer el tratamiento, evaluar su necesidad y proporcionalidad y ayudar a gestionar los riesgos para los derechos y libertades de las personas físicas derivados del tratamiento de datos personales, evaluándolos y determinado las medidas para abordarlos.

7.1.29 Habitual: Se asocial con uno o más de los siguientes significados:

- Continuando o que se produce a intervalos concretos durante un period concreto.
- Recurrente o repetido en momentos prefijados.
- Que tiene lugar de manera constant o periódica.

7.1.30 Sistematico: se asocia con uno o más de los siguientes significados:

- Que se produce de acuerdo con un sistema.
- Preestablecido, organizado o metódico.
- Que tiene lugar como parte de un plan general de recogida de datos.
- Llevado a cabo como parte de una estrategia.

7.1.31 A gran escala: se tendrán en cuenta los siguientes factores a la hora de determnar si el tratamiento se realize a gran escala:

- El número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente.
- El volume de datos o la variedad de elementos de datos que son objeto de tratamento.
- La duración, o permanencia, de la actividad de tratamento de datos.
- El alcance geográfico de la actividad de tratamiento.

2.- En particular, en relación con la evaluación de impacto relativo a la protección de datos se entenderá por:

7.2.1 Amenaza: cualquier evento que pudiera causar daño a los actives, operaciones o personal de una organización. Las amenzas habituales suelen ser:

- Ambientales: cubren desastres naturals. Es dificil proteger contra determinados desastres naturals debido a su alta naturaleza destructive.
- Técnicas: incluyen incendios, fallos de la energía eléctrica, fallos en la calefacción, ventilación y aire acondicionado, problemas en los sistemas de información y software, fallos en las telecomunicaciones y fuga de aguas. Las amenzas técnicas suelen estar presents en cada organización y son bastantes communes. Con una planificación suficiente es possible manejar las amenzas técnicas de forma adecuada.
- Ocasionadas por el hombre: pueden incluir daños derivados de empleados/as descontentos, sabotaje corporativo e inestabilidad política que interrumpe las funciones de negocio. Tales

amenazadas son, por lo general, fáciles de identificar por su ubicación y contesto, y con una planificación adecuada es possible protegerse contra ellas.

7.2.2 Vulnerabilidad: es una debilidad en un sistema, tecnología, proceso, personas o control que puede explotarse y provocar una exposición. Una vulnerabilidad que puede ser explotada por amenazas genera un riesgo. Uno de los aspectos de la gestión de riesgo es el tratamiento de las vulnerabilidades para mantener el riesgo dentro de los límites aceptables determinados por la toleracia al riesgo de la organización. La gestión de vulnerabilidades forma parte de la capacidad de gestión de incidentes; es la identificación, monitoreo y solución proactivos de cualquier debilidad.

7.2.3 **Riesgo** es una análisis importantísimo que es la base para la gestión de la seguridad de la información. Existen varios riesgos que son especificios de la gestión y respuesta a incidentes y deben considerarse con base en su magnitude y frecuencia, así como en la posibilidad de que ocasionen un impacto.

7.2.4 Contención del riesgo: después de que se haya identificado y confirmado un incidente, el equipo de gestión de incidentes se pone en marcha. El equipo lleva a cabo una evaluación detallada y se pone en contacto con el responsible del sistema o de los actives de información afectados a fin de coordinar las acciones que se llevaran a cabo. La acción que se tome en esta fase tundra el propósito de limitar o contener la exposición.

7.2.5 Erradicación: cuando se han aplicado las medidas de contención, es el momento para determiner la causa raíz del incidente y erradicarla.

7.2.6 Recuperación: esta fase garantiza que los sistemas o servicios afectados se restablezcan.

8.- PROCEDIMIENTO A SEGUIR EN LA EIPD.-

8.1 Determinación del riesgo inherente.

El riesgo inherente es el riesgo intrínsico de cada actividad, sin tener en cuenta las medidas de control que mitigan o reducen su nivel de exposición. El riesgo inherente surge de la exposición que se tenga a la operación de tratamiento en particular y de la probabilidad de que la amenza asociada al riesgo se materialice.

La probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice. En tal sentido, se utilizará una metodología de evaluación de la probabilidad basada en cuatro niveles posibles (despreciable-limitada-significativa-máxima), de acuerdo con lo recogido en la norma ISO/IEC 23134:2017 "***Directrices para la evaluación de impacto sobre la privacidad."***

ESCALA DE PROBABILIDAD	
PROBABILIDAD DESPRECIABLE	La probabilidad de ocurrencia es muy baja (ej. Un evento que puede pasar de forma fortuita.
PROBABILIDAD LIMITADA	La probabilidad de oucrrencia es baja (ej. Un

	evento que puede pasar de forma occasional)
PROBABILIDAD SIGNIFICATIVA	La probabilidad de ocurrencia es alta (ej. Un evento puede pasar con bastante frecuencia.)
PROBABILIDAD MÁXIMA	La probabilidad de ocurrencia es muy elevada (ej. Un evento cuya ocurrencia se produce con mucha frecuencia.

El impacto se determina en base a los posibles daños que se pueden producIr si la amenaza se materializa. De igual modo, se utilizará una metodología de evaluación del impacto basada en cuatro niveles posibles (despreciable, limitado, significativo, máximo,) de acuerdo con lo recogido en la norma ISO/IEC 29134:2017 "Directrices para la evaluación de impacto sobre la privacidad."

ESCALA DE IMPACTO	
IMPACTO DESPRECIABLE	El impacto es muy bajo (ej. Un evento cuyas consecuencias son prácticamente despreciables sin impacto sobre el interesado).
IMPACTO LIMITADO	El impacto es bajo (por ejempo, un evento cuyas consecuencias implican un daño menor sin impacto relevante sobre el interesado).
IMPACTO SIGNIFICATIVO	El impacto es alto (ej. Un evento cuyas consecuencias implican un daño elevado con impacto relevante sobre el interesado).
IMPACTO MÁXIMO	El impacto es muy alto (ej. Un evento cuyas consecuencias implican un daño muy elevado con impacto critic sobre el interesado).

Tomando como base las escalas de probabilidad e impacto, para poder determiner el riesgo inherente, es necesario asignar valores numéricos a cada uno de los niveles de las escalas de probabilidad e impacto. La escala de asignación de valores numéricos comprende desde el valor 1, en el caso de que la magnitude sea despreciable, hasta el valor 4 en el caso donde la magnitude es maxima.

ESCALA DE VALORES	
1	DESPRECIABLE
2	LIMITADO
3	SIGNIFICATIVO
4	MÁXIMO

El cálculo del riesgo inherente se realize mediante la siguiente formula:

RIESGO= PROBABILIDAD X IMPACTO

Se ha de seguir una EIPD desde un punto de vista del interés del sujeto interesado, no focalizando en el interés de la entidad y el riesgo al que ser sometido.

En la evaluación será importante hacer una valoración de los riesgos, en base a la probabilidad de los mismos y su impacto, siguiendo una metodología que no se concreta por ley, porque será adaptada o personalizada por cada identidad de tratamiento de datos.

1. VALORACIÓN DEL RIESGO INHERENTE.- El riesgo inherente hace referencia al nivel de amenaza que existe de modo intrínseco a la propia figura del responsable según su actividad, organización, estructura y planteamiento de cumplimiento. Es decir, se trata de aquellas amenazas que se localizan en la entidad sin aplicar ninguna medida de seguridad.

   El impacto se refiere al conjunto de consecuencias que tendría el evento dañoso en caso de que se acabase materializando.

   La probabilidad es la frecuencia con la teóricamente se podría llegar a producir el riesgo al no haber controles que la mitiguen. Se determina en base a las posibilidades que existen de que la amenaza se materialice.

2. VALORACION DEL RIESGO RESIDUAL.- Dicho riesgo es el que afecta a cada actividad una vez se hayan aplicado las medidas de control para mitigar o reducir su nivel de exposición. La fórmula es:

   RIESGO RESIDUAL = PROBABILIDAD X IMPACTO

3. PLAN DE ACCION.- El plan de acción es el conjunto de iniciativas que deben llevarse a cabo para implantar los controles que ayudan a reducir el riesgo de una actividad de tratamiento hasta un nivel considerado aceptable. Este plan deberá incluir al menos algunos de los siguientes aspectos:
   - Control y su descripción
   - Responsable de implantación
   - Plazo de implantación.

PROBABILIDAD	**MAXIMA 4**	**4**	**8**	**12**	**16**
	SIGNIFICATIVA 3	**3**	**6**	**9**	**12**
	LIMITADA 2	**2**	**4**	**6**	**8**
	DESPRECIABLRE 1	**1**	**2**	**3**	**4**
MATRIZ DE RIESGOS		**Despreciable 1**	**Limitado 2**	**Significativo 3**	**Máximo 4**
		IMPACTO			

Determinando, en function de la escala de asignación de valores numéricos predefinida, el valor de la probabilidad y el valor del impacto, se obtiene una posición en la matriz de riesgos que se corresponden con el riesgo inherente, resultando de aplicar la formula “riesgo=probabiliad * impacto”.

En función del valor obtenido como resultado de la aplicación de la formula para el cálculo del riesgo inherente, se determna el nivel de riesgo inherente (bajo, medio, alto, muy alto), en base a la siguiente escala.

NIVEL DE RIESGO INHERENTE

BAJO	Si el valor resultante se sitúa entre los valores 1 y 2
MEDIO	Si el valor resultante es mayor de 2 y menor o igual que 6
ALTO	Si el valor resultante es mayor que 6 y menor o igual que 9
MUY ALTO	Si el valor resultante es mayor que 9

De conformidad con lo señalado por la Agencia Española de Protección de Datos en su Guía práctica para la evaluaciones de impacto en la protección de los datos sujetas al RGPD, durante la fase de evaluación de riesgos, se debe realizar este ejercicio para cada una de las amenazas identificadas, considerando los riesgos asociados, el impacto y la probabilidad de que se materialicen.

8.2 Gestión el riesgo:

En esta etapa de la EIPD se definen las medidas necesarias para disminuir la probabilidad y/o el impacto de que se terminen materializando el riesgo inherente de una operación de tratamiento.

Dependiendo de las circunstancias concretas, las medidas de control propuestas pretenderán la consecución de alguna de las siguiente finalidades:

- **Mitigar el riesgo inherente**: En este se desarrollarrán acciones concretas que, o bien disminuyan la probabilidad de que se materialice la amenaza, o bien disminuyan el impacto en caso de que se acaben materializando.

- **Eliminar el riesgo inherente**: Se establecerían medidas que modificasen por complete las condiciones originals a partir de las cuales se genera la amenaza.

- **Aceptar el riesgo inherente:** Estableciendo una política, estableciendo de forma paralela una política de actuación que se active en caso de que la amenaza terminarse por matrializarse.

- **Transferir el riesgo inherente:** De esta manera, se trasladaría el impacto negative del riesgo a un tercero.

Independientemente de su character, todas las medidas de control tienen como objetivo minimizar el riesgo asociado a una operación de tratamiento hasta un nivel que permita a la entidad garantizar los derechos y libertades de los interesados a la vez que continua ejerciendo su actividad propia en las mismas condiciones.

9.- RESPONSABLE:

9.1 Identificación de roles:

Cumpliendo con la obligación legal determinada en el artículo 24 del REGLAMENTO (UE) 2016/679 DEL PARLAMENTO EUROPEO Y DEL CONSEJO de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos en calidad de Responsable de Tratamiento, **CLUB NATACIÓN ALMERÍA** ha elaborado el presente Documento.

Será responsabilidad del Responsable del Tratamiento, mantener el presente Documento debidamente actualizado y conforme a la legislación y normativa aplicable en cada momento.

El responsable debe estar obligado a aplicar medidas oportunas y eficaces y ha de poder demostrar la conformidad de las actividades de tratamiento con el Reglamento General de Protección de Datos, incluida la eficacia de las medidas. Dichas medidas deben tener en cuenta la naturaleza, el ámbito de contexto y los findes del tratamiento así como el riesgo para los derechos y libertades de las personas físicas.

9.1.1 Identificación de roles (Responsabilidad del responsable del tratamiento).

Como indica el artículo 24 del RGP, cuyo encabezamiento coincide con el de este apartado, "el responsible del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento."

Asimismo, los artículos 5,25, y 35 reiteran la responsabilidad del Responsible del Tratamiento (UPNA) en lo relativo a sus obligaciones: responsabilidad proactive, licitud, lealtad y transparencia, limitación de la finalidad, privacidad desde el diseño y por defecto, así como evaluación de impacto en material de protección de datos.

9.1.2 Identificación de roles (Encargado del Tratamiento).

Conforme a los artículos 4.8 y 28 del RGPD, el Encargado de Tratamiento de Datos es la persona o entidad que trate datos personales por cuenta del responsible del tratamiento. Asimismo, el Encargado deberá actuar siguiendo las instrucciones del Responsible (artículo 29 del RGPD).

El cumplimiento normativo que regirá en éste ámbito será:

9.2 PRINCIPIOS RELATIVOS AL TRATAMIENTO:

*Se recogen los datos personales con fines explícitos.

*Los datos personales se mantienen exactos.

*Se mantienen actualizados.

*Se rectifican los datos personales inexactos respecto de la finalidad.

*Se suprimen los datos personales inexactos respectos de la finalidad.

*Se mantienen durante más tiempo del necesario respecto de la finalidad.

*Se han implantado medidas de seguridad para proteger la identidad y confidencialidad de los datos.

*Se mantiene la trazabilidad de los fines del tratamiento.

9.3 LICITUD DEL TRATAMIENTO.-

Se tiene consentimiento para cada finalidad del tratamiento.

El tratamiento es necesario para ejecutar un contrato o precontrato.

Existe obligación legal.

9.4 CONDICIONES PARA EL CONSENTIMIENTO.-

Se puede demostrar que el afectado dio su consentimiento para el tratamiento.

Se solicita usando lenguaje claro y sencillo.

Se permite retirar el consentimiento con la misma facilidad con la que se recaba.

Se ofrecen medio para retirar el consentimiento en cualquier momento

Para prestar el servicio se solicitan todos los datos necesarios

9.5 CONSENTIMIENTO DE NIÑOS EN RELACIÓN CON LOS SERVICIOS A PRESTAR-

Se recaba el consentimiento de menores de 14 años al titular de la patria potestad o tutela sobre el niño

Se verifica que el consentimiento fue dado por el titular de la patria potestad o tutela sobre el niño.

10.- METODOLOGIA DE LA EIPD.-

El equipo de trabajo interviniente en ésta evaluación de impacto es la dirección del Club de Natación Almería. Dicho equipo está formado en materia de protección de datos, y lleva a cabo cada una de las actividades requeridas para tener actualizada su documentación en éste tema.

10.1 DOCUMENTACION DE REFERENCIA:

- Guía práctica para la 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 infromación.
- Norma UNE-EN ISO/IEC 27002:2017 Código de prácticas para los controles de seguridad de la información.
- Norma ISO/IEC 27701:2019 Extensión 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.

10.2 ANÁLISIS DE LA NECESIDAD DEL TRATAMIENTO.-

El Club de Natación Almería es responsable de distintos registros de actividades de tratamiento con datos de carácter personal. Para ello llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta del responsable, y que contenga:

1. Nombre y datos de contacto del encargado y de cada responsable por cuenta del cual actúe el encargado, y en su caso, del representante del responsable o del encargado, y del delegado de protección de datos en su caso.

2. Las categorías de tratamientos efectuados por cuenta de cada responsable.

3. Las transferencias de datos personales a un tercer país u organización, en el caso de transferencias indicadas en el art. 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas.

4. Cuando se posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1 del reglamento.

Los registros constarán por escrito, inclusive en formato electrónico.

El Club de Natación de Almería dispone de distintos equipos mediante los cuales se tratan o almacenan datos de carácter personal. Asímismo también dispone de diferentes programas informáticos mediante los cuales se tratan o almacenan datos de carácter personal.

Todos aquellos datos de carácter personal (rasgos faciales, huella digital, etc), serán transformados en datos biométricos a través de la empresa externa contratada para ello.

10.3 BENEFICIOS PARA LOS INTERESADOS.-

El correcto mantenimiento de los datos resulta de gran interés para el titular de los mismos. En general el correcto tratamiento de los datos otorgados a Club Natación Almeria, para el ejercicio de su actividad genera los siguientes beneficios:

1.- Beneficio directo y objetivo para los sujetos sobre los que inciden los riegos.

2.- Mejor servicio para todos lo socios/as del club.

3.- Mayor accesibilidad a la información.

4.- Mayor sostenibilidad medioambiental.

5.- Mayor transparencia en el tratamiento de los datos.

6.- Mayor confidencialidad en last areas realizadas por el Club.

7.- Disminuir la discriminación por género, por edad, por nacionalidad, por discapacidad.

8.- Empoderamiento del interesado

10.4 BENEFICIOS PARA EL CLUB DE NATACION ALMERIA.-

Los posibles beneficios para la entidad son los siguientes:

1.- Cumplimiento de las normas

2.- Mejora de la eficiencia al recabar únicamente los datos que resulten necesarios.

3.- Reducción de costes

4.- Mejora de la seguridad de los involucrados.

5.- Incremento del control.

6.- Mejora de imagen.

7.- Mayor transparencia en las actuaciones del club.

8.- Alineación del Club con la responsabilidad social.

ALTERNATIVA AL TRATAMIENTO Y POR QUÉ NO SE HAN ELEGIDO:

Las cuestiones relativas a tratamiento de datos se han llevado a cabo bajo los criterios de idoneidad, buscando que sean los menos lesivos posibles a los intereses de los titulares de datos.

Los datos de la relación cliente/usuarios del Club Natación se encuentran siempre en el ámbito de las actividades enmarcadas en los fines recogidos en los Estatutos del Club Natación Almeria.

En el Registro de Tratamiento de los datos se pormenorizan tales procedimientos.

A estos efectos descritos, se considera que utilizando las medidas de protección implementadas por el Club Natación Almería se adoptan medidas suficientes para la protección de datos personales, lo que se encuentran perfectamente ajustado a los objetivos perseguidos por el Club.

Los datos solicitados siempre tenderán al mínimo posible para el fin propuesto.

MEDIDAS PARA LA REDUCCIÓN DEL RIESGO:

El objeto de este apartado es el de establecer medidas de gestión, organización, definición del tratamiento, procedimentales y técnicas que permiten gestionar cada uno de los elementos de riesgo identificados en el apartado VII "analisis de la obligación de realizar una EIPD: evaluación del riesto.

Optimización del tratamiento:

Los mayores riesgos relativos a los datos en la actividad del Club Natación radican en el mantenimiento y posterior comunicación de los datos a las entidades necesarias para las gestiones con los socios/as, como a las del resto de usuarios.

Respecto del mantenimiento se establecen contraseñas para el acceso a cualquier aplicación del Club (apps y web). Para el almacenamiento de los documentos físicos que seran conservados en sitios de acceso público se hará uso de llave en puertas y armarios según corresponda.

Respecto de la emisión de los datos, siempre serán utilizados con la única finalidad para la que son recopilados.

Medidas PBDD

Para una major gestión de los datos, las medidas de "privacidad desde el diseño y por defecto" aplicables por parte del Club Natación Almería dependerá del tipo de tratamiento. Entre otras medidas se aplicarán las siguientes:

1.- Minimación de datos:

- Eliminación más temprana posible de los datos que no sean necesarios.
- Minimizar los datos recogidos y tratados en cada una de las etapas del tratamiento.
- MIniminación de la frecuencia con que se produce la recogida de datos.
- Anonimización temprana de los dados, en su caso.
- Limitación de la accesibilidad de bases de datos a través de la red.
- Seudoanonimación de los datos almacenados, en su caso.
- Seudoanonimación de los datos en alguno de los subprocesos del tratamiento, en su caso.

2.- Ocultación:

- Anonimación temprana.
- Seudoanonimación de los datos almacenados.
- Seudonomimación de los datos en algunos de los subprocesos del tratamiento.

- Introducción de medidas perturbativas en los datos de origen
- Control de la privacidad de los metadatos en las comunicaciones electrónicas.
- Uso de credenciales basadas en atributos.
- Cifrando de la información almacenada o en tránstio.

3.- Separación:

- Compartimentación del acceso a los datos a lo largo del tiempo.
- Compartimentación del acceso a los datos entre diferentes tratamientos.
- Particionamiento por atributos de la base de datos.
- Separación física de las Fuentes de datos en que estén en distintos ficheros.
- Bloqueo de datos.

4.- Agregación:

- Generalización de datos personales.
- Agregación de registros.
- Reducción de la presión, granularidad de recogida de los datos.
- Aplicación de diferenciales de privacidad en la diffusion y acceso a los resultados del tratamiento.
-

5.- Información:

- Transparencia de la extension del tratamiento para el sujeto de los datos.
- Transparencia sobre el momento en que se está realizando una recogida de datos.
- Actualización periódica de las políticas de protección de datos .
- Actualización perióidica de firma de protección de datos en las comunicaciones electrónicas y físicas.
- Actualización periodica de la cláusula de protección de datos.

6.- Control

- Control del usuario en la recogida de sus datos personales.
- Control del usuario del tratamiento de sus datos personales.
- Cifrado de la información extreme-extremo.

11.- JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL

11.1 JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL (Finalidad):

El Club Natación Almería fundamenta la implantación de un sistema de reconocimiento facial para acceder a nuestras instalaciones en la necesidad de controlar el aforo o nivel de ocupacion de las instalaciones y la pertenencia o vinculación de quiénes acceden al club, particularmente en periodos de gran afluencia de personas o escasez de espacios libres.

11.2 JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL (necesidad):

El CNA estima que el uso de la tarjeta de acceso al club no acredita suficientemente la comprobación de quién accede en todo momento a las intalaciones, requiriéndose, por consiguiente, un sistema que sí permita inequívocamente una identificación univocal y fidedigna.

11.3 JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL (idoneidad):

En base a los apartados 4.1 y 4.2 el CAN concibe el sistema de reconocimeinto facial previsto como un tratamiento de datos adecuado a la finalidad perseguida, necesario e idóneo. Asimismo, lo percibe como un tratamiento proporcional, dado que se basa en el consentimiento de las personas afectadas. Por ello, el CNA prevé un sistema alternative de identificación y registro diarios para aquellas personas, que deseando acceder a las instalaciones deportivas, no consientan el reconocimiento facial implementado.

11.4 JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL (conclusión):

Ante el recordatorio, formulado por el DPD, sobre la exigencia legal de suficiente poderación de los factores aludidos en los apartados 4.1, 4.2 y 4.3, el CNA, como responsible, ratifica y confirma la suficiencia de la ponderación efectuada en el mardo de su propia responsabilidad.

La discrecionalidad del CNA en la poderación de los factores indicados no excluiría la fiscalización, por parte de la autoridad de control o los tribunals de aspect tales como la tutela de los derechos fundamentals, el control de elementos reglados, la comprobación de los hechos determinandes y la interdicción de arbitrariedad o de desviación de poder.

Mas allá del recordatorio indicado y de la edición del presente document informative, el DPD solo puede, en relación con la ponderación mencionada, informar a cualquier persona afectada sobre su posibilidad de presenter una reclamación ante DPD del club y en su defecto ante la Agencia Española de Protección de Datos https://aepd.es/es.

12.- SISTEMA DE RECONOCIMIENTO FACIAL:

12.1 JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL (objeto técnico):

El sistema de reconocimiento facial consiste en un modelo de verificación biométrica fundamentado en el esquema uno-a-varios.

Para los usuarios de las instalaciones deportivas se generará un vector biométrico temporal, en el momento de acceso, que sera cotejado con los vectores permanentemente alojados en la base de datos biométricos vinculados al sistema.

El vector biométrico temporal será generado de forma instantenea en cada acceso para cada usuario. Los vectores permanents corresponden a aquellos vectores generados a partir de una imagen facilitada por los usuarios previamente registrados a fin de accedes a las instalaciones deportivas.

El sistema cotejará el vector generado para cada usuario en el momento de acceso con los vectores permanents de la base de datos de uruarios registrados. El cotejo sera positive si se detecta un nivel de coincidencia suficiente entre el vector instantáneo de acceso y alguno de los vectores permanents registrados. La positividad del cotejo habilitará el acceso deseado.

12.2 JUSTIFICACION DEL SISTEMA DE RECONOCIMIENTO FACIAL (tratamiento de datos de caracter especial):

Este tipo de reconocimiento facial constituye un sistema de verificación biométrica o identificación uno-a-varios. Por ello, constituye un tratameinto de datos personales biométricos de caracter especial. Esta calificación resulta acorde a lo dispuesto en los artículos 4.14 y 9.1 del Reglamento General de Protección de Datos de la Unión Europea (RGPD).

Esta distinction puede observarse claramente en el Dictamen 3/2012 del grupo de trabajo 29 vinculado al Comité Europeo de Protección de Datos. Dicho dictamen distingue entre la biometría de identificación y la biometría de autenticación o verificación.

La biometría de identificación consiste en comparer un vector biométrico instantaneo del sujeto a identificar con potencialmente todos los vectores permanents de los sujetos previamente identificados y registrados en una base de datos. Esta operación identificativa de comparación termina con la conclusion de identidad entre el vector instantáneo y el permanente del mismo sujeto.

La biometría de verificación o autenticación se limita a cotejar directa y únicamente el vector instantáneo del sujero a verificar con su vector permanente previamente registrado.

Mas allá de los aspectos técnicos implicados, la biometría de verificación o autenticación es considerada una forma de tratamiento de datos de caracter ordinario. No obstante, la biometría de identifiación es considerada legalmente como un tratamiento de datos de caracter especial.

12.3 CARACTER VOLUNTARIO DEL SISTEMA (exigencia de consentimiento):

Considerando lo restrictive de las bases jurídicas que legitiman el tratamiento de datos de carácter especial (artículo 9.2. del RGPD), el CNA decide basar la legitimación del reconocimiento facial en el consentimiento de las personas afectadas (artículo 9.2.a) del RGPD.

Se descarta fundamentar dicha legitimación en otras bses previstas en el artículo 9.2. ni siquiera en el intereés public esencial que habilitaría el reconocimiento facial para control de

acceso a centrales nucleares, quirófanos higienizados y laboratorios con riesgos biológicos o que suele ser usado en ámbitos aduaneros, transfronterizos o de tránsito internacional.

Por todo ello, se concluye que solo cabe basar el sistema proyectado en el consentimiento de las personas afectadas. Esta circunstancia require respetar la verdadera voluntariedad del consentimiento y, consecuentemente, proveer un sistema de acceso alternative que no implique el tratamiento de datos de character especial.

12.4 CARACTER VOLUNTARIO DEL SISTEMA (provision de sistema alternativo):

Los usuarios que no consientan el tratamiento de datos aludido podrán acceder a las instalaciones deportivas previo registro y provision de un identificador que les permita tal acceso durante el día en curso.

La identificación, el registro y la provision de un identificador para el acceso a las instalaciones deportivas del CNA constituyen datos personales de character no especial. El Responsible de Tratamiento de estos datos personales es igualmente el propio club. El Encargado de Tratamientos es también el contratista del sistema de reconocimiento facial en la medida de su participación en las operaciones de tratamiento de datos de identificación, registro y provision de identificador.

La habilitación de este sistema de acceso alternative deberá ser facilitado igualmente por el club, permitiendo el acceso de estos socios/as a las instalaciones deportivas del CNA sin someterse al sistema de reconocimiento facial. Esta finalidad puede lograrse mediente la deshabilitación de dicho sistema en el momento de su acceso o a través de una acceso distinto al vinculado al sistema, opción esta última es a la que adoptará el Club Natación Almería.

La legitimación para el tratamento de datos de identificación, registro y provision de identificador se base en la mission de interés public que constituye la finalidad de controlar el aforo de usuarios y su pertenencia al Club Natación Almeria.

El tratamiento de datos de identificación, registro y provisión de identificador se fundamenta en el interés publico descrito y no en el consentimiento de las personas interesadas. Por ello, se erige como un tratamiento de datos de caracter obligatorio para facilitar un acceso alternativo a las instalaciones del club a las personas que no consientan su reconocimiento facial como forma de acceso.

12.5 CARACTER VOLUNTARIO DEL SISTEMA (tratamiento alternativo y obligatorio de datos ordinarios):

La disonancia entre la voluntariedad del reconocimiento facial y la obligatoriedad de registro e identificación de quién no consienta dicho reconocimiento se basa en las distinta naturaleza de los datos a tartar. Los datos de identificación, registro y provision de identificador son datos de character no especial, sujetos a las bases generals de legitimación prevista en el artículo 6.1. del RGPD. Los datos de identificación biométrica (reconocimiento facial) son datos de character especial, sujetos a las bases específicas y restrictivas del artículo 9.2. del RGPD.

El CNA, como responsible de tratamiento, ostenta legitimación suficiente para tartar de forma obligatoria, por razón de interés public, datos de carácter no especial de los usuarios del Club Natación Almería para el control de accesos a las mismas. Sin embargo, en el caso de los datos especiales (reconocimiento facial), su hipotética obligatoriedad exigiría una fundamentación basada en interés publico esencial (artículo 9.2. del RGPD). La compleja apreciación de la esencialidad aludida y el respeto a la decision de los usuarios sobre su reconocimiento facial aconsejan que el CNA limite el reconocimiento facial solo a aquellos socios/as que así lo consientan.

La identificación y el registro de los socios/as del club que vaya a accede a dicha instalación deportiva resultan en todo caso obligatorios pero su reconocimiento facial ostenta un character voluntario, sujeto a su propio consentimiento. Para aquéllos que no lo consientan se articula un sistema de provision diaria de identificadores de acceso.

12.6 DEBER DE INFORMACION A LOS AFECTADOS POR RECONOCIMIENTO FACIAL O AUTORREGISTRO DIARIO:

El CNA como Responsible de Tratamiento, facilitará a los interesados el ejercicio de sus derechos de mayor información, acceso, oposición, supresion y otros en relación con sus datos facilitándoles la comunicación con denuncias@cnalmeria.com y haciéndoles constar su facultad de plantear la correspondiente reclamación ante https://www.aepd.es/es.

12.7 Sistema de acceso para los trabajadores:

Los trabajadores pertenecientes a la plantilla del Club Natación Almería, accederan a sus instalaciones a través del porton anexo.

12.8 INTERVENCION DEL REPONSABLE DE TRATAMIENTO:

El Delegado de Protección de Datos (DPD) ha inducido un proceso de reflexión por parte de la UPNA (Responsable de Tratamiento de Datos) sobre las siguientes cuestiones:

- El reconocimeinto facial no es una técnica anónima de gestión de información de las personas.

- El reconocimiento facial sí comprota el tratamiento de datos de character personal.
- La conservación de imagen (foto) no faculta la generación de vectores biométricos a partir de tal imagen sin informar a las personas afectadas ni recabar su consentimiento.
- El tratamiento de datos inherente al reconocimiento facial empleado ostenta character especial.
- El empleo de dicho sistema no puee fundamentarse en bases distintas al consentimiento.
- El consentimiento exige respetar su character voluntario y proveer acceso alternative.
- El responsible de Tratamiento responde de la necesidad, idoneidad y proporcionalidad del tratamiento de datos resultante del sistema previsto de reconocimiento facial.
- La Evaluación de Impacto corresponde en primer y principal término al Responsible (UPNA).

La Agencia Española de Protección de Datos (AEPD) ha resuelto una cuestión planteada sobre el reconocimiento facial, cuyo contenido se adjunta en el enlace facilitado a continuación:
https://www2.unavarra.es/gesadj/seguridadInf/normativa-proteccion-datos/consulta_aepd.pdf.

Asimismo este DPD continua a disposición del Responsible de Tratamiento para asesorar a dicho responsible en cualquier evaluación que precise en la material.

12.9 RECLAMACIÓN ANTE LA AGENCIA ESPAÑOLA DE PROTECCION DE DATOS:

El Delegado de Protección de Datos o el Encargado del Tratamiento informará a cualquier persona afectada o interesada en los tratamientos de datos descritos en la presenta Evaluación de Impacto. Parte de dicha labor informativa consiste en exponer el derecho de las personas a presentar una reclamación ante la AEPD.

Habiendo desarrollado el Responsible de Tratamiento (UPNA) un proceso previo de reflexión sobre las condiciones del reconocimiento facial, el ejercicio de derechos frente a dicha condiciones, sin perjuicio de la información y orientación del DPD, puede canalizarse medienta la presentación de la correspondiente reclamación ante la EAPD https://www.aepd.es/es.

12.10 ACCESO BIOMETRICO DAS-GATE:

12.10.1 Acceso biométrico al club:

El acceso al club cuenta con un software de control de accesos y un software de gestión con el que actualmente cumplen al menos tres funciones:

*Mantener una ficha de cada socio.

*Gestionar reservas de pistas, recursos y suscripciones a actividades.

*Controlar los derechos de acceso de los socios.

El club cuenta con una pagina web.

En lo relativo a la autenticación de usuarios para el acceso, el club normalmente cuenta con varias alternativas. Las habituales son:

- Tarjetas para su lectura automatic en las propias puertas de acceso al parking y al edificio del gimnasio y vestuarios.
- Aplicación móvil que le permite la comunicación con el club.
- Carnet y fichas de socios, con fotografías facials, para el reconocimiento por el personal del club de no poder accede por los otros canales así como para supervisor el uso del resto de métodos de autenticación.

  Los lectores colocados en las puertas de acceso se comunican con una controladora o con un servidor central que es el encargado de revisar los derechos de acceso de la persona identificada y activar o no la aperture de la puerta correspondiente, dejando constancia en los sistemas del club del acceso del socio.

Los parámetros más importantes que definen la integración entre los sistemas y la operación de Das Gate son:

- Se prioria la conveniencia y comodidad de los socios sobre criterios.
- Se mantienene operatives los sistemas alternatives de autenticación, como las tarjetas, el control físico por parte del personal de control de acceso al club. La autenticación biométrica debe poder convivir con el resto de mecanismos de autenticación, tanto si están instalados en puertas o carriles diferentes como si están instalados en la misma puerta o carril.
- Es necesario recabar el consentimiento de cada socio, de manera individual.
- Es necesario completer la evaluación de impacto antes de poner en marcha el sistema.

12.10.2 ALTA DE SOCIO DE DAS-GATE:

El alta se produce como secuencia de la prestación del consentimiento por parte del socio, que lo presta a través de los sistemas del club. La prestación del consentimiento desencadena las llamadas entre sistemas necesarias para completer el alta.

Los pasos son los siguientes:

- Se recoge el consentimiento expreso del socio por los medios establecidos por el club, ya sea de forma presencial o remota.
- Los sistemas del club envían la información necesaria a Das-Gate para el alta del socio.
- La nube de Das-Gate procesa la foto generando el vector biométrico correspondien te y eliminando la foto a continuación.
- Das-Gate comleta el alta del usuario, almacenando en BBDD el vector biométrico y el identificador del acceso, y relacionándolos con un identificador único.
- Das-Gate prolonga los cambios en BBDD a todos los terminals biométricos asociados al cliente para así habilitar el acceso biométrico al usuario.

- Das-Gate registra en sus logs el alta del usuario.

12.10.3 BAJA DE SOCIO DE DAS-GATE:

Durante este proceso, el socio no interactúa directamente con Das-Gate en ningún momento. El deseo de dares de baja o de ejercer el derecho de suppression de datos se presta a través de los sistemas del club y desencadena las llamadas entre sistemas necesarios para completer la cancelación de cuenta en Das-Gate y el borrado de los datos del usuario tanto en la nube como en los terminals de Das-Gate

Los pasos son:

- Se recoge el derecho de baja o suppression de datos por los medios establecidos por el club.
- Los sistemas del club envían la petición de cancelación de cuenta para el usuario correspondiente a Das-Gate a través de una llamada.
- Das-Gate procesa la petición y marca la cuenta y datos del socio para su borrado.
- En un plazo temporal nunca superior a 24 horas, Das-Gate borra las cuentas y datos marcados para su borrado.
- Das-Gate sincroniza los cambios en la BBDD central a los terminals biométricos.
- Das-Gate registra en sus logs el ejercicio de derechos.

12.10.4 RECTIFICACION DE DATOS:

Durante este proceso, el socio no interactúa directamente con Das-Gate en ningún momento. El deseo de actualizar el identificador de acceso o la foto del socio se gestiona a través de los sistemas del club., que se encargan de realizar las llamadas entre sistemas necesarias para completer la actualización de los datos en las cuentas de Das-Gate.

Los pasos a seguir son:

- Se recoge el deseo de actualización del selfie así como la nueva foto a través de los sistemas del club, ya sea mediante un proceso presencial o remote.
- Los sistemas del club envían a la nube de Das-Gate la petición de actualización de la credencial biométrica del socio, incluyendo la nueva foto en la petición.
- Das-Gate procesa la foto, obtiene el Nuevo vector biométrico y lo almacena en su BBD, reemplazando el anteriormente asociado al usuario.
- Das-Gate sincroniza los camibos en BBDD a los terminals biométricos, actualizando debidamente el vector biométrico asociado al socio con user_ide.
- Das-Gate registra en sus logs el ejercicio de derechos.

Los pasos para la actualización del identificador de acceso son los siguientes:

- Los sistemas del club envían a la nube de Das-Gate la petición de actualización del identificador de acceso para el usuario con user_id, incluyendo el nuevo identificador en la petición.
- Das-Gate reemplaza el identificador anteriormente asociado al usuario con user-id, con el nuevo identificador recibido en la petición.
- Da-Gate sincroniza los cambios en BBDD a los terminals biométricos, actualizando debidamente el identificador de acceso asociado al vector biométrico del socio.
- Das-Gate registra en su logs el ejercicio de derechos.

12.11.5 Acceso de datos:

12.11.5.1 Trabajadores:

SISTEMA DE ACCESO PARA LOS TRABAJADORES QUE PRESTAN SUS SERVICIOS EN LAS INSTALACIONES DEL CLUB NATACION ALMERIA.

Este sistema, no basado en reconocimiento facial ni en registro diario, debe habilitar un acceso permanente a los trabajadores del club que presten habitualmente sus funciones en las citadas instalaciones y temporal a aquellos otros que efectúen cometidos ocasionales en las mismas.

El sistema deberá evitar para tales trabajadores toda operación de tratamiento de datos. Si ello no fuera posible, deberá emplear formulas que minimicen cualquier tratamiento de datos, tales como el suministro de códigos conjuntos para todo el colectivo de empleados afectados u otras formulas que impidan la trazabilidad de las entradas y salidas de cada empleado.

Resulta esencial eximir de todo tratamiento de datos a estos empleados o, si no fuera técnicamente posible, minimizar cualquier tratamiento de datos que afectare a este colectivo.

Considerando que el CNA justifica el control de accesos a la instalación deportiva en una correcta gestión de aforo, no precisa, para ello, tartar los datos de dichos empleados. Si el CNA aprecia dificultades o impedimentos de carácter técnico para evitar estos tratamientos, esta institución debe minimizar cualquier tratamiento que resultare técnicamente indispensable.

12.11.5.2 Usuarios:

Durante este proceso, el socio no interectúa directamente con Das-Gate en ningún momento. El deseo de ejercer su derecho de acceso se gestiona a través de los sistemas del club (software de gestión, software de control de acceso o gestor especifico de consentimiento) Estas acciones desencadenan las llamadas entre sistemas necesarias para completer el ejercicio de derechos de acceso a los datos almacenados por Das-Gate.

Los pasos para ejercer este derecho son_

- Se recoge el deseo de acceso a datos a través de los sistemas del club, ya sea mediante un proceso presencial (asistido) o remoto.
- Los sistemas del club envían a la nube de Das-Gate la petición de acceso a los datos almacenados en Das-Gate, junto con la contraseña con la que encriptar el archive .zip

que Das-Gate generará, que deberá cumplir unos requerimientos mínimos de seguridad establecidos por Das-gate (al menos ocho caracteres, incluyendo al menos una minuscule, una mayúscula, un número y un character especial)

- Das-Gate devuelve un enlace de acceso único y period de expiración de setenta y dos horas con el que los datos solicitados podrán descargarse desde los sistemas del club Das-Gate, procesa la petición, y un plazo máximo de 48 horas, disponibiliza un archive .zip con todos los datos almacenados en la plataforma asociada al usuario con identificador user_id. Solo se puede accede al archive .zip desde el mismo sistema en el que se realize la petición, una única vez, entre las cuarenta y ocho y setenta y dos horas desde la solicitud de los datos. El archive generado estará protegido mediante contraseña recibida en Das-Gate como parte de la petición. Los datos incluídos en el fichero son:
  - Identificador de usuario de Das-Gate (anónimo)
  - Identificador de acceso (el utilizado por el sistema de control de acceso)
  - Fecha y hora del alta en el sistema.
  - Listado de ejercicios de derecho ejecutados por el socio/a indicando fecha, hora, derechos, y si procede, valor rectificado.
  - Listado de intentos de acceso, indicando fecha, hora y punto de acceso de la autenticación, así como identificador de acceso utilizado para la solicitud de acceso al sistema externo de control de accesos, y si el acceso fué permitido o denegado.
- Das-Gate registra logs correspondientes a este ejercicio de derechos.

12.11.5.3 Acceso mediante reconocimiento facial:

Durante este proceso, el socio/a interactúa directamente con los terminales biométricos de Das-Gate. Los terminales biométricos muestran por pantalla una imagen que invita a los usuarios/as a acercarse para poder ser reconocidos y accede a las instalaciones.

Durante el proceso de reconocimiento, todo el procesamiento es realizado por el propio terminal biométrico de Das-Gate y ninguna imagen ni vector biométrico sale del mismo para su almacenamiento o procesamiento.

El proceso consta de los siguientes pasos:

- Los terminales están analizando constantemente el canal de profundidad proporcionado por su cámara estereoscópica.
- Los terminales solo procesan las imágenes en el espectro visible si detectan algo a menos de un metro de distancia en el canal de profundidad.
- Al procesar la imagen en el espectro visible, el primer paso es aplicar un algoritmo de búsqueda de caras. Todas aquellas caras situadas a más de un metro de distancia son ignoradas. Si hay una o más caras a menos de un metro de distancia, entonces el terminal cambia la imagen mostrada por pantalla y pasa a presenter el espejo digital

(video que está capturando la cámara) para ayudar al usuario a posicionarse correctamente.

- De las caras detectadas a menos de un metro, el terminal descarta todas menos la más prominente.
- Sobre la cara más prominente se aplica el algoritmo biométrico para calcular el vector biométrico asociado a la cara. El terminal también aplica el algoritmo de detección de ataques de suplantación de la identidad para determiner si la cara que está analizando corresponde a un usuario genuine o se trata de un ataque de presentación por pantalla-impresa.
- Una vez obtenido el vector, el terminal realize una búsqueda en su BBDD para localizer el vector de registro más parecido al que acaba de obtener para la cara que tiene delante.
- El terminal compara la puntuación de similitude biométrica obtenido con el umbral de seguridad establecido. Si se supera el umbral, quiere decir que la autenticación del usuario ha sido exitosa.
- Tras una autenticación exitosa, el terminal recupera de su BBDD el identificador de acceso asociado al vector de registro identificado, y lo envía como parte de una petición de acceso al sistema de control de accesos del club junto con cierta información sobre el terminal. La información proporcionada sobre el terminal depende del protocol de comunicación implementado para la integración con los sistemas del club, pero típicamente es una cadena de caracteres representative del punto de acceso donde está instalado el terminal, y/o el número de serie del terminal. En este punto, y según el tipo de protocol de comunicación con el sistema de control de accesos, el terminal pasa a mostrar una pantalla de “verificando credenciales” o “verificando derechos de acceso”.
- Una vez se recibe la respuesta del sistema de control de accesos, si la integración lo permite, el terminal muestra por pantala el mensaje de éxito o fracas correspondiente.
- Los sistemas del club actúan sobre las puertas para permitir, o no, el paso del socio durante el period que tenga establecido.

Una vez comienza un proceso de reconocimiento, con una cara detectada a menos de un metro, el terminal establece un period máximo de reconocimiento (típicamente 5 a 10 sg.) Si dicho period se supera sin un reconocimiento existoso, el terminal muestra una pantalla indicando que no ha podido completer con éxito el reconocimiento del usuario y animándole a pasar por recepción a prestart el consentimien to y comenzar a disfrutrar del acceso biométrico.

13.- FINALIDAD Y CONSENTIMIENTO:

Por parte del responsible del tratamiento, y en este caso particular de Das-Gate como encargado del tratamiento, se adoptarán medidas reforzadas encaminadas a minimizar los riesgos derivados del tratamiento. Es precido tener en particular en cuenta tanto en lo referente al procedimiento de reconocimiento facial, como al modo en que se establece el correspondiente

patron, que no se limita a la mera medición de puntos de la característica biométrica del sujeto, sino que se genera a partir de algoritmos de Inteligencia Artificial, unidos en su caso a otros posibles components del modelo.

Igualmente, deben tenerse en cuenta las consideraciones efectuadas en lo que respecta a las limitaciones de distancia para la obtención de la imagen del interesado en el momento de su acceso a las instalaciones, así como la no conservación por parte de Das-Gate de ningún dato del abonado distinto de su patron facial y que permita asociar dicho patron con información adicional del interesado y la limitación del uso del citado patron a la identificación del abonado que accede al recinto deportivo, sin que los datos sean siquiera utilizados para el entrenamiento y mejora del modelo.

14.- PUBLICACION DE LA EIPD

Como consecuencia del compromiso del CLUB NATACION ALMERIA, con su propia política de protección de datos, la citada entidad se rige, entre otros, por el principio de "licitud, lealtad y transparencia", según el cual los datos personales deben ser tratados de manera lícita, leal y transparente en relación con el interesado.

De tal modo, los resultados finales de la evaluación de impacto relative a la protección de datos (EIAP) se dividen en un Informe interno de evaluación de impacto (informe final), para su conocimeinto por el Órgano de Gobierno de la entidad responsible del tratamiento, y un informe publico de evaluación de impacto (informe final), para fomenter la transparencia y la confianza de los interesados en las operaciones de tratamiento del responsible

15.- LUGAR Y FECHA DE EMISIÓN DEL INFORME:

El presente "informe publico de evaluación de impacto en la protección de datos (Informe Final) se emite en la ciudad de Almeria en fecha 02/02/2022.

Firma en nombre de la entidad responsible del tratamiento (CAN)

Firmado: Luis Carretero Torres
Gerente del Club Natación Almería.

16.- ANEXO I

Puede encontrarse el Registro de Actividades de Tratamiento, siempre a disposición de la AEPD en la web htpps://www.cnalmeria.com.