RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR POR INFRACCIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS PERSONALES

Resolución	RPS-2024/018
Procedimiento Sancionador	PS-2023/020
Expediente	RCO-2022/046 y RCO-2023/084
Entidad incoada	Diputación Provincial de Sevilla
Motivo de la reclamación	Implantación de sistema de control de acceso del personal mediante uso de datos biométricos (reconocimiento facial y de la palma de la mano) sin la necesaria legitimidad, sin EIPD previa ni información al personal.
Artículos afectados	9 y 35 RGPD

Abreviaturas:
RGPD. 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)
LOPDGDD. Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
LOPDP. Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.
LTPA. Ley 1/2014, de 24 de junio, de Transparencia Pública de Andalucía
ESTATUTOS CTPDA. Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, aprobados por Decreto 434/2015, de 29 de septiembre.
LPAC. Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas
LRJSP. Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.
ENS. Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

ANTECEDENTES

Primero. Presentación de la reclamación.

1. El 26 de marzo de 2022 tuvo entrada en el Consejo de Transparencia y Protección de Datos de Andalucía (en adelante, el Consejo) una reclamación suscrita por [NOMBRE DE PERSONA RECLAMANTE], por una presunta infracción de la normativa de protección de datos personales.

En la citada reclamación se exponía lo siguiente:

> " Que el pasado 18 de octubre de 2021 se comunica a través del portal de empleo público (entiéndase en adelante en la empresa Diputación de Sevilla) lo siguiente:
> " (...)INSTALACIÓN DE NUEVOS LECTORES PARA EL CONTROL DE ACCESOS EN TODOS LOS CENTROS DE LA CORPORACIÓN.

Desde hoy lunes, en coordinación con el Área de Régimen Interior, se está procediendo a la sustitución de los antiguos lectores de tarjeta por otros biométricos/reconocimiento facial. Durante este proceso y hasta nueva comunicación, coexistirán los dos sistemas para las entradas y salidas de los diferentes centros, los nuevos lectores que se instalen tienen integrado lectores de tarjetas, con lo que hasta la total extinción de las mismas se podrán utilizar como se ha venido haciendo hasta ahora.

En próximo comunicado, se establecerá el calendario para la toma de los datos necesarios que se precisan (huella /reconocimiento facial), que se fijará con citas por Áreas y Centros de la Corporación."

Este comunicado está firmado por el Director del Área de Empleado Público.

- Que la semana posterior a este comunicado se procede a tomar los datos en mi centro de trabajo y en todo el complejo *[nombre del complejo]* a todas las trabajadoras y trabajadores por una trabajadora asignada a control de presencia.

-Que en ningún caso se solicitó la voluntariedad de la toma de datos, ni se informó de su finalidad y custodia de los mismos, más allá de la interpretación que pudiera desprenderse de acto voluntario por parte de una trabajadora o trabajador frente al empresario.

-Que con fecha 7 de diciembre de 2021, se emite nuevo comunicado a través del mismo medio y con el mismo firmante donde se dice "A partir del próximo jueves 9 de diciembre, se va a proceder al cambio de los tornos situados en la entrada de la Sede Central de la Diputación. Hasta que los datos en los nuevos lectores de reconocimiento facial no estén cargados definitivamente, recomendamos utilicen la tarjeta de empleado/a para realizar las entradas/salidas del edificio.

Pedimos disculpas por los inconvenientes que pudieran producirse hasta la definitiva puesta en marcha del nuevo sistema de entradas y salidas de la Corporación."

- Que el pasado 4 de febrero del presente, sin firma, se realiza a través de nuevo del portal, un comunicado del Área de Empleado Público donde se cita de personal y Comité de Empresa pidieron información sin que la respuesta del Área de Empleado Público respondiera al carácter voluntario u obligatorio, si existen medios menos invasivos para el mismo fin, cuál es esta finalidad, quién custodia los datos y nivel de protección de datos tan vulnerables."

A continuación la reclamante invoca una serie de preceptos jurídicos de la normativa de protección de datos y de resoluciones de la AEPD que considera aplicables en defensa de su derecho.

Seguidamente prosigue argumentando lo siguiente:

"-Que la respuesta del Área de Empleado Público es del todo insatisfactoria para la que suscribe puesto que considera que:

. El acceso mediante tarjeta no requiere contacto físico. Ya que además de ser compatible con el nuevo sistema, sirve de justificación a la empresa para el uso de un sistema tan invasivo.

. Que ninguna trabajadora o trabajador ha sido informado ni tiene constancia de que su temperatura se registre mediante este sistema, lo cual, como argumento, me sigue pareciendo más contrario a la protección de datos que justificación

.Que la empresa aduce que está en pruebas ya que se ha instaurado antes de realizar una evaluación de impacto. No entiende la que suscribe como se puede "jugar a hacer pruebas" con los datos biométricos de las empleadas y empleados de la empresa.

- Que solicité la limitación de mis datos y la empresa no me responde en ningún sentido sobre qué ha hecho exactamente con ellos.
Entendiendo que el uso de datos biométricos es desproporcionado en la Diputación de Sevilla y que, en todo caso, esta empresa no ha procedido de forma adecuada ni en la recopilación, ni en la información ni en la recopilación de consentimiento ni en la evaluación de estos datos,

SOLICITA

La intervención de la Agencia Andaluza de Protección de Datos para ver la procedencia y legitimidad de este sistema de control de presencia, así como, de serlo, sobre su forma de implantación en la empresa Diputación de Sevilla y si es o no legítimo el uso se este sistema por el Área de Empleo Público y si ha de prevalecer sobre los derechos a la protección de datos de la interesada y resto de trabajadoras y trabajadores de esta Corporación."

A dicho escrito se acompañaban :
1- Escrito de la reclamante dirigido al Delegado de Protección de Datos de la Diputación de Sevilla solicitando limitación de datos barométricos , de fecha 10 de febrero de 2022.
2- Escrito de respuesta de la Diputación de Sevilla, de fecha 9 de marzo de 2022.

Segundo. Traslado previo al Delegado de Protección de Datos (DPD). Arts. 37.1 y 65.4 LOPDGDD.

1. En virtud de los artículos 37 y 65 LOPDGDD, con fecha 4 de abril de 2022 se dio traslado de la reclamación al Delegado de Protección de Datos de la Diputación de Sevilla para que, en el plazo máximo de un mes, nos informase en relación con las circunstancias expuestas en la misma así como de las medidas que se hayan podido adoptar tanto en relación con lo expresado en la reclamación como, en su caso, para que no se produzcan situaciones similares en el futuro. Igualmente se indicaba que en su respuesta al Consejo debía indicar además la identidad del órgano responsable del tratamiento objeto de reclamación, así como la denominación de dicho tratamiento en el correspondiente Registro de Actividades de Tratamiento.

2. En respuesta a dicho requerimiento, con fecha 3 de mayo de 2022, tuvo entrada un Informe de la DPD de la Diputación en el que se indica:

"(...)Recibida el pasado día 4 de abril la reclamaci6n RCO-.2022/046, y dada la materia de la reclamación, se remite al Área de Empleado Publico para que informe sobre la misma.
El día 29 de abril siguiente remite, el Área identificada, informe en el asunto que se incorpora en todos sus términos a este escrito[URL de verificación], ademas remiten la ficha del Registro de Actividades de Tratamiento[URL de verificaci6n_]que se acompaña al informe que se remite.-
Indicar ademas, que en fecha 9 de febrero se presenta escrito de una trabajadora dirigido a esta delegada. No obstante ello, del suplico del mismo se desprendía que la empleada estaba ejercitando sus derechos en materia de protección de datos, el escrito terminaba solicitando " ...Que se proceda a la limitación de los datos biométricos ...", " Que se considere del todo insuficiente la respuesta del Área de Empleado Publico..." "... que se proceda al bloqueo de los datos ...".
El escrito fue remitido al Área de Empleado Publico emitiendo informe que fue comunicado a la interesada.".

A dicho informe se acompaña Informe del Servicio de personal, de fecha 29 de abril de 2022, indicando:

"Con carácter previo, se ha de hacer referencia a la actuación que tuvo ese Consejo el pasado día 20 de enero, procedimiento *[nnnnn]* , en el mismo se requería a esta Diputación, información sobre de la utilización por parte de la Diputación Provincial de Sevilla de tornos de acceso para el personal con terminales biométricos de reconocimiento facial y sensores de temperatura."

Por otra parte, conviene señalar que una empleada de la Diputación, presentó, el pasado *[dd/mm/aa]* escrito en el que, tras hacer una serie de alegaciones, solicitaba lo siguiente:

"Que se proceda a la limitación de los datos biométricos tomados de forma no voluntaria, sin información sobre la finalidad, si existen medios menos invasivos y con menor riesgo de vulnerabilidad para obtener dichos fines, sobre quién custodia estos datos y los derechos a limitación o supresión de los mismos.
Que se considere del todo insuficiente la respuesta del Área de Empleado Publico a los representantes de las trabajadores y trabajadores y que no responden a ningunas de las cuestiones planteadas en el punto anterior y exigibles legalmente.
Que, de no atenderse la solicitud anterior, se proceda al bloqueo de los datos previa a la comunicación de los hechos a la Agencia Andaluza de Protección de Datos y en cumplimiento del art.52 de la LOPDGDD relativo al Deber de Colaboración."

Ese escrito fue contestado por parte de la Diputación de Sevilla a través del informe que se adjunta a este escrito.

A pesar de ello, se ha recibido el pasado 4 de marzo, la reclamación RCO-2022/046, en la que expresamente se deja constancia de los apartado 4A y 4B, sobre el ejercicio de los derechos y en el apartado 5 describe la reclamación, aportando ademas escrito. Ese apartado 5 es del siguiente tenor:

"La diputación de Sevilla, concretamente el área de Empleado Publico, implementó maquinas de acceso biométricos (mediante reconocimiento facial y de palma de la mano) sin previa información sobre su uso y derechos a su personal
Tras solicitar información sobre lo proporcionado de este método a la delegada de protección de datos, se me facilita respuesta del responsable de esta implementación, el área de Empleado Publico.
Se me responde con argumentos que, a mi parecer, no solo no justifica sino que agrava este uso desproporcionado (Datos biométricos) para el control del personal: Es una prueba, la evaluación de impacto se hace con posterioridad, se aduce que no precisa contacto mientras que el pique con tarjeta tampoco, se dice que se esta recogiendo la temperatura del personal (dato totalmente desconocido por la mayoría de los trabajadores/as).
Se desconoce si tras su petición la empresa a procedido a la limitación, supresión o que ha hecho con los datos de la persona que suscribe esta reclamación.

Dado que mantengo mis dudas sobre la legitimidad y proporción de la toma y uso de datos biométricos para el control de asistencia de los empleados y empleadas, a la falta de información ofrecida a estos/as sobre sus derechos y a la falta de una evaluación de impacto previa solicito la intervención de este Consejo para que se informe si es legitimo el uso de datos biométricos por considerarlo innecesario e invasivo frente a otros métodos de control y si ha de prevalecer sobre los derechos de protección de datos de sus empleadas y empleados y se proceda a la toma de las medidas que correspondan."

Por otra parte, el escrito que adjunta termina solicitando lo siguiente:

"La intervención.., para ver la procedencia y legitimidad de este sistema de control ...sobre su forma de implementación.., y si es o no legitimo el uso de este sistema por el Área de Empelado Público y si ha de prevalecer sobre los derechos de la protección de datos de la interesada y resto..."

En virtud de lo que antecede, se INFORMA por el Servicio de Personal lo siguiente:

PRIMERO. Con fecha de 2 de agosto de 2021 se aprueba la Resolución n.° *[nnnnn]* para la contratación del "Suministro e instalación de tornos de acceso con terminales faciales con palma de la mano y con sensor de temperatura para la Diputación de Sevilla", siendo firmado el contrato el *[dd/mm/aa]* con la adjudicataria [Nombre empresa proveedora].
Dicho contrato tiene su razón de ser en la necesidad y mejora en la aplicación y control de la prestación del tiempo de trabajo del personal empleado de la Diputación Provincial de Sevilla, a la vista de los artículos 21 y 36 de los vigentes Acuerdos de Funcionarios y Convenio Colectivo del Personal Laboral, afectando al personal que presta servicios profesionales en la Corporación Provincial y cuya coordinación es llevada a cabo por la Unidad de Control de Presencia adscrita al Servicio de Personal del Área del Empleado Público de la misma.
La situación de crisis sanitaria ocasionada por la pandemia actualmente en curso derivada de la enfermedad causada por el virus SARS CoV-2 (Covid-19) y sus consiguientes cepas evidencian, aun hoy, una incertidumbre en cuanto a su duración, generando en consecuencia, la toma de una serie de precauciones entre las que se encuentra evitar, en la medida de lo posible, el contacto cercano interpersonal, así como eludir las superficies, en particular las que se tocan con regularidad por distintos usuarios, sustituyendo los medios de acceso hasta ahora utilizados por otros que ayuden a impedir la propagación del virus y sus rebrotes, como así se desprende de la Memoria justificativa del contrato para el suministro e instalación de "Tornos de acceso con terminales faciales con palma de la mano con sensor de temperatura" para la Diputación de Sevilla.
Asimismo, la transformación digital es ya una realidad en la Administración pública y la aplicación de las nuevas tecnologías por parte de la Corporación, tiene como principal consecuencia un notable aumento de la calidad del servicio tanto a los ciudadanos como al personal empleado en la misma, así como una mejora de la seguridad en el control de acceso y salidas y la asunción de un riesgo mínimo para todos.
SEGUNDO. En relación a la fundamentación para el tratamiento de los datos, debemos destacar las letras c) y b) del apartado 1 del articulo 6 del RGPD, que disponen que "El tratamiento sera licito si se cumple al menos una de las siguientes condiciones: (...) c) el tratamiento es necesario

para el cumplimiento de una obligación legal aplicable al responsable del tratamiento y b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales (..)". En su virtud, el tratamiento seria licito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral.

Por otra parte, el considerando 51 del mismo RGPD, en la medida en que los datos biométricos son de categoría especial en los supuestos de identificación biométrica (art. 9.1 RGPD), sera necesario que concurra,-ademas de una de las bases legitimadoras establecidas en el articulo 6 del RGPD-, alguna de las excepciones previstas en el articulo 9.2 del RGPD, que permitirían levantar la prohibición general del tratamiento de estos tipos de datos establecida en el articulo 9.1.

En este sentido, conviene mencionar la letra b) del articulo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no sera de aplicación cuando "el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Union de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado", encontrando justificación en el articulo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores.

TERCERO. El nuevo sistema de tornos de acceso con terminales faciales con palma de la mano, sin contacto, y con cámara térmica para determinación de la temperatura de manera previa a su-entrada, implantados en la Diputación de Sevilla, consta del mismo software para el tratamiento de datos que la Unidad de Control de Presencia ha venido utilizando desde mucho antes de la puesta en marcha de los nuevos lectores, de tal modo que no se ha procedido a la compra de una nueva licencia para su explotación.

En este sentido, el almacenamiento y tratamiento de datos biométricos, como huella, palma, facial, etc, es el que reside y se lleva aplicando desde la instalación de sistema NET en el año 2002. Esta información se guarda encriptada y se envía a los terminales, no pudiéndose tener acceso a ella debido a que los servidores en los que se almacenan los datos de acceso son propiedad de la Diputación de Sevilla y están ubicados en sus propias instalaciones, contando con todas las garantías de seguridad.

A mayor abundamiento y, reproduciendo el tenor literal de informe emitido por la Gerencia de INPRO (Sociedad Provincial de Informática de Sevilla, S.A.U.) de fecha 1 de febrero de 2022:

"La tecnología biométrica de la que disponen los terminales tiene un método de lectura que es mediante una cámara ubicada en el terminal. El sensor no guarda datos biométricos sino que recoge distintos puntos de la cara o palma (convergencias, desviaciones, empalmes, interrupciones, fragmentos, islote, bifurcación, punto, cortada, horquilla, encierro...). Una vez recogidos los distintos puntos y, en función de los parámetros establecidos por el fabricante, se crea una secuencia alfanumérica y esa secuencia se encripta mediante un algoritmo. Esto da lugar a una secuencia alfanumérica encriptada. El terminal no escanea la cara ni la palma por lo que de una cara o palma se obtiene una clave alfanumérica encriptada. El proceso es irreversible, de esa clave no se puede obtener la cara o palma.

No se producen tratamiento de datos personales por parte de la empresa adjudicataria, y los servidores donde se almacenan los datos están ubicados en la Diputaci6én de Sevilla y bajo los controles de seguridad de la Red corporativa.
El lector base situado en las dependencias del departamento de Control de Presencia del Área del Empleado Publico tiene precargado los datos de DNI y Nombre del empleado del tratamiento de datos ya declarado y publicado en la sección http:·.... cumpliendo con la normativa actual. En dicho lector base, a dichos datos se le asocia una clave alfanumérica encriptada que en ningún caso recoge ninguna característica física del empleado publico, estando dicho terminal inaccesible a cualquier servicio, aplicacid6n o sistema diferente de los terminales de control de acceso."
CUARTO. Desde la instalación, con carácter provisional, el 18 de octubre de 2021, del nuevo sistema de tornos de acceso, se esta llevando a cabo un periodo de prueba de dicho sistema de acceso coexistente con el sistema anterior, siendo el uso de ambos perfectamente compatibles, hasta el extremo de que no todo el personal empleado en la Corporación esta haciendo uso del nuevo sistema, dado que parte del mismo aún no se ha sometido al reconocimiento facial o de la palma de la mano previo.
En este sentido, durante dicho periodo de prueba se está procediendo al estudio de las incidencias que se van sucediendo, por lo que no se implantara el nuevo sistema de manera definitiva en tanto en cuanto no estén resueltas dichas incidencias.
No obstante lo anterior, se ha procedido a la actualización de las Fichas de Registro de Actividades de Tratamiento del personal funcionario y del personal de vigilancia, video-vigilancia y control de acceso a las instalaciones corporativas, así como a la modificación e indicación de la URL en la que se puede consultar la inclusión en el Inventario de Actividades de Tratamiento.
A este respecto, ya con anterioridad se informé al respecto, por un lado a la Junta de Personal y Comité de Empresa de la Diputación de Sevilla, y asimismo al conjunto de la parte social en Mesa de Coordinación con la representación Corporativa del Área del Empleado Público. En el mismo sentido, también se emitieron dos comunicados dirigidos al personal empleado de la Corporación, si bien, se publicó otro anuncio a comienzos del mes de febrero con el siguiente tenor literal:

"En relación a la implantación del nuevo sistema de control de acceso a las instalaciones de la Corporación, se informa que dicho proceso continua en fase de prueba, pudiéndose acceder mediante el reconocimiento facial o el uso de la tarjeta para evitar incidencias. En este sentido, queremos destacar la colaboración voluntaria prestada por los empleados/as para la recogida de los datos biométricos, señalando, que en cumplimiento de la normativa existente en la materia, se están guardando todos los requerimientos exigidos en lo que a su tratamiento y a seguridad se refiere, en este sentido se esta elaborando un informe de evaluación de impacto en la protección de datos, que garantice el proceso de implantación del nuevo sistema.
Por ultimo, les indicamos que pueden comunicar sus incidencias durante esta fase de prueba y obtener mas información sobre el registro de datos y el procedimiento de ejercicio de derechos, en el siguiente enlace:
https://www.dipusevilla.es....
Se informará con carácter previo al personal y a la parte social la fecha de implantación del nuevo sistema."
A mayor abundamiento y, al hilo de lo anteriormente expuesto, se esta en proceso de tramitación la elaboración del informe de evaluación de impacto en la protección de datos (EIPD), tal y como requiere la normativa reguladora en esta materia. En dicho informe se esta llevando a cabo un

exhaustivo análisis de los riesgos que el nuevo sistema de información puede suponer para el derecho a la protección de datos del personal empleado cuyos datos se tratan.

A consecuencia de dicha elaboración, desde el Área del Empleado Publico se ha procedido, con fecha de 13 de abril del corriente, a remitir oficio a la gerencia de la sociedad provincial de informática de Sevilla, solicitándole informe con el fin de proceder a la finalización de la EIPD mediante la cumplimentación de la información de la que se carece desde este área.

A tal efecto, una vez recibido el informe y, como resultado del análisis llevado a cabo en la confección del EIPD, del que se dará traslado a la parte social, se procederá a la gestión de dichos riesgos mediante la adopción de las medidas necesarias para eliminar o atenuar en lo posible aquellos que se identifiquen, antes de la implantación definitiva del nuevo sistema acceso con terminales faciales con palma de la mano y con sensor de temperatura.

QUINTO. En referencia a lo manifestado en la reclamación remitida por el Consejo de Transparencia y Protección de Datos sobre que el acceso mediante tarjeta no requiere contacto físico, es del todo incierto, dado que, para acceder o salir del edificio, la tarjeta se pasa por una maquina por la que transitan las tarjetas de los demás empleados, entrando posteriormente en contacto con las manos del usuario de la misma.

SEXTO. Por lo que se refiere a la solicitud de limitación del tratamiento, dicha materia se regula en el art. 18.1 del RGPD, que dispone:

"1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;

b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;

d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

2. Cuando el tratamiento de datos personales se haya limitado en virtud del apartado 1, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés publico importante de la Union o de un determinado Estado miembro.

3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación."

De esos apartados, entendemos que ninguno se ajusta a la situación que aquí se plantea, dado que los datos obtenidos son exactos, son para un tratamiento licito, el responsable los necesita para la finalidad del tratamiento y el motivo por lo que los ha de tener el responsable es legitimo.

Esto se ha de hacer extensivo a la solicitud de supresión de los datos [art. 17 del RGPD], a la que también alude en el escrito, en la medida que solo procedería en caso de que el tratamiento fuera ilícito cuestión que entendemos que no se da en este supuesto.

SÉPTIMO. Por Ultimo, respecto de los datos solicitados por el Consejo de Transparencia y Protección de Datos sobre la identidad del Órgano responsable del tratamiento objeto de la

reclamación, así como la denominación de dicho tratamiento en el correspondiente Registro de Actividades de Tratamiento, se informa que el Órgano responsable es la Diputación de Sevilla, siendo la denominación del tratamiento: "Servicio de Personal". (Se adjunta anexada a este informe Ficha de Registro de Actividades de Tratamiento.)

En relación a lo expuesto, cabe CONCLUIR que el nuevo sistema de identificación se encuentra en la actualidad en fase de prueba, coexistiendo con el anterior y pudiendo usarse uno u otro según voluntad del personal. Asimismo, con carácter previo a su implantación definitiva, se esta realizando un informe de evaluación de impacto de protección de datos, tal y como requiere la normativa reguladora de esta materia, y se procederá a dar previo traslado a la parte social y al conjunto del los empleados públicos. Por Ultimo, tal y como se anunció al personal mediante comunicado en el portal, éste, ademas de tener la facultad de comunicar las incidencias que pudieran surgir durante la fase actual de prueba, puede obtener mas información sobre el registro de datos y el procedimiento de ejercicio de derechos mediante enlace telemático habilitado al efecto.".

A dicho escrito acompaña:
-Copia del Registro de actividades de Tratamiento "Servicio de personal".
-Informe del Servicio de Personal sobre solicitud en materia de protección de datos, de fecha 9 de marzo de 2022.

3. En relación con el expediente *[nnnnn]* abierto por el Consejo, al que se refiere el órgano reclamado, el mismo tuvo lugar con anterioridad a la presentación de la reclamación, en el marco de una actuación informativa relacionada con los hechos que posteriormente se denuncian en la reclamación que da origen al presente procedimiento. Siendo así, los argumentos e informes aportados por la entidad reclamada en dicha actuación informativa se incorporan al expediente de esta reclamación y constan en la descripción de los hechos y consideraciones jurídicas de este Acuerdo.

Tercero. Admisión a trámite de la reclamación y apertura de Actuaciones Previas de Investigación (arts. 65.5 y 67.1 LOPDGDD; Art.55.2 LPAC).

Con fecha 10 de octubre de 2022, el Director del Consejo de Transparencia y Protección de Datos de Andalucía, acordó la admisión a trámite de la reclamación presentada y, al mismo tiempo, también la iniciación de oficio de actuaciones previas de investigación, a fin de lograr una mejor determinación de los hechos y circunstancias que justificasen la tramitación, en su caso, de un procedimiento por infracción de la normativa de protección de datos personales.

Cuarto. Sobre las Actuaciones Previas de Investigación.

1. En el marco de dichas actuaciones y con el objeto de completar la información relacionada con los hechos denunciados, el 14 de octubre de 2022, desde el Consejo se requirió al DPD para que remitiera información y documentación sobre las actuaciones llevadas a cabo en relación con la reclamación; en particular, se solicitaba, entre otra documentación:

"(...)

1.- Copia del documento donde se recoja la Evaluación de impacto relativa a la protección de datos (EIPD) realizado o, en su defecto, informe sobre la elaboración de la misma.

2.- Resultado del análisis de riesgo efectuado al nuevo sistema de información (incluido estudio de la proporcionalidad del tratamiento objeto de la reclamación) y, en su caso, medidas adoptadas como consecuencia del mismo, anteriores a su implantación definitiva.
3.- Copia de la cláusula de información o documentación en virtud de la cual se informa a los interesados de la instalación del sistema de acceso mediante el uso de datos biométricos y del tratamiento de sus datos personales [artículos 13 RGPD].
4.- Copia de la información proporcionada a las personas afectadas sobre la voluntariedad de la utilización del sistema mencionado y las alternativas existentes al mismo.
5.- Copia de los comunicados dirigidos al personal sobre la implantación del nuevo sistema,a los que se hace referencia en el Informe del Director del Área de Empleado Público así como indicación de la fecha e información completa del comunicado dirigido al personal y publicado por el Área del empleado Público.
6.- Justificación de las distintas finalidades en relación con los datos biométricos que pueden obtenerse (datos faciales, datos sobre temperatura corporal, otros), y base que legitima el tratamiento en cada caso. En su caso, referencia a esta información en el análisis de riesgo o evaluación de impacto realizadas.".

2. En respuesta a dicha solicitud, con fecha 14 de noviembre de 2022, tiene entrada escrito del DPD del órgano reclamado aportando Informe del Área del Empleado Público. Concretamente se indica:

> "(...)
> PRIMERO. Con fecha de 2 de agosto de 2021 se aprueba la Resolución n.° *[nnnnn]* para la contratación del Suministro e instalación de tornos de acceso con terminales faciales con palma de la mano y con sensor de temperatura para la Diputación de Sevilla", siendo firmado el contrato el *[dd/mm/aa]* con la adjudicataria [Nombre de empresa proveedora].
> SEGUNDO. El control de acceso a las instalaciones de la Diputación Provincial de Sevilla para la prestación del tiempo de trabajo ha ido sufriendo una evolución/ desde una entrada mediante tarjeta con chip, hasta un acceso utilizando tarjeta de proximidad o, mediante la alternancia, en la actualidad, de esta última tarjeta con el acceso a través del uso de datos biométricos.
> TERCERO. El control de presencia basado en datos biométricos fue implantado de manera provisional en la Diputación Provincial de Sevilla el 9 de diciembre de 2021, de forma simultánea y alternativa, a voluntad del personal empleado, con el sistema de control por medio de lector de tarjeta, siendo intención proceder a su implantación definitiva y exclusiva a partir del 1 de marzo de 2023.
> CUARTO. Con fecha de 4 de abril de 2022, se recibió por parte del Consejo de Transparencia y Protección de Datos de Andalucía petición de antecedentes e informe sobre la Reclamación N.° RCO-2O 22/046, con el fin de dar respuesta a una reclamación recibida por una presunta vulneración de la normativa de protección de datos personales/ siéndole enviado lo solicitado con fecha de 29 de abril.
> En virtud de lo que antecede, se INFORMA por el Servicio de Personal lo siguiente:
> PRIMERO. Dicho contrato tiene su razón de ser en la necesidad y mejora en la aplicación y control de la prestación del tiempo de trabajo del personal empleado de la Diputación Provincial de Sevilla, a la vista de los artículos 21 y 36 de los vigentes Acuerdos de Funcionarios y Convenio Colectivo del Personal Laboral, así como en aplicación del Real Decreto Legislativo 5/2015, de 30 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto Básico del Empleado

Público y del Real Decreto 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores/ afectando al personal que presta servicios profesionales en la Corporación Provincial y cuya coordinación es llevada a cabo por la Unidad de Control de Presencia adscrita al Servicio de Personal del Área del Empleado Público de la misma.

Si bien, como ya se expuso desde este Área en informe remitido con fecha de 10 de febrero del año en curso, la situación de crisis sanitaria ocasionada por la pandemia derivada de la enfermedad causada por el virus SARS-CoV-2 (Covid"19) y sus consiguientes cepas, generó extremar las precauciones en cuanto a evitar, en la medida de lo posible/ el contacto cercano interpersonal y las superficies que son tocadas con alta frecuencia por los distintos usuarios y, por ende, sustituir los medios de acceso hasta ahora utilizados en la Corporación, no se debe obviar,como también se manifestó en el informe mencionado que la aplicación de las nuevas tecnologías por parte de la Corporación, tiene como principal consecuencia un notable aumento de la calidad del servicio tanto a los ciudadanos como al personal empleado en la misma, así como una mejora de la seguridad en el control de acceso y salidas y la asunción de un riesgo mínimo para todos.

SEGUNDO. La base legitimadora del tratamiento radica en el "'cumplimiento de una misión realizada (...) en el ejercicio de poderes públicos conferidos al responsable del tratamiento" (Artículo 6.1. f) RGPD), así como en que "el tratamiento es necesario para el cumplimiento cíe una obligación legal aplicable al responsable del tratamiento" (Artículo 6.1. c) RGPD). En base a ello, el tratamiento seria licito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral.

Asimismo, el uso de datos biométricos, al ser catalogados como "especiales", tiene como consecuencia que, aunque en un principio debería considerarse la prohibición de su tratamiento según lo dispuesto en el articulo 9.1 RGPD, la letra b) del apartado 2 del mencionado articulo 9 autoriza dicho tratamiento en la medida que" *(...) es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado",* en la medida que existen normas convencionales (Convenio Colectivo para el Personal Laboral y Acuerdo para el Personal Funcionario) con arreglo a derecho en la Diputación Provincial de Sevilla en aplicación del articulo 20 del Texto refundido del Estatuto de los trabajadores (TE)/ aprobado por el Real decreto legislativo 2/2015, de 23 de octubre/ el cual prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores.

TERCERO. En la implantación, hasta ahora provisional, de los tornos de acceso con terminales faciales con palma de la mano y con sensor de temperatura en la Diputación Provincial de Sevilla, se han llevado a cabo las medidas técnicas y organizativas apropiadas, tal y como se establece en el apartado B del Anexo X de la Guía de protección de datos por defecto elaborada por la Agencia española de protección de datos, como la minimización de datos, de tal manera que se proporcionan las garantías necesarias en el tratamiento/ a fin de cumplir los requisitos del Reglamento y proteger los derechos del personal empleado en la Corporación. Tales medidas garantizan en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.

Al hilo de lo anteriormente expuesto, como así se manifestaba en los informes de INPRO y de la empresa adjudicataria [Nombre de empresa proveedora], el almacenamiento de datos biométricos, como huella, palma/ facial, etc, trata una información que se guarda encriptada y se envía a los terminales, no pudiéndose tener acceso a ella debido a que los servidores en los que se almacenan los datos de acceso son propiedad de la Diputación Provincial de Sevilla y están ubicados en sus propias instalaciones, contando con todas las garantías de seguridad.

Las medidas técnicas y organizativas dan cumplimiento, pues, a lo establecido en el articulo 25 del RGPD en tanto en cuanto la tecnología biométrica de la que disponen los terminales tiene un método de lectura que es mediante una cámara ubicada en el terminal. Como ya se manifestó en el informe emitido por la Gerencia de INPRO (Sociedad Provincial de Informática de Sevilla/ S.A.U.) de fecha 1 de febrero de 2022, el sensor no guarda datos biométricos sino que recoge distintos puntos de la cara o palma (convergencias, desviaciones, empalmes, interrupciones, fragmentos, islote/ bifurcación/ punto/ cortada, horquilla/ encierro...). Una vez recogidos los distintos puntos y, en función de los parámetros establecidos por el fabricante/ se crea una secuencia alfanumérica y esa secuencia se encripta mediante un algoritmo. Esto da lugar a una secuencia alfanumérica encriptada. El terminal no escanea la cara ni la palma por lo que de una cara o palma se obtiene una clave alfanumérica encriptada. El proceso es irreversible, de esa clave no se puede obtener la cara o palma.

A mayor abundamiento, no se producen tratamiento de datos personales por parte de la empresa adjudicataria, y los servidores donde se almacenan los datos están ubicados en la Diputación de Sevilla y bajo los controles de seguridad de la Red corporativa. El lector base situado en las dependencias del departamento de Control de Presencia del Área del Empleado Público tiene precargado los datos de DNI y Nombre del empleado del tratamiento de datos ya declarado y publicado en la el Registro de Actividades de Tratamiento de la Diputación/ cumpliendo con la normativa actual. En dicho lector base, a dichos datos se le asocia una clave alfanumérica encriptada que en ningún caso recoge ninguna característica física del empleado público, estando dicho terminal inaccesible a cualquier servicio, aplicación o sistema diferente de los terminales de control de acceso, como así quedó avalado en los informes remitidos y ya mencionados, tanto por INPRO como por la empresa adjudicataria.

CUARTO. Durante este período provisional de adaptación al nuevo sistema de acceso en la Diputación Provincial de Sevilla, se ha procedido a la actualización de las Fichas de Registro de Actividades de Tratamiento, a la modificación e indicación de la URL en la que se puede consultar la inclusión en el Inventario de Actividades de Tratamiento y a la emisión de varios comunicados dirigidos al personal empleado de la Corporación.

Asimismo, se ha llevado a cabo la elaboración del informe de evaluación de impacto en la protección de datos (EIPD), tal y como requiere la normativa reguladora en esta materia. Para dicha elaboración, han tenido lugar diversas reuniones entre el Servicio de Personal del Área del Empleado Público y la Delegada de Protección de Datos de la Corporación, así como con la gerencia de la sociedad provincial de informática de Sevilla, en pro de un adecuado y exhaustivo análisis de riesgo que dieran forma y contenido a la EIPD, antes de la implantación definitiva del nuevo sistema acceso con terminales faciales con palma de la mano y con sensor de temperatura, información ésta que será objeto de una nueva comunicación a la parte social y al conjunto del personal empleado público.

QUINTO. Respecto a la información/documentación requerida en relación a la reclamación remitida desde el Consejo de Transparencia y Protección de Datos de Andalucía-Sevilla con N.° RCO-2022/046/ se manifiesta lo siguiente:

1 y 2.- Se adjunta copia del documento donde se recoge la Evaluación de impacto relativa a la protección de datos (EIPD) realizado con el resultado del análisis de riesgo efectuado al nuevo sistema de información (incluido estudio de la proporcionalidad del tratamiento objeto de la reclamación) y, en su caso/ medidas adoptadas como consecuencia del mismo/ anteriores a su implantación definitiva.

3. - En cuanto a la remisión de copia de la cláusula de información o documentación en virtud de la cual se informa a los interesados de la instalación del sistema de acceso mediante el uso de datos biométricos y del tratamiento de sus datos personales [articulas 13 RGPD]/ se ha de entender las comunicaciones llevadas a cabo con fechas de *[dd/mm/aa]* transmitiéndose la misma, además de manera personal e individualizada, en el momento de la toma de la fotografía para incorporarla al lector base situado en las dependencias del departamento de Control de Presencia del Área del Empleado Público, el cual tiene precargado los datos de DNI y Nombre del empleado del tratamiento de datos ya declarado y publicado en la ficha de Registro de Actividades de Tratamiento de la Diputación/ cumpliendo con la normativa actual. Como se ha manifestado anteriormente, en dicho lector base, se asocia a los datos una clave alfanumérica encriptada que en ningún caso recoge ninguna característica física del empleado público, estando dicho terminal inaccesible a cualquier servicio, aplicación o sistema diferente de los terminales de control de acceso.

4.- Respecto a la copia de la información proporcionada a las personas afectadas sobre la voluntariedad de la utilización del sistema mencionado y las alternativas existentes al mismo, si bien es cierto que el control de presencia basado en datos biométricos ha sido implantado de manera provisional en la Corporación, en plena alternancia, a voluntad del personal empleado, con el sistema de control por medio de lector de tarjeta, su implantación definitiva/ prevista para el 1 de marzo de 2023, goza de una legitimidad normativa en cuanto al tratamiento de los datos, como así ha quedado expuesto en el punto segundo del presente informe.

5.- Las copias de los comunicados dirigidos al personal sobre la implantación del nuevo sistema, a los que se hace referencia en el Informe del Director del Área de Empleado Público así como indicación de la fecha e información completa del comunicado dirigido al personal y publicado por el Área del empleado Público, fueron remitidas al Consejo de Transparencia y Protección de Datos con fecha de 10 de febrero de 2022, siendo el número de registro de salida el *[nnnnn]*

6.- Justificación de las distintas finalidades en relación con los datos que pueden obtenerse (datos fáciles, datos sobre temperatura corporal, otros), base que legitima el tratamiento en cada caso. En su caso, referencia a esta información en el análisis de riesgo o evaluación de impacto realizadas. Respecto a esta cuestión, el nuevo sistema de acceso con terminales faciales con palma de la mano y con sensor de temperatura para la Diputación de Sevilla, tiene como una finalidad la necesidad y mejora en la aplicación y control de la prestación del tiempo de trabajo, afectando exclusivamente al personal que presta servicios profesionales en la Corporación Provincial y cuya coordinación es llevada a cabo por la Unidad de Control de Presencia adscrita al Servicio de Personal del Área del Empleado Público de la misma. Dicho tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autoriza un convenio colectivo con arreglo a Derecho y que

dispone de las garantías adecuadas del respeto de los derechos fundamentales y de los intereses del personal empleado en la Corporación .

En base a lo anteriormente expuesto/ CABE CONCLUIR/ respecto a los principios relativos al tratamiento, a la vista de los informes técnicos de INPRO y de *[nombre de empresa]*, así como de las múltiples reuniones con la Delegada de Protección de Datos, que, efectivamente los datos son exactos y actualizados, recogiéndose para fines determinados, explícito e implantándose las medidas de seguridad pertinentes para proteger la integridad y confidencialidad de los datos, contra el tratamiento no autorizado o ilícito de los mismos y para evitar su pérdida, destrucción o daño accidental. Asimismo, el tratamiento es licito a causa de su necesidad para el cumplimiento de interés público, no existiendo condiciones para el tratamiento tanto por dicha razón como en ejercicio de una potestad de la Administración. Por último, en cuanto a encontrarnos ante una categoría especial de datos, el tratamiento de los datos biométricos es exclusivamente el necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos en el ámbito del derecho laboral y de la seguridad y protección.

De igual modo, respecto a los derechos de los interesados recogidos en la Lista de Cumplimiento Normativo elaborada por la Agencia Española de Protección de Datos, se da cumplimiento a los mismos, disponiendo el personal empleado de la Diputación Provincial de Sevilla tanto de un sistema de información sobre el ejercicio de derechos en el Portal de Protección de Datos de la Corporación, como de un procedimiento reglado para dicho ejercicio en su Sede Electrónica. En el mismo sentido, y respecto a la notificación de brechas de la seguridad de los datos personales a la autoridad de control, así como la comunicación de brechas al interesado, existe un procedimiento a través de la Delegada de Protección de Datos, nombrada y en ejercicio en la Diputación Provincial de Sevilla.

En virtud de lo que antecede, desde la Diputación Provincial de Sevilla entendemos que se ha actuado conforme al ordenamiento jurídico, tanto en lo que respecta a la implantación de un sistema, por ahora provisional, para la adaptación paulatina y adecuada con todas las medidas de seguridad, como en la limitación hacia todo el personal empleado de los datos biométricos recogidos, siendo estos datos los mínimos y absolutamente necesarios para el acceso a las instalaciones ."

A dicho escrito se acompañaba:

-Informe de Evaluación de Impacto en la protección de la Diputación de Sevilla, firmado con fecha 14 de noviembre de 2022.

-Informe técnico expediente implantación del nuevo sistema de control de presencia, firmado con fecha 9 de febrero de 2022.

-Copia del Registro de actividades de Tratamiento (P4100000a) "Sistema de control de acceso de personal a las instalaciones de la Diputación basado en tornos de acceso con terminales receptoras de datos biométricos"

-Copia de del Registro de actividades de Tratamiento "Gestión "RED" (Red Interadministrativa Provincial de Comunicaciones de la Diputación de Sevilla) y Centro de Procesamiento de Datos corporativo (C,P.D.)"

-Informe de Evaluación de Riesgos, de fecha 11 de noviembre de 2022, en el cual figura nota de "Riesgo muy alto, es obligatoria una EIPD".

Con fecha 17 de noviembre de 2022, se remite por el DPD una corrección a la documentación anterior en relación con el Informe técnico implementación del nuevo sistema de control,

aportando comunicación , de fecha 17 de junio de 2022 y certificado de tipo de lectura biométrica del terminal, de fecha 20 de octubre de 2021.

3. Con fecha 23 de febrero de 2023 tiene entrada en este Consejo un nuevo escrito de la reclamante, solicitando que se adjuntara diversa documentación. Concretamente indicaba:

"(...) Que en el 9 de Febrero de 2022, presenté ante la delegada de protección de datos de la Diputación de Sevilla escrito en el que planteaba dudas sobre la legitimidad del uso de los datos biométricos de los trabajadores y trabajadoras por la Diputación de Sevilla como mecanismo de control de la presencia de los mismos, en referencia a los siguientes aspectos:
-La proporcionalidad de la tenencia por parte de la Empresa, su custodia y legitimidad para ello de los datos biométricos del personal.
- Ausencia de Informe de evaluación de impacto, análisis de riesgo o ficha en el registro de actividades de tratamiento.
- La ausencia en el personal de voluntariedad y desconocimiento de la finalidad en la recopilación de estos datos por parte de los trabajadores.
- Custodia y tratamiento de estos datos, persona responsable y garantías.
- Derechos y obligaciones que nos amparan ante la posesión de estos datos por parte de terceros.
- Petición de limitación y bloqueo de mis datos biométricos y traslado de esta petición al CTPDA sobre la procedencia del sistema.
- Que el pasado 16 de Febrero del corriente, se comunica a los trabajadores a través del Portal del Empleado lo siguiente:

[" COMUNICADO

ÁREA DE EMPLEADO PÚBLICO

Nuevo Sistema de Control de Acceso a las Instalaciones de la Corporación

En relación a la implantación del nuevo sistema de control de acceso a las instalaciones de la Corporación, se informa que dicho proceso se encuentra en fase de prueba desde el 9 de diciembre de 2021, como así se hizo saber en anteriores comunicados, de tal manera que se ha estado pudiendo acceder, de forma simultánea y alternativa, a voluntad del personal empleado, mediante el reconocimiento facial o el uso de la tarjeta con el fin, por un lado, de evitar incidencias y, por otro, de ir obteniendo y cargando los datos en los nuevos lectores de reconocimiento facial, guardando todos los requerimientos exigidos en lo que a su tratamiento y a seguridad se refiere, en cumplimiento de la normativa existente en la materia.
En este sentido, se procedió a la elaboración de un Informe de Evaluación de Impacto en la Protección de Datos de la Diputación de Sevilla, junto al análisis de riesgo, la incorporación de la ficha correspondiente en el Registro de Actividades de Tratamiento y la posibilidad del personal empleado en la Corporación de ejercitar sus derechos en la sede electrónica de la misma, e incluso a través del correo electrónico de la Delegada de Protección de Datos, de acuerdo con lo dispuesto en el Reglamento Europeo de Protección de Datos de Carácter Personal y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
En virtud de lo que antecede, el próximo ***1 de marzo de 2023*** *se procederá a la implantación definitiva del Sistema de Control de Acceso a las Instalaciones de la Diputación de Sevilla mediante reconocimiento facial y de la palma de la mano , dejando de ser operativo el acceso a través de los tornos con el uso de la tarjeta Por último, reiteramos la importancia de la colaboración voluntaria prestada por los*

empleados y empleadas para la recogida de los datos biométricos de aquellos que aún no lo hayan hecho, debiéndose personar en la Unidad de Control de Presencia con anterioridad a la citada fecha.
DIRECTOR GENERAL DEL ÁREA DE EMPLEADO PÚBLICO
[NOMBRE DEL DIRECTOR GENERAL DEL ÁREA DE EMPLEADO PÚBLICO]"

-Que se me adjunta contestación/ informe del Área de Empleado Público.
- Que no se ejecuta mi solicitud de limitación y bloqueo(o al menos no se me informa), desconociendo si se dio traslado a este Consejo y mis datos biométricos siguen activos en el sistema de control como he podido comprobar accidentalmente al pasar mi mano por el lector en una ocasión reciente.
-Que entiendo que mi derecho de limitación y bloqueo, pero manteniendo mis datos custodiados –que no operativos-, se comunicaría al Consejo de Transparencia y Protección de Datos de Andalucía en espera de una resolución que a mí no se me ha comunicado en la fecha.
- Que en ningún caso debe entenderse mi voluntad ni intención de que Diputación de Sevilla posea mis datos biométricos y, menos aún, sin información clara, concisa y por escrito de forma personalizada.
- Que no es hasta este escrito de la pasada semana donde aparece la existencia de Informe de Evaluación de Impacto en la Protección de Datos de la Diputación de Sevilla, análisis de riesgo, incorporación de la ficha correspondiente en el Registro de Actividades de Tratamiento y la posibilidad del personal empleado en la Corporación de ejercitar sus derechos en la sede electrónica de la misma, e incluso a través del correo electrónico de la Delegada de Protección de Datos. Vuelvo a señalar que yo los ejercí sin que se haya ejecutado mi derecho de oposición.
Que con fecha de 22 de febrero de 2023 reitero mi deseo de limitar y bloquear mis datos biométricos a la empresa Diputación de Sevilla, se me informe por qué no se ha ejecutado este derecho, si la delegada de protección de datos tramitó mi derecho al ejercicio de limitación y bloqueo al CTPDA y de ser así si hay resolución al respecto, se omita la palabra "voluntariedad" de los escritos referidos al tema mientras no se proporcionen consentimientos informados, se me indique ante mi oposición manifiesta y ejercida en tiempo y forma cómo puedo justificar mi presencia en la empresa a partir del próximo día 1 de marzo si se eliminan las alternativas al reconocimiento biométrico.
- Que igualmente, he solicitado que se me informe sobre si los datos se recogen con una aplicación de autenticación o identificación biométrica y las razones de seguridad que han motivado la elección.
- Que para acrecentar aún más la preocupación sobre los riesgos de seguridad sobre este tipo de datos tan sensibles, solo cinco días después de lanzar el comunicado anterior, el 21 de febrero de 2023, hacen el siguiente a través del mismo medio (portal del empleado público):
"Noticias Medidas URGENTES sobre cibera taques (*[dd/mm/aa]*)
[Correo electrónico advirtiendo de que se están produciendo cibera taques]

No debemos olvidar que Diputación de Sevilla cuenta con más de 1200 empleadas y empleados y que algunos de ellos acceden desde sus propios domicilios o lugares ajenos a la propia red de la empresa en la modalidad de teletrabajo o por las características de su trabajo itinerante.

SOLICITA:

-Se adjunte al expediente RCO-2022/046 el nuevo comunicado del Área de Empleado Público de la Diputación de Sevilla.
- Se adjunte nuevo escrito remitido por la que suscribe a la Delegada de protección de Datos de la Diputación de Sevilla.
- Se tenga por reiterado mi derecho de limitación y bloqueo, manifestando igualmente que se conserven en custodia para las pertinentes comprobaciones a las que pudiera dar lugar esta o futuras reclamaciones.".

A dicho escrito adjuntaba:
-Comunicado del Área de Empleado Público de la Diputación Provincial, referente a la implantación definitiva, a partir del día 1 de marzo de 2023,del Sistema de Control de Acceso a las Instalaciones de la Diputación de Sevilla, mediante reconocimiento facial y de la palma de la mano, dejando de ser operativo el acceso a través de los tornos con el uso de la tarjeta.
-Nuevo escrito de la reclamante a la DPD de la Diputación, de fecha 23 de febrero de 2023, en relación con su solicitud de ejercicio de derechos, de fecha 9 de febrero de 2022.

4. Como continuación de las actuaciones previas de investigación, desde este Consejo, con fecha 15 de marzo de 2023, se remite un requerimiento al DPD del órgano reclamado, para que aporte diversa documentación. Concretamente:

" (..)1- Estudio de la necesidad, proporcionalidad e idoneidad, en relación con cada uno de los tratamientos efectuados (relativo a datos faciales, palma de la mano y temperatura corporal), que ha servido de base para llegar a las conclusiones que aparecen en el apartado correspondiente del Informe de Evaluación de Impacto en la Protección de Datos aportado (apartado V, pág. 5 del mismo).
2- En relación con el apartado 3 de nuestro anterior requerimiento (*3.- Copia de la cláusula de información o documentación en virtud de la cual se informa a los interesados de la instalación del sistema de acceso mediante el uso de datos biométricos y del tratamiento de sus datos personales [artículos 13 RGPD]),* se observa que si bien se han remitido las comunicaciones informativas que se han realizado sobre la implantación del sistema, no consta la remisión de la cláusula de información o documentación por la que se informa sobre el tratamiento concreto que nos ocupa, en los términos previstos en el citado precepto.
Igualmente se le comunica que con fecha 23 de febrero de 2023, la reclamante ha presentado ante este Consejo nueva documentación, de la cual se le da traslado. Señala en la misma, entre otras cuestiones, que no se le ha dado respuesta a su solicitud de limitación y bloqueo de sus datos presentada en la Diputación Provincial con fecha 9 de febrero de 2022.
En relación con ello consta en el expediente su escrito, firmado el 3 de mayo de 2022, en el que se indica que el Área de de Empleado Público emitió informe al respecto que fue comunicado a la interesada. No obstante, analizado el Informe del Servicio de Personal que se acompaña a dicho escrito, firmado con fecha 9 de marzo de 2022, y que se entiende fue el remitido a la reclamante (Informe del Servicio de Personal sobre solicitud en materia de protección de datos), se comprueba que dicho informe no se pronuncia sobre la cuestión planteada relativa al ejercicio de derecho.
Por ello, se recuerda la obligación del responsable del tratamiento de responder a la solicitud de ejercicio de derecho de la reclamante, debiendo aportar a este Consejo, en el plazo anteriormente señalado, copia de la respuesta dada al mismo y acreditación de su remisión a la reclamante.".

5. Con fecha 30 de marzo de 2021, la reclamante presenta nueva documentación para su incorporación al expediente, consistente en respuesta a su ejercicio de derecho de fecha 9 de febrero de 2022 y contestación a la reiteración realizada en 2023.

6. Con fecha 4 de abril de 2023 tiene entrada escrito escrito de la DPD del órgano reclamado en respuesta a nuestro anterior requerimiento, conteniendo principalmente, el Informe del Área del Empleado Público de 3 de abril de 2023. Concretamente indica:

> "(..) En virtud de lo que antecede y, en contestación al requerimiento del CTPDA remitido por la Delegada de Protección de Datos de la Corporación, se INFORMA por el Servicio de Personal lo siguiente:
>
> PRIMERO.- Respecto al estudio de la necesidad, proporcionalidad e idoneidad, en relación con cada uno de los tratamientos efectuados (relativo a datos faciales, palma de la mano y temperatura corporal), que ha servido de base para llegar a las conclusiones que aparecen en el apartado correspondiente del Informe de Evaluación de Impacto en la Protección de Datos aportado (apartado V, pag. 5 del mismo).
> Diferentes fuentes han servido de base para la conclusiones que aparecen en el punto V del Estudio de Evaluación de Impacto en materia de protección de datos. Así, hemos de citar los informes que, en materia de protección de datos, han sido elaborados desde el Área de Empleado Publico y remitidos a ese Consejo. Estos son:
> 1.- Informe de 10 de febrero de 2022, remitido a ese Consejo en la misma fecha.
> 2.- Informe de 9 de marzo de 2022, remitido a ese Consejo en la misma fecha.
> 3.- Informe de 29 de abril de 2022, remitido a ese Consejo en fecha 3 de mayo de 2022.
> 4.- Informe de 14 de noviembre de 2022, remitido a ese Consejo en la misma fecha.
> Asimismo, se han elaborado diversos informes por la Sra. Gerente de INPRO. En concreto:
> 1.- Informe de 9 de febrero de 2022, remitido a ese Consejo en fecha 10 de febrero.
> 2.- Informe de 17 de junio de 2022, remitido a ese Consejo en fecha 16 de noviembre de 2022.
> Por ultimo, se ha de hacer referencia al propio documento de Evaluación de Impacto en la Protección de Datos de la Diputación de Sevilla, tanto con carácter general, como de manera particular en referencia a los siguientes epígrafes: "Sobre el tratamiento", incluido en el Resumen Ejecutivo; lo descrito en el epígrafe III "nombre y descripción del tratamiento", referido a Datos Básicos; y en el extenso apartado que recoge el "análisis de bases jurídicas del tratamiento y cumplimiento normativo".
> De todos estos informes se coligen de manera clara y precisa los elementos que han dado lugar al cuadro resumen que se ha plasmado en el estudio de Evaluación de Impacto, determinando el equipo de trabajo la suficiencia del contenido del mismo, y para no ser reiterativos, con lo ya expresado en los documentos descritos, entendiéndose que se cumple con lo preceptuado en el art. 35.7b) del RGPD.
> SEGUNDO.- Respecto a la no constancia de la remisión de la clausula de información o documentación por la que se informa sobre el tratamiento concreto que nos ocupa, en los términos previstos en el articulo 13 del RGPD.
> Durante el periodo provisional de adaptación al nuevo sistema de acceso en la Diputación Provincial de Sevilla, ademas de varios comunicados dirigidos al personal empleado en la

Diputación Provincial de Sevilla, y que se han mantenido en el Portal del Empleado Público, se procedió a la actualización de las Fichas de Registro de Actividades de Tratamiento, así como a la modificación e indicación de la URL en la que se puede consultar la inclusión en el Inventario de Actividades de Tratamiento.

En dichas Fichas se especifica con claridad diversas cuestiones en relación con el tratamiento de los datos, tanto para la Gestión "Red" y Centro de Procesamiento de Datos corporativo, como para el Sistema de control de acceso de personal a las instalaciones de la Diputación basado en tornos de acceso con terminales receptoras de datos biométricos. En concreto, se detalla el área funcional, la finalidad, legitimación y origen del tratamiento, así como las categorías de personas físicas afectadas por el mismo y los datos personales requeridos para ello. Asimismo, se concretan los plazos previstos para la supresión de datos personales requeridos para el tratamiento y destino posterior de estos, y las medidas de seguridad técnicas y organizativas.

Al hilo de lo anteriormente expuesto, al actualizar las Fichas de Registro de Actividades de Tratamiento, se procedió a precisar el ejercicio de los derechos e indicación de la URL, con el siguiente tenor literal:

"El ciudadano puede ejercer los derechos previstos en el Reglamento Europeo de Protección de Datos de Carácter Personal y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales en los siguientes canales:

. Delegada de Protección de Datos de la Diputación de Sevilla.

Avda. Menéndez Pelayo, 32, Sevilla, 41071, Teléfono.

« Sede electrónica de la Diputación de Sevilla.

* Consejo de Transparencia y Protección de Datos de Andalucía."

En virtud de lo que antecede, se considera altamente garantista el sistema de información sobre el ejercicio de derechos recogido en el Portal de Protección de Datos de la Corporación, así como el procedimiento reglado para dicho ejercicio en su Sede Electrónica.

TERCERO.- Respecto a la solicitud de limitación y bloqueo de sus datos personales presentada por la reclamante, se adjunta copia de la respuesta dada a la misma, con fecha de 30 de marzo de 2023 y del siguiente tenor literal:

"Habiéndose recibido escrito del Consejo de Transparencia y Protección de Datos de Andalucía. (CTPDA) en relación con su solicitud y, de acuerdo con lo dispuesto en el mismo, le comunico lo siguiente:

1° Nos reiteramos en el informe de fecha 9 de febrero de 2022 que le fue notificado, en el que claramente se le informaba del sistema que se iba a implantar para el control de acceso a los empleados, comunicándole ademas que en aquel momento tenia carácter provisional - punto cuarto del informe -.

2° Una vez recibida la contestación Vd. se dirigió al CTPDA y en respuesta al requerimiento efectuado por el Consejo, se le remitió informe de fecha 29 de abril de 2022, que se adjunta. En concreto, en el punto sexto del informe se trata la limitación de los datos, no pudiendo acceder a su pretensión por los motivos allí expuestos y, por ende, al bloqueo de sus datos.

3° A mayor abundamiento, y como ha tenido conocimiento a través de los comunicados de esta Dirección, publicados en el Portal del Empleado Publico, desde el pasado 1 de marzo, el sistema de acceso con datos biométricos ha pasado de ser provisional a adoptar carácter definitivo, al ser el único sistema de control de acceso del personal de la Diputación."

CUARTO.- Respecto a la nueva documentación incorporada al expediente por [Nombre de la reclamante], se ha de manifestar lo siguiente:

En fecha de 22 de febrero de 2023, se presenta escrito por la Sra. [Nombre de la reclamante], a la Delegada de Protección de Datos en el que reitera su solicitud de limitar y bloquear sus datos biométricos, remitiendo a su vez escrito al CTPDA con fecha de 23 de febrero de 2023.
Por lo que hace al escrito dirigido a la Delegada de Protección de Datos, fue contestado en fecha de 21 de febrero de 2023 y notificado al día siguiente.
Por lo que hace al escrito presentado al CTPDA, e incluido en el requerimiento del pasado 15 de marzo de 2023, se le informa que mediante oficio de 30 de marzo de 2023, notificado de manera telemática en la misma fecha, se desestima lo solicitado en fecha de 9 de febrero de 2022 sobre limitación y bloqueo de datos, dado que ninguno de los apartados del art. 18.1 del RGPD, se ajusta a la situación planteada por la Sra. [Nombre de la reclamante], debido a que los datos obtenidos son exactos, para un tratamiento licito, el responsable los necesita para la finalidad del tratamiento y el motivo por lo que los ha de tener el responsable es legitimo.
A mayor abundamiento, sobre la alegación referida al anuncio sobre ataques cibernéticos publicado en el Portal del Empleado Público, se le informa que dicho anuncio iba dirigido a la utilización, por parte del personal empleado en la Corporación, de los medios telemáticos,información sobre seguridad que no debería traspasar el entorno al que va dirigido. Asimismo, nos reiteramos en las medidas de seguridad del sistema de acceso a Diputación que se recogen en los informes emitidos por la Sra. Gerente de INPRO y que constan en el CTPDA, lo que se informa a ese Servicio de Transparencia, Protección de Datos y Registro Electrónico, a fin de dar cumplimiento a lo solicitado por el CTPDA.".

A dicho informe se acompaña:
1-Comunicación de 30 de marzo de 2023, dirigida a la reclamante y acreditación de su envío. En escrito se hace referencia al envío del Informe del Servicio de personal, de fecha 29 de abril de 2022, cuya copia se adjunta.
2-Contestación de la DPD sobre cuestiones planteadas por la reclamante, con fecha 21 de marzo de 2023, junto con la acreditación de su remisión.

Quinto. Acuerdo de inicio de procedimiento sancionador. (arts. 68 LOPDGDD; Art. 64 LPAC).

1. El 26 de junio de 2023 el director del Consejo dictó Acuerdo de Inicio de procedimiento sancionador contra la Diputación Provincial de Sevilla, con CIF *[NNNNN]*, por la presunta infracción de los artículos 5, 6, y 9 del RGPD, tipificada en el artículo 83.5 a) RGPD, y calificada a efectos de prescripción como muy grave en los artículos 72.1a), 72.1b) y 72.1e) LOPDGDD; así como por una presunta infracción del artículo 35 RGPD, tipificada en el artículo 83.4 a) RGPD; y calificada a los efectos de prescripción como grave en el artículo 73.t LOPDGDD.

2. Notificado el acuerdo de inicio al órgano reclamado, el 27 de junio de 2023, éste presentó alegaciones en las que, en síntesis, manifestaba lo siguiente:

"(...)Se remite la documentación remitida en el día de hoy consistente en oficio remitido por el Sr. Director del Área de Empleado Público, informe en el que se contienen las alegaciones que han de surtir efecto en el Procedimiento n.º PS-2023/020 (RCO-2022/046), así como informe emitido por la Gerente de Sociedad Provincial de Informática de Sevilla M.P. , S.A.U. (INPRO)".

En la Comunicación del Director del Área del Empleado Público, de fecha 11 de julio de 2023 (n.º nnnnn) se indicaba:

"(...)
En virtud de lo que antecede y, en contestación al acuerdo de inicio de procedimiento sancionador en el Expte. RCO-2022/046 dictado por el CTPDA, se procede por el Servicio de Personal a formular las siguientes ALEGACIONES:

PRIMERA.- Respecto a la necesidad, proporcionalidad e idoneidad, en relación con el tratamiento de los datos biométricos de carácter especial para el control horario del personal empleado público de la Diputación Provincial de Sevilla, su justificación se fundamenta en el principio de autoorganización de la Diputación Provincial de Sevilla en su calidad de Administración Pública, establecido dentro de la esfera de sus competencias, por el art. 4.1.a) de la Ley 7/1985, de 2 de abril, Reguladora de las Bases del Régimen Local y por el art. 4 del Real Decreto 2568/1986, de 28 de noviembre, por el que se aprueba el Reglamento de Organización, Funcionamiento y Régimen Jurídico de las Entidades Locales.
En este sentido, los tratamientos efectuados son necesarios para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorizan las Leyes reguladoras del Estatuto de los Trabajadores, como el TREBEP, como un convenio colectivo de personal laboral y un acuerdo de funcionarios con arreglo a Derecho y que dispone de las garantías adecuadas del respeto de los derechos fundamentales y de los intereses del personal empleado en la Corporación.
Asimismo, la necesidad, proporcionalidad e idoneidad, en relación con cada uno de los tratamientos mencionados, tiene su razón de ser en diversos informes que, en materia de protección de datos, han sido elaborados desde el Área de Empleado Público y remitidos a ese Consejo anteriormente en relación con este expediente. En este sentido, las garantías adoptadas en el sistema de tratamiento de datos biométricos por parte de la Corporación son relevantes a la hora de valorar la injerencia en el derecho fundamental de protección de datos y en la proporcionalidad de la medida. A tal fin debe tomarse en consideración que se ha extremado la confidencialidad con la creación de una secuencia alfanumérica que se encripta mediante un algoritmo, de tal manera que no se guardan los datos biométricos, tratando así de minimizar así la injerencia en el derecho fundamental.

Al hilo de lo anteriormente expuesto, se solicitó con fecha de 6 de julio de 2023, desde la Dirección General del Área del Empleado Público a la Gerencia de la Sociedad Provincial de Informática de Sevilla M.P. SAU (en adelante INPRo), informe que diera respuesta a las siguientes consultas:
"• Características técnicas del sistema de datos biométricos utilizados, beneficios y ventajas de su uso.
• Descripción del método encriptado y longitud de la clave de encriptación.
• Informe acerca de si pudiera producirse "invasión" de datos personales de los empleados públicos a los que va dirigido el sistema de datos biométricos utilizado y evidencia de la seguridad de la que adolece dicho sistema.
• Información sobre si se ha producido durante el tiempo de aplicación de este sistema, algún uso fraudulento del mismo, como por ejemplo:

◦ Error en la configuración de un sistema, aplicación, estación de trabajo, impresora o componente de red.
◦ Posibilidad de boicoteo de los elementos de control.
◦ Software malicioso (virus, troyanos, secuestradores de información).
◦ Fuga de información.
◦ Robo o extravío de equipos, soportes o dispositivos con datos personales.
◦ Acceso a una información, servicios, aplicaciones o dispositivos de forma no consentida, por personas no autorizadas, traspaso de barreras (Hacking) y ataques de denegación de servicio.
◦ Existencia de errores técnicos o fallos que ocasionen la indisponibilidad de los sistemas de información.
◦ Suplantación de identidad en el uso del sistema de datos biométricos.
• Información acerca de si otras Entidades Públicas utilizan datos biométricos como sistema de acceso y/o control de presencia en las instalaciones correspondientes."

Recibido informe de INPRO con fecha de 7 de julio de 2023 y, aunque se adjunta como Documento N.º 1, en dicho informe se pone de manifiesto que *"Desde "sistema" no se puede acceder a la información de datos biométricos de los empleados públicos, debido a que no es accesible desde la web ni está en Base de datos. Está almacenada en ficheros del servidor que está alojado en la Diputación de Sevilla, en ficheros con claves alfanuméricas y hash encriptados y son los que son compartidos puntualmente entre los terminales, para las altas."*

Asimismo, respecto de la consulta planteada acerca de si se ha producido durante el tiempo de aplicación de este sistema, algún uso fraudulento del mismo, a todos los ejemplos planteados en la solicitud de informe, se responde negativamente, evidenciando por tanto, la seguridad que tiene el nuevo sistema de control de presencia implantado en la Diputación de Sevilla. Asimismo, a la pregunta de si otras Entidades Públicas utilizan datos biométricos como sistema de acceso y/o control de presencia en las instalaciones correspondientes, se responde que el Cabildo de Tenerife está usando huella biométrica.

Además, se adjunta en el informe de INPRO el datasheet del terminal y documento en el que se describe el método de encriptado de los terminales. (Se adjunta informe de INPRO como Documento N.º 1).

En concordancia con lo anteriormente expuesto, se manifiesta que la necesidad, que no simple utilidad, del sistema de control de acceso y salidas mediante el tratamiento de datos biométricos, mejora la seguridad en dicho control, dado que el punto de inflexión en esta Corporación que llevó a la instauración de un nuevo sistema de control de presencia, deviene de diversas situaciones que se han producido por la obsolescencia del anterior sistema de tarjeta de proximidad, tanto respecto al boicoteo de los elementos de control de los lectores de tarjetas como a manifestaciones de suplantación de identidad por parte de algunos empleados públicos, tanto de la Corporación como de empresas externas a la misma, debido a que dicha tarjeta llevaba incorporado tanto el nombre, apellidos y DNI del titular como una fotografía del mismo, con el consiguiente riesgo de seguridad en caso de pérdida o sustracción de la tarjeta, situaciones que solían ocurrir a menudo, dando lugar a un intrusismo y fraude, que conllevaba a la instrucción de expedientes disciplinarios, resueltos en unos casos por la jurisdicción social y en otros por la vía contencioso-administrativa. Ejemplo de ello son la sentencia de 13/09/2016 recaída en demanda (Autos n.º 780/14), en el Juzgado de lo Social N.º 9 de Sevilla, confirmatoria de la sanción de suspensión de empleo y sueldo impuesta a la actora, así como el Decreto de desistimiento de la empleada demandada, dictado por el Juzgado de lo Contencioso-Administrativo n.º 5 de Sevilla

en el Recurso n.º 373/14 relativo a Expte. Disciplinario por el que se imponía sanción de suspensión de funciones.

A mayor abundamiento, podemos citar la Sentencia dictada por la Audiencia Nacional en fecha 19/9/19, recaída en el recurso n.º 774/2018, que en un supuesto similar, se cuestiona por parte de la AEPD el control de acceso por datos biométricos, a un gimnasio. La sentencia estima las actuaciones "valorando todas las circunstancias concurrentes expuestas y atendiendo a la normativa aplicable ratione temporis".

Por otro lado, si bien el virus de la COVID-19 se encuentra actualmente en una fase de estabilidad de la enfermedad, ésta no está erradicada por completo, de ahí que la flexibilización de las medidas preventivas será nuevamente sometida a revisión a partir del próximo 21 de octubre de 2023, a la luz de la evolución en este período y ante la entrada de la próxima estación invernal, atendiendo a la presión hospitalaria y a la aparición de posibles nuevas variantes del SARS-Cov2, como así establece la Orden de 19 de junio de 2023, por la que se prorrogan las medidas establecidas en la Orden de 17 de diciembre de 2021, publicada en BOJA Extraordinario núm. 17, de 20 de junio de 2023. No obstante, este no fue el motivo fundamental para la instauración del nuevo sistema, sino los que se han explicitado anteriormente.

SEGUNDA.- Respecto a la fecha de elaboración del Informe de Evaluación de Impacto de la Protección de Datos, se ha de aclarar que la elaboración del mismo fue previa a su instauración, estando finalizado y enviado con anterioridad a la implantación del nuevo sistema de control de presencia el 1 de marzo de 2023. Solamente, con carácter previo han utilizado este sistema algunos empleados que, voluntariamente y por la novedad y comodidad que les suponía, decidieron hacer uso del mismo. Es decir, el nuevo sistema de control de presencia basado en datos biométricos, no sólo se encontraba en período de prueba, sino que el acceso a través del mismo estaba sometido a la voluntariedad del personal empleado público,

TERCERA.- Respecto a la licitud del tratamiento, tiene su base legal en los artículos 6.1.c) y 9.2.b) del RGPD. El Registro de Actividades de Tratamiento de la Diputación declara que el tratamiento es lícito basado en los siguientes apartados del art. 6 del RGPD: apartado c) *"el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento", y en el apartado e) "el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento".*

Asimismo, el art. 9.2.b) del RGPD expresamente determina que *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado."*

En este supuesto se ha de tener en cuenta que el cambio operado en el control de acceso se puede entender ajustado a la tecnología existente en el momento, que es cuando se produjo la adquisición de los terminales, no siendo invasivo, como así se recoge en los informes anteriormente enviados y en el más reciente mencionado antes.

Si bien en el Acuerdo de inicio del procedimiento sancionador, el CTPDA manifiesta que la normativa referida no *"obliga a realizar ese control ni registro a través del tratamiento de datos biométricos de carácter especial puesto que ni lo exige expresamente ni puede deducirse necesariamente tal cosa de la naturaleza de la obligación, existiendo métodos alternativos perfectamente viables y contrastados para alcanzar el mismo fin"*, es palpable que el control del

cumplimiento de la jornada laboral y su registro, entra dentro del poder de Dirección de la Diputación de Sevilla, entendiéndose que el sistema de control de acceso ha sufrido una evolución con el devenir de los tiempos. En este sentido, la rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. - considerando 6 del RGPD -, razón por la que cuando se cambia el sistema, se adquiere uno que controle el acceso mediante datos biométricos.

En otras palabras, la Diputación ha de cumplir y cumple con las normas de protección de datos personales, y en base a dicho cumplimiento, se informó a los trabajadores, se adaptó el Registro de Actividades de Tratamiento (RAT), se llevó a cabo el Informe de Evaluación de Impacto en la Protección de Datos (EIPD) y, lo más importante, se mantienen unas infalibles **medidas de seguridad,** como así queda acreditado en los informes del expediente y, en especial, en el más reciente de fecha 7 de julio de 2023.

En este orden de ideas, si no fuera "necesario" el tratamiento de datos biométricos en la aplicación de un sistema de control de presencia, se produciría una incongruencia respecto a la imposibilidad de adaptar a las nuevas tecnologías, las distintas actuaciones de las Administraciones Públicas, obligándonos a anclarnos a sistemas antiguos e incluso obsoletos. Por ello, como ya se ha manifestado, y adaptándonos a los tiempos actuales, la necesidad existe desde el punto y hora que se adquieren esos equipos por problemas de seguridad en el sistema anterior (suplantación de identidad y boicoteo de los elementos de control), y respetando los requisitos que impone el ordenamiento jurídico de protección de datos personales, con los que la Corporación ha cumplido.

A mayor abundamiento, y analizados otras Fichas de Registro de Actividades (RAT) de otras administraciones, se observa que no solo la Diputación de Sevilla utiliza datos biométricos para el control de acceso, sino también otras Diputaciones de esta Comunidad Autónoma, entre ellas, Cádiz y Almería. Asimismo, en la Agencia Estatal de la Administración Tributaria (AEAT), consta la publicación de su RAT sobre el control de acceso por reconocimiento de huella dactilar mediante el tratamiento de datos de los empleados de la AEAT, incluidos colaboradores y empresas externas para el control horario y de facturación. En dicha ficha se detallan los datos objeto de tratamiento, siendo estos DNI, nombre, apellidos y datos biométricos.

Como conclusión de todo lo manifestado, entendemos que por la Diputación de Sevilla no se ha infringido ninguno de los preceptos de la normativa citados.

En este sentido, como ya ha quedado alegado y acreditado en este escrito, el tratamiento de los datos biométricos resulta necesario para el control de acceso de los empleados públicos a sus puestos de trabajo, por lo que nos encontramos ante el supuesto del art. 9.2.b) del RGPD; por otro lado, existe licitud en el tratamiento de los datos personales, por cuanto halla su base jurídica en los artículos 6.1.c) y el mencionado 9.2.b) del RGPD; el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento, estando ésta definida tanto en el Estatuto de los Trabajadores como en el Estatuto Básico del Empleado Público, ya identificadas estas Leyes en los distintos informes y en la Evaluación de Impacto realizada, no existiendo un tratamiento de datos excesivo, por cuanto no es posible el acceso a la información de datos biométricos de los empleados públicos; por último,por lo que hace a la evaluación de impacto, nos remitimos a la alegación segunda de este escrito.

Por lo expuesto,

SUPLICO AL CONSEJO que, teniendo por presentado este escrito y documento que se acompaña, lo admita, tenga por evacuado el mismo y tras la tramitación de Ley dicte Resolución por la que acuerde el archivo del procedimiento. Es justicia.
OTROSÍ DIGO que, al derecho de esta parte y como medios de prueba, se dejan citados los informes emitidos por el Servicio de Personal del Área de Empleado Público que ya constan en ese Consejo, además los informes, junto con la documentación que los acompaña, emitidos por la Sra. Gerente de INPRO, de fechas 9 de febrero de 2022, 17 de junio de 2022, así como el de 7 de julio del corriente que se aporta a este escrito. Todo ello por ser de justicia, que reitero, en Sevilla a la fecha de la firma electrónica.".

A dicho escrito se acompañaba Informe emitido por la Gerente de la Sociedad Provincial de Informática de Sevilla MP, S.A.U. (INPRO), de fecha 7 de julio de 2023; y un documento técnico en inglés que según manifiesta el órgano incoado, se trata del datasheet del terminal.

4. Con fecha 25 de enero de 2024 se recibe en este Consejo un escrito de la Delegada de Protección de Datos de la Diputación Provincial de Sevilla donde se indica:

"Recibido, con fecha de 23 de diciembre de 2023, escrito del Director General del Área de Empleado Público, procedemos a su remisión a efectos de que resuelva conforme a lo expuesto y solicitado en dicho escrito.".

A dicho escrito se acompañaba la "Comunicación Interior n.º 13672 de la Dirección General del Área de Empleado Público" en la que se exponía:

"Asunto: Tratamientos de control de presencia mediante sistemas biométricos.
Recibido, con fecha de 8 de enero de 2024, informe técnico-jurídico en materia de protección de datos, solicitado a la Delegada de Protección de Datos desde este Área, referente a las pautas a seguir en relación con la adaptación del control de presencia del personal de la Diputación de Sevilla, a fin de dar cumplimiento a los criterios exigidos por la Agencia Española de Protección de Datos (AEPD), a la vista de la Guía sobre Tratamientos de Control de Presencia mediante Sistemas Biométricos, se le informa que se ha publicado en esta Corporación, con fecha de 18 de enero de 2024, comunicado en el que se manifiesta que *"…a partir del próximo 22 de enero, se activará el sistema de acceso mediante tarjeta, que convivirá junto con el de reconocimiento de datos biométricos hasta el día 16 de febrero, fecha a partir de la cual dejará de estar activo, permitiéndose únicamente el acceso mediante tarjeta."*
Asimismo, se está procediendo a la revisión del Registro de la Actividad de Tratamiento del Sistema de control de acceso de personal a las instalaciones de la Diputación basado en tornos de acceso con terminales receptoras de datos biométricos, así como al bloqueo del tratamiento de dichos datos.
En virtud lo que antecede, del comunicado emitido y de los argumentos esgrimidos por la AEPD en la Guía mencionada, se solicita comunique al Consejo de Transparencia de Protección de Datos de Andalucía (CTPDA), las actuaciones practicadas con el fin de que se proceda al archivo del procedimiento sancionador con núm. PS 2023/020, así como de los expedientes relacionados con el citado procedimiento.
LA DIRECCIÓN DEL ÁREA DE EMPLEADO PÚBLICO.".

Sexto. Propuesta de resolución. (art. 89 LPAC).

1. Finalizada la instrucción del procedimiento, se procedió a realizar la correspondiente propuesta de resolución, estableciendo el plazo de diez días para la formulación de alegaciones, de conformidad con el artículo 89.2 LPACAP y en relación con el artículo 73.1 de la misma norma.

2. Notificada la propuesta de resolución al órgano reclamado el 2 de mayo de 2024, éste presentó alegaciones en las que, en síntesis, manifestaba lo siguiente:

"(...)QUINTO. Con fecha de 26 de mayo de 2023, se recibió por parte del Consejo de Transparencia y Protección de Datos de Andalucía, petición de informe sobre la Reclamación N.º RCO-2023/084, con el fin de dar respuesta a una reclamación recibida por una presunta implantación de sistema de control de acceso del personal mediante uso de datos biométricos (reconocimiento facial y de la palma de la mano) sin la necesaria legitimidad, siéndole enviado lo solicitado con fecha de 19 de junio de dicho año. En este sentido, se ha de poner de manifiesto que los reclamantes en estos procedimientos y el resto de empleados públicos, pudieron acceder a través del sistema de tarjeta hasta el 28/2/23, pues en tanto no se produjo la implantación definitiva en fecha 1/3/23, coexistían ambos sistemas de acceso.

SEXTO. Con fecha de 14 de diciembre de 2023, se recibe en este Área escrito de Secretaría General solicitando que, debido a la publicación el 23/11/2023 por la AEPD de una "Guía sobre Tratamientos de Control de Presencia mediante Sistemas Biométricos" y del procedimiento sancionador abierto por el CTPDA a la Diputación de Sevilla, se analice dicha Guía con el fin de adaptar el control de presencia del personal de la Corporación a los criterios dados por la AEPD o, si fuera necesario, sustituir por otros sistemas que cumplan las Directrices 5/2022, del Comité Europeo de Protección de Datos.

SÉPTIMO. Con fecha de 28/12/2023, se solicita a la Delegada de Protección de Datos de la Diputación de Sevilla, informe en materia de protección de datos, referente a las pautas a seguir en relación con la adaptación del control de presencia del personal de la Corporación, a fin de dar cumplimiento a los criterios exigidos por la AEPD, a la vista de la Guía mencionada, recibiéndose informe técnico-jurídico al respecto con fecha de 5 de enero de 2024, en el que se propone, para dar cumplimiento al contenido de la Guía de la AEPD, de fecha 23 de noviembre de 2023, eliminar el sistema de acceso mediante datos biométricos y volver al uso de tarjeta, debiéndose informar de ello al personal empleado, debiéndose adaptar, asimismo, el Registro de la Actividad de Tratamiento (RAT), y proceder, al menos, al bloqueo de dichos datos e incluso suprimir los obtenidos de acuerdo con la actual ficha del RAT, y por último, dar cuenta de lo actuado al CTPDA, dado que el expediente se encuentra abierto.

OCTAVO. Con fecha de 18 de enero de 2024, se publica en el tablón de anuncios del Portal, un comunicado dirigido a todo el personal de la Corporación, en el que se da conocimiento de la inminente eliminación del sistema de acceso mediante datos biométricos con fecha de 16 de febrero de 2024, y la vuelta al antiguo sistema de tarjeta, procediéndose ese mismo día a la desactivación del sistema de control de acceso mediante datos biométricos, y a la eliminación de

estos datos del personal, que constaban en dicho sistema, tanto los faciales como los de la palma de la mano.

ALEGACIONES:

Primera.- Se deviene por esta parte la necesidad de solicitar el archivo del procedimiento, en base a la permanente voluntad por esta Corporación de cumplir tanto la normativa en materia de protección de datos como las pautas y directrices marcadas por el CTPDA.

Sobre esta materia, se señala que la diferente documentación publicada de la AEPD no preveían la imposibilidad o ilicitud de tratar datos personales para el control horario, en este sentido dejamos citada la guía "la protección de datos en las relaciones laborales". No obstante, y como ya se ha puesto de manifiesto en el ordinal octavo de los hechos, cuando la AEPD, el pasado noviembre, publicaba la "Guía sobre el tratamiento de de control de presencia mediante sistemas biómetricos" es cuando de manera inmediata se adoptan las medidas necesarias para adecuarse a lo que ella dispone.

En este sentido, entendemos que desde el inicio de este proceso por el CTPDA, amplio en el tiempo, no se ha adoptado por el Consejo medida cautelar alguna que evidenciara una falta de legitimidad en la aplicación y control de la prestación del tiempo de trabajo del personal empleado de la Diputación Provincial de Sevilla. A mayor abundamiento, entendemos que durante este espacio de tiempo existe una causa sobrevenida que hace inviable la ejecución de la sanción propuesta, dado que ya ha sido eliminado todo sistema de control de acceso con datos biométricos, considerándose que no es posible ejecutar una sanción de unos hechos que no existen, ya que el responsable, motu propio, lo ha llevado a cabo. En este sentido, conviene señalar que todos los requerimientos realizados por ese Consejo, han sido atendidos en tiempo y forma, por lo que, reiteramos el archivo del procedimiento.-

Segunda.- En este sentido, en el punto 1.4 sobre tipificación, se alega infringido el art. 83.5. a), entendiendo esta parte, en estricto término de defensa, que no estamos ante un supuesto de ese tipo. Como es sabido el consentimiento decae en este caso. No se puede mediar consentimiento en relaciones de jerarquía, como esta, pues el consentimiento en cualquier caso estaría viciado. El empleado para el acceso al centro de trabajo ha de someterse a la decisión de la empleadora, de tal forma y manera que en esas relaciones no existe la libertad de prestar el consentimiento y poder en cualquier momentos desistir de este, todo ello de acuerdo con el art. 7 de RGPD, cuando regula "Condiciones para el consentimiento".

Así siguiendo a la AEPD, manifiesta al respecto:

"Con carácter general y para la implementación del registro de jornada no se precisa el consentimiento del trabajador, siendo base suficiente de legitimación la propia norma laboral, que en el artículo 34.9 ET establece la obligación de las empresas de realizar dicho registro de la jornada con carácter individual de cada persona trabajadora y que, de acuerdo con lo previsto en el artículo 6.1.c del Reglamento europeo 2016/679 (RGPD), el tratamiento de datos personales de los trabajadores derivado de la implantación del registro de jornada es necesario para el

cumplimiento de una obligación legal aplicable al responsable del tratamiento. No obstante lo anterior, la existencia de una lícita condición para el tratamiento de los datos de los empleados sin necesidad del consentimiento de los trabajadores no excluye el deber de las empresas de informar a los trabajadores de la existencia del registro y de la finalidad del tratamiento de los datos personales individuales que se obtienen con dicho registro".
Por lo que esta tipificación ha de decaer en toda su extensión.

Tercera.- En lo que se refiere a la realización de la Evaluación de impacto, esta se ha realizado antes de la implantación definitiva, que se llevó a cabo el 1/3/2023. Es cierto que ese Consejo requirió ampliación/aclaración de la Evaluación llevada a cabo, trámite que fue cumplimentado oportunamente, por lo que no consideramos correctas las consideraciones que se hacen a la Evaluación de impacto, señalándose expresamente que esta se ha realizado de acuerdo con la guía de la AEPD, y cumpliendo con las orientaciones allí manifestadas.

Cuarta.- Finalmente, consideramos que no se han encontrado evidencias que acrediten la existencia de infracción por parte de la Diputación de Sevilla. Muy al contrario, una vez tenido el conocimiento de la existencia de la nueva "Guía sobre utilización de datos biométricos para el control de presencia y acceso" de acuerdo con el Reglamento General de Protección de Datos (UE) 2016/679 (RGPD), publicada por la Agencia Española de Protección de Datos el pasado 23 de noviembre, y visto que los criterios recogidos en ella rompían con la opinión mantenida hasta ese momento por la Agencia, limitando el uso de datos biométricos por parte de las empresas para fines de control horario de jornada, de manera inmediata se tomaron por la Corporación las medidas necesarias para la utilización de sistemas de tratamiento menos invasivos para las personas, procediendo a la activación del sistema de acceso mediante tarjeta.

En virtud de lo que antecede, CABE CONCLUIR que, desde la Diputación Provincial de Sevilla, entendemos que se ha actuado conforme a Derecho y con todas las medidas de seguridad requeridas, tanto en lo que respecta a la implantación del sistema de acceso, como en la limitación de los datos biométricos recogidos a todo el personal empleado, siendo éstos los mínimos y absolutamente necesarios para el acceso a las instalaciones.
Asimismo, se informa se ha procedido a la eliminación de la Ficha del Registro de Actividades de Tratamiento "Sistema de control de acceso de personal a las instalaciones de la Diputación basado en tornos de acceso con terminales receptoras de datos biométricos".
Se adjunta a este escrito de alegaciones, documental probatoria requerida por el CTPDA, incluido certificado de la supresión de todos los datos biométricos faciales y de la palma de la mano de todas las personas empleadas en la Corporación, obtenidos hasta la fecha como consecuencia de la implantación del sistema de control presencial y de horario fundamentado en la utilización de datos personales biométricos.

Es por ello que, por la Diputación de Sevilla se solicita al Consejo de Transparencia y Protección de Datos de Andalucía, el archivo, del Procedimiento Sancionador PS-2023/2020 en relación con los Expedientes RCO-2022/046 y RCO-2023/084.

DOCUMENTACIÓN ADJUNTA:

Doc. 1.- Remisión, por DPD, de la Guía de AEPD. (14/12/2023)
Doc. 2.- Petición de informe a DPD sobre pautas a seguir. (28/12/2023)
Doc. 3.- Recepción de informe de DPD. (05/01/2024)
Doc. 4.- Comunicado a todo el personal de la Diputación de Sevilla sobre la vuelta a control de acceso mediante tarjeta. (18/01/2024)
Doc. 5.- Comunicado recordando la fecha de vuelta a tarjeta como sistema de control de acceso. (15/02/2024)
Doc. 6.- Certificado de supresión de los datos biométricos. ".

A dichas alegaciones se acompañaban entre otros la siguiente documentación:

1-Escrito del Secretario General al Director General del Área de Empleado Público, de 14 de diciembre de 2023, solicitando análisis de la situación tras la publicación de la Agencia Española de Protección de Datos de la Guía sobre tratamientos de control de presencia mediante sistemas biométricos, adjunto dicha guía.
2- Escrito del Director General del Área de Empleado Público a la Delegada de Protección de Datos, de fecha 28 de diciembre de 2023, solicitando informe de las pautas a seguir.
3- Escrito de la Delegada de Protección de Datos al Director del Área de Empleado Público, de fecha 5 de enero de 2024 por el que se le remite el Informe solicitado, que se adjunta (Informe n.º 80/2023).
4-Comunicado al personal de la Diputación de Sevilla sobre la vuelta a control de acceso mediante tarjeta. (18/01/2024)
5- Escrito del Director General del Área de Empleado Público recordando la fecha de la vuelta a la tarjeta como sistema de control de acceso.
6-Escrito de la Subdirectora del Area de empleado público, sin fechar, certificando la eliminación de datos biométricos faciales y de la palma de la mano, que ha concluido el 16 de febrero de 2024.

HECHOS PROBADOS

De los documentos obrantes en el expediente y de las actuaciones practicadas, pueden considerarse como hechos probados:

Primero. La Diputación Provincial de Sevilla implantó y utilizó un sistema de control horario mediante el uso de datos biométricos (reconocimiento facial y de la palma de la mano), desde el 9 de diciembre de 2021 hasta el 16 de febrero de 2024.

Desde el 9 de diciembre de 2021 hasta el 1 de marzo de 2023 se implantó de forma experimental, conviviendo con el sistema de tarjeta de proximidad y desde el 22 de enero de 2024 hasta el 16 de febrero de 2024 convivieron también los dos sistemas con vistas al cese del uso del sistema biométrico.

Desde el 1 de marzo de 2023 hasta el 22 de enero de 2024 el único sistema posible de control horario fue el biométrico.

Segundo. El informe de evaluación de impacto en la protección de datos (EIPD) aportada por el órgano reclamado aparece firmado con fecha 14 de noviembre de 2022.

FUNDAMENTOS JURÍDICOS

Primero. Sobre la competencia.

1. De conformidad con lo previsto en el artículo 57.1 y 64.2 LOPDGDD y el artículo 43.1 LTPA en relación con el artículo 3.1 LTPA corresponde a este Consejo como autoridad autonómica de protección de datos personales y dentro de su ámbito competencial, el ejercicio de la potestad sancionadora y de los poderes previstos en el artículo 58 RGPD.
2. 2. La competencia para la adopción de esta resolución reside en el Director, conforme al art. 48.1.i) LTPA y el art. 10.3.i) Estatutos.

3. Debe destacarse a su vez que, en virtud del artículo 16.5 del Decreto 434/2015, de 29 de septiembre, por el que se aprueban los Estatutos del Consejo de Transparencia y Protección de Datos de Andalucía, *"[e]l personal funcionario del Consejo, cuando realice funciones de investigación en materias propias de la competencia del Consejo, tendrá el carácter de agente de la autoridad"*, con las consecuencias que de aquí se derivan para los sujetos obligados en relación con la puesta a disposición de la información que les sea requerida en el curso de tales funciones investigadoras.
4. Este procedimiento se inicia como consecuencia de una presunta vulneración de la normativa de protección de datos por parte de una entidad bajo el control del Consejo en lo que respecta al cumplimiento de dicha normativa. Por ello, en el presente caso, solo serán analizadas y valoradas aquellas cuestiones planteadas por el reclamante, en relación con la materia de protección de datos personales, que queden incluidas dentro de la esfera de responsabilidad de la mencionada entidad.

Segundo. Sobre el tratamiento de datos personales.

1. El Art. 2.1. RGPD dispone: *"[e]l presente Reglamento se aplica al tratamiento total o parcialmente automatizado de datos personales, así como al tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero*".

2. El Art. 4.1 RGPD define «dato personal» como *"[t]oda 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"*.

   Los datos personales a los que se refiere la denuncia son categorías especiales de datos biométricos y concretamente datos de reconocimiento facial y de la palma de la mano.

3. De acuerdo con el Art. 4.2 RGPD, el tratamiento de datos personales es *"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".

En este caso, los tratamientos relacionados con la reclamación son la recogida, registro y almacenamiento de datos biométricos (reconocimiento facial y de la palma de la mano).

En relación a las operaciones de tratamiento realizadas, la entidad reclamada dispone de Registro de Actividades de Tratamiento, habiendo informado que aquellas operaciones se enmarcarían en la actividad de tratamiento "Sistema de control de acceso de personal a las instalaciones de la Diputación basado en tornos de acceso con terminales receptoras de datos biométricos"

4. Por último el Art. 4.7 RGPD considera responsable del tratamiento a aquella "...autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento..." Esta identificación del responsable de tratamiento debe entenderse completada por la concreción del tercero realizada en el art. 4.10 RGPD, e incluir por tanto a las "personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable...".

   El responsable de los tratamientos es la Diputación Provincial de Sevilla (Art. 4.7 RGPD).

Tercero. Sobre la calificación jurídica de los hechos.

1. Consideraciones sobre el tratamiento de datos biométricos de reconocimiento facial y de palma de la mano

1.1. Preceptos infringidos.

El artículo 9 RGPD en relación con el tratamiento de categorías especiales de datos personales establece que:

> *"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.*
>
> *2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:*
>
> *[...]*
>
> *b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;*
> *[...]*

La definición de datos biométricos se establece en el artículo 4 RGPD:

> *"14) «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;"*

Por su parte el Considerando 51 RGPD explica que:

> *(51) Especial protección merecen los datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. […] El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física. Tales datos personales no deben ser tratados, a menos que se permita su tratamiento en situaciones específicas contempladas en el presente Reglamento, habida cuenta de que los Estados miembros pueden establecer disposiciones específicas sobre protección de datos con objeto de adaptar la aplicación de las normas del presente Reglamento al cumplimiento de una obligación legal o al cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento. Además de los requisitos específicos de ese tratamiento, deben aplicarse los principios generales y otras normas del presente Reglamento, sobre todo en lo que se refiere a las condiciones de licitud del tratamiento.[…]"*

1.2. Consideraciones jurídicas sobre la existencia de infracción.

Analizaremos, por este orden, cuales son las categorías de datos tratadas y si se trata o no de datos biométricos; si tales datos biométricos deben considerarse categoría especiales de datos sujetas a la prohibición general de su tratamiento establecida en el artículo 9.1 RGPD; por último, si en el caso que nos ocupa existe alguna circunstancia de las previstas en el artículo 9.2 RGPD que permitan levantar dicha prohibición general de tratamiento.

En relación con las categorías de datos tratados, el órgano reclamado alega, en un informe de la Sociedad Provincial de Informática de Sevilla S.A.U. que :

> "La tecnología biométrica de la que disponen los terminales tiene un método de lectura que es mediante una cámara ubicada en el terminal. El sensor no guarda datos biométricos sino que recoge distintos puntos de la cara o palma (convergencias, desviaciones, empalmes) interrupciones, fragmentos, islote, bifurcación, punto, cortada} horquilla, encierro…). Una vez recogidos los distintos puntos y, en función de los parámetros establecidos por el fabricante, se crea una secuencia alfanumérica y esa secuencia se encripta mediante un algoritmo. Esto da lugar a una secuencia alfanumérica encriptada. El terminal no escanea la cara ni la palma por lo que de una cara o palma se obtiene una clave alfanumérica encriptada. El proceso es irreversible, de esa clave no se puede obtener la cara o palma."

Pues bien, técnicamente, la plantilla biométrica contra la que se coteja la muestra, es el producto de una medición que identifica unívoca y únicamente al individuo. En este caso es el resultado de la medición de los distintos puntos de la cara o palma (convergencias, desviaciones, empalmes, interrupciones, fragmentos, islote, bifurcación, punto, cortada, horquilla, encierro...). Es decir, son precisamente esas mediciones, convertidas en datos alfanuméricos lo que constituyen datos biométricos de carácter especial. Cuestión aparte es si, a través de la codificación o a través del cifrado de dichos datos, estos se almacenan con una mayor o menor seguridad. Pero tales circunstancias no afectan a su naturaleza como datos biométricos y al hecho de que se haya realizado un tratamiento, pues para empezar la recogida de los mismos ya constituye un tratamiento e implica, por tanto, ciertos riesgos.

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

La imagen del rostro o de la palma de la mano de la persona, en sí mismas, no tienen la consideración de datos biométricos. Los datos que tienen la consideración de datos biométricos son precisamente los datos alfanuméricos que permiten la identificación o la autenticación unívocas de una persona física, obtenidos del procesado de la imagen del rostro o de la palma de la mano mediante medios técnicos específicos destinados a tal fin.

El algoritmo del software, sobre la muestra biométrica, extrae las características biométricas, reduce y transforma en etiqueta o números esa muestra, constituyendo una representación matemática de la característica biométrica original, que es la plantilla biométrica. La plantilla se almacena para su comparación en la ultima fase, en la cual, con la muestra biométrica -cara- y con la plantilla previamente grabada, identificando unívocamente al empleado, en cada ocasión que entra o sale prestando su cara al dispositivo.

Ahora bien, no todos los datos biométricos tienen la consideración de categorías especiales de datos pues solamente tienen tal consideración los datos biométricos "dirigidos a identificar de manera unívoca a una persona física" (artículo 9.1 RGPD).

Analizaremos a continuación si los datos biométricos tratados en este caso (reconocimiento facial y de palma de la mano) tienen la consideración de categorías especiales de datos y, por tanto, es necesario acogerse a una de las circunstancias establecidas en el artículo 9.2 para levantar la prohibición general de su tratamiento prevista en el artículo 9.1 RGPD.

De la lectura conjunta del artículo 9 RGPD, 4.14 RGPD, y del Considerando 51 RGPD, se desprende que el elemento clave a la hora de considerar los datos relativos a las características físicas, fisiológicas o conductuales de una persona física como datos biométricos es que estos datos se traten con medios técnicos específicos con el fin de identificar o autenticar de forma unívoca su identidad y que cuando

esto sucede, nos encontraremos ante un tratamiento de datos personales que forman parte de una de las categorías especiales de datos a los que se refiere el artículo 9 RGPD.

El análisis del artículo 4.14 RGPD permite concluir que dentro de esta categoría especial de datos tienen cabida los datos biométricos que permiten tanto la identificación como la autenticación. Al respecto resulta concluyente la utilización de la expresión *"permitan o confirmen la identificación única"* dado que la confirmación de la identidad sería el caso de la autenticación.

Por si alguna duda cabe, como ya se ha expuesto, el Considerando 51 RGPD viene a explicitar que *"El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física."*

Ahora bien, también es cierto que el artículo 9.1 del RGPD, al prohibir el tratamiento de los datos biométricos destinados a identificar de forma unívoca a una persona física, no hace referencia explícita a la autenticación, a diferencia del artículo 4.14) del RGPD, que, al definir los datos biométricos, hace referencia tanto a la identificación como a la autenticación (*"permitan o confirman la identificación única"*).

Esto, junto con el hecho de que los sistemas biométricos, es decir, los sistemas que extraen y tratan los datos biométricos, tienen objetivos diferentes en el caso de la identificación uno a varios y en el caso de la autenticación uno a uno, han llevado en algunas ocasiones a plantear si realmente los datos biométricos tratados con medios técnicos para autenticar a una persona física deben considerarse categorías especiales de datos.

El Grupo de Trabajo del Artículo 29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, señalaba, entre otras cuestiones, que el tratamiento de los datos biométricos en un sistema biométrico suele constar de distintos procesos, tales como el registro de los datos biométricos, el almacenamiento biométrico y la correspondencia biométrica, entendida esta última como "el proceso de comparación de los datos o plantillas biométricas (capturados durante el registro) con los datos o plantillas biométricas recogidos en una nueva muestra a efectos de identificación, verificación y autenticación o categorización."

Se define en dicho dictamen la identificación biométrica, es decir, la identificación de una persona por un sistema biométrico como "el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios)."

Y se define la verificación o autenticación biométrica, es decir, la verificación de una persona por un sistema biométrico como "el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno)."

Ahora bien, esta distinción, fue hecha en un momento previo a la aprobación del RGPD en que ni unos ni otros datos biométricos tenían la consideración de categoría especial de datos. Por tanto, no se puede llegar a la conclusión de que sólo sean categoría especial de datos los que tienen como objetivo identificar a partir de la correspondencia uno a varios, dado que esto se opone claramente a la definición de datos biométricos contenida en el artículo 4.14) del RGPD. Se podría plantear, que a pesar de ser datos biométricos, la utilización de estos datos para realizar una autenticación no estuviera sometida al régimen del artículo 9 del RGPD. Pero lo cierto es que también debe descartarse esta posibilidad, dado que el artículo 9 no distingue entre unas y otras y simplemente se refiere a datos biométricos (y recordamos que el artículo 4.14 define qué hay que entender por datos biométricos "a efectos del presente Reglamento"). Por tanto, el concepto que da el artículo 4.14 es a todos los efectos del presente Reglamento, o sea, cuando el artículo 9 se refiere a datos biométricos, este concepto debe entenderse con el contenido del concepto previsto en el artículo 4.14.

Por otra parte, el artículo 9 sólo establece una condición, esto es, que los datos persigan la identificación unívoca de una persona física. Y este fin se cumple tanto en el caso de la autenticación como en el caso de la identificación de una persona entre varias.

Los sistemas biométricos pueden cumplir dos funciones diferentes: identificar a una persona entre un conjunto, para acabar determinando quién es una persona (o al menos si hay coincidencia con alguna de las personas previamente registradas) y autenticar (o determinar que una persona es realmente quien dice que es). Esta distinción entre el objetivo pretendido (si lo que se pretende es identificar o autenticar) puede decirse que resulta relevante en lo que respecta al desarrollo de los sistemas biométricos, desde el punto de vista de que el reconocimiento y la verificación implican utilizar técnicas diferentes y que algunos datos biométricos podrían ser más apropiados para la identificación y otros para la autenticación.

En cualquier caso, desde la vertiente de la protección de datos, dada la finalidad última de ambos supuestos y la definición contenida en el artículo 4.14 del RGPD, no parecería pertinente hacer esta distinción en cuanto a su consideración como a categoría especial de datos.

La biometría, como se ha visto, se refiere al análisis de una serie de características distintivas de cada individuo, en el sentido de que son rasgos únicos de cada persona, intransferibles, inolvidables y que permanecen inalterables o estables a lo largo del tiempo .

El tratamiento inadecuado de datos biométricos, con independencia de que sea a efectos de identificación o autenticación, puede comportar consecuencias importantes, incluso, irreparables, para los derechos y libertades fundamentales de las personas afectadas. El ejemplo más evidente es que, a diferencia de otros sistemas de identificación y autenticación, una vez comprometidos, estos datos lo estarán para siempre.

Cuestión distinta es que, en algunos supuestos, la utilización de la biometría para identificar a una persona de entre un conjunto pueda comportar unos riesgos mucho más elevados para los ciudadanos que un sistema que sólo tenga por objetivo la autenticación, pero en otros casos, los riesgos pueden ser similares.

Así, no parecería conveniente excluir una parte de los datos biométricos (aquellos que se someten a un tratamiento técnico específico con el fin de verificar la identidad de una persona) de la protección reforzada que el RGPD reconoce a aquellos datos personales que , por su naturaleza y el contexto en que se tratan, resultan particularmente sensibles, en atención a las consecuencias que, para las personas afectadas, pueden derivarse de su tratamiento, lo que tendría lugar si no se las reconociera como categoría especial de datos.

Es necesario pues interpretar que, cuando el RGPD se refiere a la identificación unívoca de una persona física en el artículo 9.1, también está haciendo referencia a la autenticación de la identidad de esa persona ("confirmar").

Por su parte, el Comité Europeo de Protección de Datos (CEPD) publicó las Directrices 05/2022 sobre el uso de técnicas de reconocimiento facial en el ámbito de la aplicación de la ley, que tienen por cometido aclarar algunas cuestiones sobre el tratamiento de datos biométricos en dicho ámbito.

Dichas Directrices 05/2022 del CEPD se dictaron en el ámbito específico de la aplicación de la Directiva (UE) 2016/680 del Parlamento y el Consejo, de 27 de abril de 2016, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. Esta Directiva (UE) 2016/680, del Parlamento y el Consejo, de 27 de abril de 2016 fue traspuesta al ordenamiento jurídico español a través de la Ley Orgánica 7/2021, de 26 de mayo, de protección de datos personales tratados para fines de prevención, detección, investigación y enjuiciamiento de infracciones penales y de ejecución de sanciones penales.

No obstante, las definiciones de los conceptos de dato personal, dato biométrico y dato de carácter especial contenidas en los artículo 3 y 10 de la Directiva (UE) 2016/680, de 27 de abril de 2016 y las establecidas en los artículos 5 y 13 de la Ley Orgánica 7/2021, de 26 de mayo son sustancialmente idénticas a las contenidas en los artículos 4 y 9 del RGPD. Por lo tanto, las afirmaciones de las Directrices 05/2022 del CEPD referidas a la definición de dichos conceptos se pueden considerar, en general, igualmente aplicables tanto al RGPD y la Ley Orgánica 3/2018, de 5 de diciembre, como a la Directiva (UE) 2016/680, de 27 de abril de 2016 y la Ley Orgánica 7/2021, de 26 de mayo.

Pues bien, en el párrafo 12 de las Directrices 05/2022 el CEPD afirma lo siguiente:

> "Mientras que ambas funciones – autentificación e identificación – son distintas, ambas se refieren al tratamiento de los datos biométricos relativos a una persona física identificada o identificable y, por tanto, constituyen un tratamiento de datos personales y, más específicamente, un tratamiento de categorías especiales de datos".

En el mismo sentido se ha pronunciado este Consejo en su Dictamen 1/2023[1] al afirmar que:

1 Dictamen 1/2023 relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento, de conformidad con la normativa de protección de datos. CTPDA, 28 de julio de 2023.

> "En tal sentido, debe significarse que las Directrices 05/2022 del Comité Europeo de Protección de Datos (CEPD), sobre el uso de reconocimiento facial en el ámbito de las fuerzas de orden público, vienen a superar en su apartado 12 la posible interpretación de que dicha prohibición solo afectaría a los supuestos de datos biométricos dirigidos a la identificación de una persona a través de la comparación de sus datos con una o varias bases de datos que identifican a un conjunto de personas (proceso de búsqueda de correspondencia "uno a varios"), extendiéndola también a los supuestos de datos biométricos dirigidos a la autenticación o verificación de la persona con respecto al patrón previamente establecido para la misma (proceso de búsqueda de correspondencia "uno a uno"). Habida cuenta de que actualmente se trata de la interpretación que ofrece mayor seguridad jurídica, será el criterio adoptado por este Consejo."

Posteriormente, la "Guía de tratamientos de control de presencia mediante sistemas biométricos"[2] de la AEPD vino también a afirmar que:

> "En definitiva, se ha de considerar que, al igual que en el caso de identificación, la autenticación biométrica es un proceso que implica el tratamiento de categorías especiales de datos personales."

Por todo lo expuesto se concluye que los datos biométricos, cuando se someten a un tratamiento técnico específico con el fin de identificar (reconocer) o de autenticar (verificar) de manera unívoca a una persona física, deben considerarse una categoría especial de datos personales y, por tanto, su tratamiento debe adecuarse al régimen específico establecido para este tipo de categorías de datos en la legislación de protección de datos.

Procede, por tanto, a continuación valorar si se aprecia en el caso objeto de esta reclamación la existencia de una de las circunstancias previstas en el artículo 9 RGPD para levantar la prohibición general de tratar categorías especiales de datos establecida en el artículo 9.1 RGPD.

La entidad reclamada justifica el tratamiento de categorías especiales de datos invocando como excepción frente a la prohibición general de tratamiento de datos biométricos, la contemplada en el artículo 9.2.b RGPD del siguiente tenor literal:

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

En este sentido, compartimos lo indicado en la Resolución PS-00218/21 de la Agencia Española de Protección de Datos, la cual señala:

2 Guía de tratamientos de control de presencia mediante sistemas biométricos, AEPD 23 de noviembre de 2023

"Sin embargo, acudiendo al levantamiento de la prohibición que prevé el tratamiento de los datos biométricos, el artículo 9.2.b) del RGPD que es el que guarda relación con el ámbito laboral, determina que:
-el tratamiento ha de ser necesario para dicho cumplimiento,
-en la medida en que así lo autoricen los Estados Miembros,
- o un Convenio Colectivo también con arreglo al derecho de los Estados miembros, que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado.
Estos son requisitos cumulativos que suponen una garantía adicional en el tratamiento de datos de su titular, que tiene en cuenta que si la consecución de los fines previstos puede realizarse sin tratamiento de datos personales, será preferible esta vía y supondrá que no es necesario llevar a cabo tratamiento alguno de datos, y subsidiariamente, que la recogida de datos sea necesaria para la finalidad establecida o pretendida y si lo fuera, que sea proporcional.
En todo caso, en estos tratamientos, se debe ser muy cauteloso en la valoración que se efectué sobre si se reúnen dichos requisitos, ya que se están tratando datos especiales.
(...)
Así, se concluye que la causa de legitimación para realizar el control horario de la jornada laboral diaria, sólo alcanza a la obligación de realizarla, pero no a realizarla utilizando datos biométricos, y su uso, sin causa de excepción para el tratamiento, como se ha acreditado, supone la infracción del artículo 9.2.b) del RGPD.".

Examinemos pues, si en el caso que nos ocupa se dan los mencionados requisitos exigidos en el artículo 9.2.b) del RGPD:

*T*anto el Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los trabajadores, como el Estatuto Básico del Empleado Público, aprobado por el Real Decreto Legislativo 5/2015, de 30 de octubre obligan al control del cumplimiento de la jornada laboral del personal y su registro. Pero en ningún caso obligan a que dicho control se lleve a cabo mediante sistemas biométricos ni de la naturaleza de esa obligación surge la necesitad de hacerlo.

Tal y como se expone en el Dictamen 1/2023[3] de este Consejo:

"Ello supone, como bien apunta el Dictamen 2/2022, de la Autoridad Catalana de Protección de Datos, que "la afectación por el derecho a la protección de datos que se derive de la norma debe ser previsible" y que "no se puede considerar previsible la norma si no concreta la posibilidad de utilizar datos biométricos con el fin de realizar el control horario".

Al hilo de lo indicado,[..] puede afirmarse que en la actual normativa legal española no se contiene autorización alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo: ni para el personal laboral, puesto que los artículos 20.3 y 34.9 del ET a los que se ha hecho referencia no contienen tal autorización, ni para el personal sometido a una relación jurídica administrativa al no constituirse en necesaria

3 Dictamen 1/2023 relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento, de conformidad con la normativa de protección de datos. CTPDA, 28 de julio de 2023.

habilitación la previsión relacionada con el cumplimento de jornada y horario a la que alude el artículo 54.2 del Real Decreto Legislativo que aprueba el texto refundido de la Ley del Estatuto Básico del Empleado Público (EBEP).[...]"

Posteriormente dicha afirmación también fue recogida en la "Guía de tratamientos de control de presencia mediante sistemas biométricos"[4] de la AEPD en la que se expone que:

"Ello supone, como bien apunta el Dictamen 2/2022, de la Autoridad Catalana de Protección de Da tos, que "la afectación por el derecho a la protección de datos que se derive de la norma debe ser previsible" y que "no se puede considerar previsible la norma si no concreta la posibilidad de utilizar datos biométricos con el fin de realizar el control horario".

[...] y, como también concluye el Consejo de Transparencia y Protección de Datos, en su Dictamen 1/2023, "Relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento", en la actual normativa legal española no se contiene autorización suficientemente específica alguna para considerar necesario el tratamiento de datos biométricos con la finalidad de un control horario de la jornada de trabajo. La autorización suficientemente específica no se encuentra para el personal laboral, puesto que los artículos 20.3 y 34.9 del Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores, no contienen tal autorización. Tampoco para el personal sometido a una relación jurídica administrativa al no constituirse en necesaria habilitación la previsión relacionada con el cumplimento de jornada y horario a la que alude el art. 54.2 del texto refundido de la Ley del Estatuto Básico del Empleado Público (EBEP), aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre. "

Por otro lado, prosigue el Dictamen 1/2023[5] de este Consejo:

"No obstante, a falta de previsión legal, la referida autorización o habilitación, de acuerdo con lo indicado en el artículo 9.2 b) del RGPD, podría estar prevista en los convenios colectivos para el personal laboral y en los acuerdos sobre condiciones de trabajo del personal funcionario en el marco de la negociación colectiva (en este último supuesto con los requisitos que para su eficacia se recogen en el artículo 38.3 del EBEP), siempre con el establecimiento de las garantías adecuadas respecto a los derechos fundamentales y de los intereses de los afectados."

En relación con dicha posibilidad y respecto al caso que nos ocupa la obligación que imponen los artículos 21 y 36 de los vigentes Acuerdos de Funcionarios y Convenio Colectivo del Personal Laboral de la Diputación de Sevilla, publicados en su portal de transparencia, es la del control del cumplimiento de la jornada laboral y su registro.

4 Guía de tratamientos de control de presencia mediante sistemas biométricos, AEPD 23 de noviembre de 2023.

5 Dictamen 1/2023 relativo al tratamiento de categorías especiales de datos biométricos mediante el uso de dispositivos de reconocimiento facial y/o huella dactilar para el control horario del personal de un Ayuntamiento, de conformidad con la normativa de protección de datos. CTPDA, 28 de julio de 2023.

Sin embargo dichos instrumentos de negociación colectiva tampoco obligan ni prevén la recogida de datos biométricos de carácter especial para realizar ese control y registro de la jornada laboral.

Por consiguiente, no se cumplen los requisitos exigidos por el artículo 9.2.b) RGPD para levantar la prohibición general de tratar categorías especiales de datos personales.

No entraremos a analizar si sería aplicable la circunstancia del artículo 9.2.a) RGPD relativa al consentimiento expreso de los interesados ya que el sistema biométrico fue de uso obligatorio para todos los empleados desde el 1 de marzo de 2023 hasta el 22 de enero de 2024, lo que excluye de plano la posibilidad de que tal consentimiento fuera libre sin necesidad de ulteriores análisis sobre el cumplimiento del resto de los requisitos del consentimiento del artículo 7 RGPD ni del resto de los principios de la protección de datos personales recogidos, principalmente, en el artículo 5 RGPD.

Por último, y en relación con las bases legitimadoras del artículo 6 RGPD alegadas por la entidad incoada, compartimos la afirmación manifestada en la "Guía de tratamientos de control de presencia mediante sistemas biométricos"[6] de la AEPD en en el apartado sobre la licitud del tratamiento en el sentido de que:

> "Si no se ha levantado la prohibición del tratamiento de categorías especiales de datos personales, en este caso biométricos, es indiferente que se cuente con una base jurídica de las previstas en el art. 6.1 del RGPD, puesto que ya hay una condición que invalida el tratamiento."

En conclusión, el órgano incoado llevó a cabo entre su personal un tratamiento de categorías especiales de datos biométricos sin que se diera una circunstancia que permitiera la prohibición general de tratamiento de dichas categorías especiales de datos, lo que supone una vulneración de lo dispuesto en el artículo 9 RGPD y que el tratamiento no cumple con lo establecido en la normativa de protección de datos, por tanto, no es válido.

1.3. Valoración de las alegaciones al acuerdo de inicio, pruebas practicadas o medidas provisionales.

El órgano reclamado comienza analizando la necesidad, proporcionalidad e idoneidad, en relación con el tratamiento de datos biométricos de carácter especial para el control horario del personal empleado público de la Diputación Provincial.

Al respecto debemos señalar que no compartimos la argumentación realizada por el órgano incoado. Debe recordarse que los responsables del tratamiento deben garantizar que el análisis de la necesidad y la proporcionalidad que se efectúe debe tener en consideración una evaluación exhaustiva de las opciones alternativas menos intrusivas disponibles, documentándose la viabilidad de otras opciones alternativas disponibles que no requieran el uso de datos especiales, comparar todas las opciones y documentar las conclusiones. Ninguna de estas labores constan en la documentación presentada por el órgano incoado en el presente caso.

En las citadas alegaciones se manifiesta, por otro lado que la seguridad del sistema es infalible. Al respecto hay que reiterar que la seguridad por sí sola, por muy alta que sea, no justifica la realización

6 Guía de tratamientos de control de presencia mediante sistemas biométricos, AEPD 23 de noviembre de 2023.

de un tratamiento inválido por no ser conforme al artículo 9 RGPD. Por otro lado debemos manifestar que el riesgo cero no existe en ningún tratamiento y, por tanto, no podemos considerar ninguna seguridad como infalible, como afirma el órgano reclamado.

Por otra parte, se considera que las hipotéticas y futuribles razones sanitarias invocadas, no concurren en la actualidad sin que se espere razonablemente un episodio similar, debiéndose recordar que el anterior sistema se llevaba a cabo a través de tarjetas sin contacto. Por otra parte, el propio órgano incoado reconoce en sus alegaciones que éste no fue el motivo fundamental para la instauración del nuevo sistema.

Además, se ha de indicar que no dudamos de las potestades de autoorganización que la normativa local atribuye a las Diputaciones Provinciales, pero ello no habilita para implantar un sistema que no cumpla la normativa de protección de datos.

Por otra parte y en cuanto a la alegación general de que la necesidad se encuentra justificada en los informes aportados, se ha de reiterar que dichas cuestiones tan solo son tratadas con especificidad en la EIPD (Informe de Evaluación de Impacto), donde no se aprecia un análisis suficiente de la necesidad y la proporcionalidad del tratamiento, no constando una evaluación exhaustiva de otras opciones alternativas menos intrusivas disponibles, ni documentación acerca de la viabilidad de otras opciones alternativas disponibles que no requieran el tratamiento de categoría especiales de datos, ni comparación de todas las opciones y documentación de las conclusiones. Y en cuento al Informe de la Sociedad Provincial de Informática de Sevilla MP. SAU (INPRO) de julio de 2023, aportado con las alegaciones al Acuerdo de Inicio del expediente sancionador, se considera que dicho informe, en todo caso, pondría de manifiesto la seguridad del sistema, pero no aporta nada concluyente respecto a su necesidad ni proporcionalidad, más allá de señalar escuetamente como beneficios y ventajas: "(rápido, infalsificables, sin tocar nada…"). El resto de la documentación aportada (datasheet del terminal y documento en el que se describe el método de encriptado de los terminales.) se sigue refiriendo a la seguridad del sistema.

Sobre la alegada inexistencia de incidentes respecto a episodios de uso fraudulento por parte de los trabajadores con el sistema implantado, tampoco resulta relevante en este caso, dado el poco tiempo que lleva funcionando el sistema a la fecha del informe (implantación definitiva 1 de marzo de 2023-fecha del Informe 7 de julio de 2023). Por otro lado no es su falibilidad lo que se juzga sino el cumplimiento por el mismo del artículo 9 RGPD, es decir, la existencia de o no de alguna de las circunstancias que levantan la prohibición que, con carácter general, se establece para el tratamiento de categorías especiales de datos personales.

En relación con los dos ejemplos aportados de irregularidades anteriores por parte del personal en el uso del control horario (Sentencia de 13 de septiembre de 2016, del Juzgado de lo Social n.º 9 de Sevilla y otro documento referente al Juzgado de lo Contencioso-Administrativo n.º 5 de Sevilla), se ha de indicar que la ocasional existencia de dos expedientes disciplinarios en el tiempo, no suponen, a juicio de este Consejo, una causa suficiente para implantar un sistema tan invasivo ni para el levantamiento de la prohibición general de tratar categorías especiales de datos. Por otra parte, y en relación con la alegada sentencia de la Audiencia Nacional (de 19 de septiembre de 2019, recurso n.º 774/2018), debemos indicar que dicha sentencia es de 19 de septiembre de 2019 y se refiere a hechos

acontecidos con anterioridad a la entrada en vigor del RGPD, norma que fue la que incluyó a los datos biométricos dentro de las categorías especiales de datos, estableciendo una regulación más estricta para dicha categoría de datos que la hasta entonces existente (fundamento de derecho quinto de la sentencia indicada).

En relación con la alegación del órgano reclamado de que nos encontramos, como causa justificante del tratamiento de datos de categorías especiales, ante el supuesto contemplado en el artículo 9.2. b) RGPD, debemos reiteramos en lo ya señalado al respecto en el Acuerdo de Inicio del expediente sancionador, págs. 52 a 54, y en el subapartado anterior y a lo cual nos remitimos.

En cuanto a la afirmación sobre que otras administraciones públicas pudieran estar utilizando un sistema similar al empleado por el órgano incoado, cuestión sobre la que por otra parte no se aporta prueba, en todo caso no supone causa de legitimación para su uso por el órgano incoado ni le exime de su responsabilidad.

En relación con la licitud alegada con fundamento en el artículo 6.1.c) RGPD, ya se ha señalado que habiéndose demostrado que no se ha conseguido levantar la prohibición del tratamiento de categorías especiales de datos personales, ya que, como hemos visto, no concurre ningún supuesto de los contemplados en el artículo 9 RGPD, resulta indiferente que se cuente con una base jurídica de las previstas en el artículo 6.1 del RGPD, ya que hay una condición que invalida el tratamiento.

Por ultimo, se ha recibido en este Consejo con fecha 25 de enero de 2024, un escrito de la DPD del órgano incoado en el que se manifiesta que:

> "Recibido, con fecha de 8 de enero de 2024, informe técnico-jurídico en materia de protección de datos, solicitado a la Delegada de Protección de Datos desde este Área, referente a las pautas a seguir en relación con la adaptación del control de presencia del personal de la Diputación de Sevilla, a fin de dar cumplimiento a los criterios exigidos por la Agencia Española de Protección de Datos (AEPD), a la vista de la Guía sobre Tratamientos de Control de Presencia mediante Sistemas Biométricos, se le informa que se ha publicado en esta Corporación, con fecha de 18 de enero de 2024, comunicado en el que se manifiesta que *"…a partir del próximo 22 de enero, se activará el sistema de acceso mediante tarjeta, que convivirá junto con el de reconocimiento de datos biométricos hasta el día 16 de febrero, fecha a partir de la cual dejará de estar activo, permitiéndose únicamente el acceso mediante tarjeta."*
> Asimismo, se está procediendo a la revisión del Registro de la Actividad de Tratamiento del Sistema de control de acceso de personal a las instalaciones de la Diputación basado en tornos de acceso con terminales receptoras de datos biométricos, así como al bloqueo del tratamiento de dichos datos."

Cabe deducir por tanto, que se ha valorado que la actuación preferente no se adecuaba a los criterios aplicables desde el punto de vista de la normativa de protección de datos. En este sentido este Consejo valora muy positivamente que el órgano incoado decidiera por sí mismo a lo largo d ella instrucción de este procedimiento sustituir el sistema de control horario por biometría por otro sistema y que haya eliminado los datos biométricos de las personas interesadas.

Sin embargo, no ha quedado acreditado documentalmente que se haya producido efectivamente el cambio señalado en el sistema a partir del día 16 de febrero de 2024 y la inactivación de tal sistema, origen del presente expediente sancionador. Tampoco queda acreditado el *bloqueo* de los datos biométricos obtenidos hasta el momento.

Por otro lado, a pesar de haber indicado el 25 de enero de 2024 que, como consecuencia del abandono del sistema biométrico, se estaba procediendo entre otras tareas al bloqueo de los datos y a la revisión del Registro de Actividades de Tratamiento, por personal de este Consejo se accedió el 30 de abril de 2024 a la actividad de tratamiento "Servicio de personal"[7] del Inventario de Actividades de Tratamiento de la Diputación de Sevilla y siguen apareciendo en el apartado "Datos personales requeridos para el tratamiento" los denominados "Datos de reconocimiento biométrico a efectos de autenticación del control de presencia de su personal."

Por último y en todo caso, la subsanación de las infracciones imputadas, en el que caso de que quedase acreditada, no puede suponer el archivo del expediente sancionador ni la exención de la responsabilidad del órgano incoado, puesto que la conducta infractora habría persistido al menos hasta el 16 de febrero de 2024.

De acuerdo con todo lo expuesto, entendemos que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

1.4. Valoración de las alegaciones a la propuesta de resolución, pruebas practicadas o medidas provisionales.

En relación con las alegaciones del órgano reclamado señalar, en primer lugar, que con la documentación presentada, ha quedado acreditado que con fecha 16 de febrero de 2024, se ha procedido a sustituir el sistema de control mediante datos biométricos por el sistema anteriormente vigente mediante tarjeta (Comunicado al personal de la Diputación de Sevilla sobre la vuelta a control de acceso mediante tarjeta. (18/01/2024) y Escrito del Director General del Área de Empleado Público recordando la fecha de la vuelta a la tarjeta como sistema de control de acceso).

En segundo lugar, la sustitución del sistema utilizado de datos biométricos por otro correcto habiéndose incoado un procedimiento sancionador, constituye una obligación legal y, en todo caso, una subsanación de la infracción previamente cometida, pudiendo suponer por ello una causa de atenuación de la responsabilidad del órgano incoado, de acuerdo con los criterios contenidos en el artículo 83.3 RGPD, pero no una circunstancia eximente de la misma. Consecuentemente, no puede accederse a su petición de archivo del expediente sancionador.

En tercer lugar, debe tenerse en cuenta que la normativa aplicable (LOPDGDD), como fuente del derecho, no ha sufrido cambio respecto a los preceptos fundamentales aplicados, debiéndose recordar que la Agencia Española de Protección de Datos, ya en la resolución correspondiente al citado expediente sancionador PS-00218/2021, de fecha 1 de junio de 2022, mantenía la misma postura defendida por este Consejo.

7 https://protecciondatos.dipusevilla.es/fichaactividad/9

En cuarto lugar, y respecto a la falta de adopción de medidas cautelares por este Consejo recordar que si bien el artículo 69 LOPDGDD contempla la posibilidad de la adopción de medidas provisionales durante la realización de las actuaciones previas de investigación o iniciado un procedimiento para el ejercicio de la potestad sancionadora, no es menos cierto que se trata de una potestad discrecional ("podrán") y sujetas a límites, como son la necesidad y proporcionalidad, sin que, lógicamente, la no adopción de las mismas pueda ser esgrimida por el principal beneficiado como es el órgano incoado como prueba de la no existencia de infracción.

Debe tenerse en cuenta que en un procedimiento sancionador las medidas cautelares tienen un componente excepcional, por ser generador de perjuicios inmediatos para el órgano incoado sin que se haya comenzado o finalizado el correspondiente expediente sancionador. Por otra parte y en caso de no ser declarada finalmente la existencia de infracción puede suponer la generación de responsabilidad para la autoridad que las haya ordenado. Consecuentemente las medidas provisionales deben aplicarse bajo criterios de discrecionalidad, estricta necesidad y prudencia.

En quinto lugar, debemos señalar que no podemos compartir la afirmación relativa a la incorrecta tipificación contenida en la Propuesta de Resolución. Concretamente se indicaba en dicho documento:

"El incumplimiento de las disposiciones relativas a "los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9" del RGPD tipificada en el artículo 83.5.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción muy grave por vulneración sustancial del artículo 9) RGPD "Tratamiento de categorías especiales de datos personales" y, en particular, en el artículo 72.1 e) LOPDGDD:

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

En este supuesto, como se ha venido manteniendo a lo largo del expediente sancionador, se ha apreciado un incumplimiento sustancial del artículo 9 RGPD ,"*Tratamiento de categorías especiales de datos personales",* estando tipificado dicho incumplimiento en el artículo 83.5. a RGPD, y en particular y a efectos de prescripción en el transcrito artículo 72.1 e) LOPDGDD. Una interpretación coherente del citado artículo 83.5 a RGPD, nos lleva a la conclusión de que la referencia a las condiciones del consentimiento contenida en dicho precepto debe entenderse circunscrita al artículo 7 RGPD *"Condiciones para el consentimiento"*, no siendo este el caso que nos ocupa.

En este sentido también se ha pronunciado la Agencia Española de Protección de Datos en la ya citada Resolución correspondiente al expediente sancionador PS-00218/2021 de la con fecha 1 de junio de 2022. Concretamente:

"(...)PRIMERO: SANCIONAR (...), por las infracciones del RGPD:

-artículo 9.2.b) del RGPD, tipificada en el artículo 83.5 a) del RGPD y en el 72.1. e) de la LOPGDD. (...)".

En sexto lugar y respecto a la eliminación del tratamiento relativo a recogida de datos biométricos en la Ficha de Registro de Actividades de Tratamiento, se ha de señalar que tal y como se indicó en la Propuesta de Resolución (página 36), en relación con el Registro de Actividades de Tratamiento, por personal de este Consejo se accedió el 30 de abril de 2024 a la actividad de tratamiento "Servicio de personal" del Inventario de Actividades de Tratamiento de la Diputación de Sevilla, donde seguía apareciendo en el apartado "Datos personales requeridos para el tratamiento" los denominados "Datos de reconocimiento biométrico a efectos de autenticación del control de presencia de su personal.".

Pues bien, realizado como consecuencia de las alegaciones un nuevo acceso al Registro de Actividades de Tratamiento del órgano incoado con fecha 6 de junio de 2024, se puede comprobar que en la actividad de tratamiento "Servicio de personal" del Inventario de Actividades de Tratamiento de la Diputación de Sevilla, continúa apareciendo en el apartado "Datos personales requeridos para el tratamiento" los denominados "Datos de reconocimiento biométrico a efectos de autenticación del control de presencia de su personal.".

En séptimo lugar y en relación con la supresión de los datos biométricos de reconocimiento facial y del palma de mano, se considera como válido el aportado escrito de la Subdirectora del Área de empleado público certificando la eliminación de datos biométricos faciales y de palma de la mano. No obstante, no consta acreditado que ello se hubiera comunicado individualmente a todas las personas afectadas.

De acuerdo con todo lo expuesto, entendemos que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

1.5. Tipificación.

Los hechos atribuidos al órgano incoado, por las razones expuestas, podrían suponer las siguientes infracciones a la normativa de protección de datos personales, sin perjuicio de lo que resulte de la instrucción del procedimiento:

El incumplimiento de las disposiciones relativas a "los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9" del RGPD tipificada en el artículo 83.5.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción muy grave por vulneración sustancial del artículo 9) RGPD "Tratamiento de categorías especiales de datos personales" y, en particular, en el artículo 72.1 e) LOPDGDD:

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

2. <u>Consideraciones sobre la realización de una evaluación de impacto en la protección de datos personales cuando ya se había iniciado el tratamiento.</u>

2.1. Preceptos infringidos.

El artículo 35 RGPD, en relación con la evaluación de impacto relativa a la protección de datos personales, o EIPD, establece que:

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

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

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

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

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

[…]
7. La evaluación deberá incluir como mínimo:
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

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

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas. […]

2.2. Consideraciones jurídicas sobre la existencia de infracción.

En relación con el Informe de Evaluación de Impacto, señalar que a tenor de la definición contenida en el artículo 4.2 del RGPD del término *"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"*, la operación de "recogida" de datos personales ha de considerarse como tal.

Por otra parte, el artículo 35 del citado RGPD dispone que *"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 de impacto de las operaciones de tratamiento en la protección de datos personales.".*

En el mismo artículo 35 se prevé que el tratamiento se requerirá especialmente en caso de, entre otros, *" tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, […]".*

Por otro lado, en las listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a protección de datos publicadas por la AEPD, de conformidad con el artículo 35.4 del RGPD, encontramos los siguientes criterios aplicables al caso:

> *"4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD […]"*
> *"5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física."*
> *"10. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas".*

Recordemos que basta con la concurrencia de dos o más de estos criterios para que se considere obligatoria la realización de una Evaluación de Impacto en la Protección de Datos.

Por otro lado, no se encuentra ningún criterio aplicable al caso, que exima a la reclamada de la realización de EIPD, en la lista orientativa de tipos de tratamientos que no requieren una evaluación de impacto relativa a la protección de datos según el artículo 35.5 RGPD publicada por la AEPD.

Se concluye por tanto que la realización de una EIPD era obligatoria en este caso y lo era antes del inicio del tratamiento.

En relación con ello y de acuerdo con la documentación obrante en el expediente, se advierte que si bien obra en el mismo un Informe de Evaluación de Impacto en la Protección de Datos (EIPD),

aportado por el órgano responsable, éste fue realizado con posterioridad a iniciar la recogida de datos biométricos de los empleados.

En este sentido, afirmaba la reclamante en su reclamación que con fecha 18 de octubre de 2021 se comunicó por el órgano responsable la instalación de nuevos lectores para el control de acceso en todos centros de la Corporación, cuestión confirmada por el propio responsable en sus alegaciones.

En dicho comunicado, se establecía " (...)En próximo comunicado, se establecerá el calendario para la toma de los datos necesarios que se precisen (huella/reconocimiento facial) , que se fijará con citas por Áreas y Centros de la Corporación".

A continuación señalaba la reclamante "(...) que la semana posterior a este comunicado se procede a tomar los datos en mi centro de trabajo y en todo el complejo de *[nombre del complejo]* (...)".

Posteriormente, con fecha 4 de febrero de 2022, se produce un nuevo comunicado del órgano responsable en el que se indica, además de que se continúa el proceso en fase de prueba de instalación del nuevo sistema de acceso, se destaca la colaboración voluntaria prestada por los empleados/as para a recogida de datos biométricos.

Igualmente y respecto a esta cuestión, baste señalar que el Informe del Área del Empleado Público, de fecha 10 de febrero de 2022 se señala: " (...) se está llevando a cabo la elaboración de un informe de evaluación de impacto en la protección de datos (EIPD), con el fin de proceder al análisis de los riesgos(...)." . En el mismo se pronuncia el Informe del Servicio de Personal, de fecha 29 de abril de 2022, en el que se indica: "(...) se está en proceso de tramitación la elaboración del informe de evaluación de impacto en la protección de datos (EIPD), tal y como requiere la normativa reguladora en esta materia(...).".

Finalmente, es con motivo de un requerimiento de información y documentación realizado desde este Consejo cuando con fecha 14 de noviembre de 2022, se aporta el citado Informe de evaluación de Impacto de protección de datos (EIPD). Dicho informe carece de fecha, pero aparece firmado, tanto por el Director General del Área de Empleo Público como de la DPD, E. Por otro lado, el también aportado Informe de Riesgo aparece con fecha 11 de noviembre de 2022.

Consecuentemente y a tenor de los datos anteriormente señalados, se llega a la conclusión de que se inició el tratamiento de datos personales biométricos en octubre de 2021, con la recogida de los datos biométricos; siendo con posterioridad cuando se tramita y finaliza la Evaluación de Impacto relativa a la protección de datos, noviembre de 2022, circunstancia que conlleva la apreciación de una presunta infracción a lo dispuesto en el artículo 35 RGPD, al deber ser el citado Informe anterior al inicio del tratamiento.

Por otra parte, no es aceptable la argumentación de que el citado Informe es anterior a la implantación definitiva del sistema (1 de marzo de 2023), ya que el tratamiento de datos personales se inicia, como hemos señalado anteriormente, con la recogida de los datos y no con la posterior implantación definitiva del sistema.

Hay que destacar que ningún precepto de la normativa de protección de datos exime de la aplicación de esta a los tratamientos de datos personales por el hecho de que se encuentren en fase de pruebas o de aplicación provisional.

2.3. Valoración de las alegaciones al acuerdo de inicio, pruebas practicadas o medidas provisionales.

En relación con la alegación referente a la fecha de elaboración del Informe de Evaluación de Impacto de la Protección de datos (noviembre de 2022), y que éste estaba finalizado con anterioridad a la implantación del nuevo sistema de control de presencia (1 de marzo de 2023), nos volvemos a reiterar en lo ya señalado al respecto en el sentido de que dicha alegación no es aceptable, ya que el tratamiento de datos se inicia con la recogida de datos (octubre de 2021) y no con la posterior implantación definitiva del sistema (1 de marzo de 2023). Todo ello volviendo a reiterar que ningún precepto de la normativa de protección de datos exime de la aplicación de ésta a los tratamientos de datos personales por el hecho de que se encuentren en fase de pruebas o aplicación provisional. Por último, señalar que la realización de la EIPD, con carácter previo y necesario al inicio del tratamiento cuando, como en este caso ha quedado acreditado, ésta es obligatoria no está sujeta a la voluntariedad del personal.

2.4 Valoración de las alegaciones a la propuesta de resolución, pruebas practicadas o medidas provisionales.

En relación con la breve alegación referente a la evaluación de impacto en la protección de datos personales cuando ya se había iniciado el tratamiento, y a falta de mayor precisión, nos remitimos a lo ya señalado al respecto en la Propuesta de Resolución (página 40), debiendo reiterarse que no es aceptable como causa exculpatoria de la infracción que nos ocupa el que la Evaluación de impacto (noviembre de 2022) es anterior a la implantación definitiva del sistema (1 de marzo de 2023), ya que el tratamiento de datos personales se inicia con la recogida de los datos (octubre de 2021) y no con la posterior implantación definitiva, debiendo haberse realizado la citada Evaluación de Impacto antes de esta última fecha, es decir, antes de iniciar la recogida de datos.

En cuanto al alegado contenido del citado documento de Evaluación de Impacto y ante la ausencia de mayor detalle, nos reiteramos en lo ya señalado al respecto en la Propuesta de Resolución (página 35), en el sentido de que *" no se aprecia un análisis suficiente de la necesidad y la proporcionalidad del tratamiento, no constando una evaluación exhaustiva de otras opciones alternativas menos intrusivas disponibles, ni documentación acerca de la viabilidad de otras opciones alternativas disponibles que no requieran el tratamiento de categoría especiales de datos,ni comparación de todas las opciones y documentación de las conclusiones. ".*

De acuerdo con todo lo expuesto, entendemos que las alegaciones presentadas no desvirtúan el contenido esencial de la infracción que se declara cometida ni suponen causa de justificación o exculpación suficiente.

2.5 Tipificación.

Los hechos atribuidos al órgano incoado, por las razones expuestas, podrían suponer las siguientes infracciones a la normativa de protección de datos personales, sin perjuicio de lo que resulte de la instrucción del procedimiento:

El incumplimiento de las disposiciones relativas a "las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43" del RGPD tipificada en el artículo 83.4.a) RGPD; calificada a efectos de prescripción en la LOPDGDD como infracción grave por vulneración sustancial del artículo 35 RGPD "Evaluación de Impacto relativa a la protección de datos" y, en particular, según el artículo 73. t) LOPDGDD:

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

Cuarto. Sobre la identificación de la entidad responsable (art. 89.3 LPAC).

De conformidad con lo previsto en el artículo 70.1 LOPDGDD, se identifica como entidad responsable de las infracciones a infracción, a la Diputación Provincial de Sevilla, con CIF *[NNNNN].*

Quinto. Declaración de la infracción y medidas a adoptar (art. 77.2 LPAC y 58.2 RGPD).

El artículo 77 LOPDGDD establece el régimen sancionador aplicable a determinadas categorías de responsables o encargados del tratamiento; incluyendo, entre otros a:

> *"a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.*
> *[...]*
> *c) [...] las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.*
> *d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.*
> *e) Las autoridades administrativas independientes.*
> *[...]*
> *g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.*
> *h) Las fundaciones del sector público.*
> *i) Las Universidades Públicas.*
> *j) Los consorcios.*
> *k) Los grupos parlamentarios de [...] las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.*

En el mencionado artículo, en su apartado 2, se señala que:

> *"Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución declarando la infracción y estableciendo, en su caso, las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, con excepción de la prevista en el artículo 58.2.i del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.[...]".*

A su vez, en su apartado 3, se señala que:

> *"Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.*
>
> *Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda."*

Por otra parte, en relación con las medidas que proceda adoptar, el artículo 58.2 RGPD dispone que:

> *"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación: [...]*
>
> *d) ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado; [...]*
>
> *f) imponer una limitación temporal o definitiva del tratamiento, incluida su prohibición;*
>
> *g) ordenar la rectificación o supresión de datos personales o la limitación de tratamiento con arreglo a los artículos 16, 17 y 18 y la notificación de dichas medidas a los destinatarios a quienes se hayan comunicado datos personales con arreglo a al artículo 17, apartado 2, y al artículo 19;[...]*
>
> *j) ordenar la suspensión de los flujos de datos hacia un destinatario situado en un tercer país o hacia una organización internacional.* [...]".

Así, de acuerdo con el artículo 77.2 LOPDGDD, procede declarar la infracción o infracciones antes descritas.

En relación con las posibles medidas a adoptar es necesario tener en cuenta lo siguiente:

a) El órgano incoado ha presentado un certificado expedido por la persona titular de la Subdirección del Área de Empleado Público certificando el borrado de los datos biométricos de las personas interesadas. Esto daría cumplimiento a las medidas correctivas incluidas en la propuesta de resolución que se refería a:

> "a) Prohibir el tratamiento con carácter definitivo en ejercicio de los poderes correctivos atribuidos a esta autoridad de control en el artículo 58.2.f) RGPD. Para acreditar el cumplimiento de esta medida la Diputación Provincial de Sevilla debe remitir al Consejo, en el plazo máximo de un mes tras la

notificación de la resolución definitiva, la documentación acreditativa del cese definitivo del sistema de control presencial y de horario fundamentado en la utilización de datos personales biométricos.

b) Ordenar a la Diputación Provincial de Sevilla que, de conformidad con el artículo 58.2.d) y g) RGPD proceda, en el plazo de un mes a la supresión de los datos biométricos de todas las personas afectadas, sin perjuicio de la conservación de los datos horarios relativos a los datos de registro de entradas y salidas y control horario. Para acreditar el cumplimiento de esta medida la Diputación Provincial de Sevilla debe remitir al Consejo, en el plazo máximo de un mes tras la notificación de la resolución definitiva, la documentación acreditativa suscrita por autoridad competente de que se han suprimido todos los datos biométricos de todos los afectados, obtenidos hasta la fecha como consecuencia de la implantación del sistema de control presencial y de horario fundamentado en la utilización de datos personales biométricos."

b) Como se ha puesto de manifiesto a lo largo del procedimiento el tratamiento de categorías especiales de datos biométricos era ilícito pues no se contaba con una circunstancia para levantar la prohibición general de su tratamiento de conformidad con el artículo 9 RGPD.

El artículo 17 RGPD prevé como una de las circunstancias en las que es aplicable el derecho de supresión la de que *"d) los datos personales hayan sido tratados ilícitamente;".* Si bien este artículo regula el ejercicio de este derecho a solicitud de los interesados, este Consejo entiende que si ha quedado acreditada la ilicitud del tratamiento, como en este caso, el responsable, en ejercicio del principio de responsabilidad activa demostrable establecido en el artículo 5.2 RGPD y del principio de lealtad establecido en el artículo 5.1.a) RGPD, debe proceder a la supresión de oficio de los datos biométricos de los que son titulares todas las personas afectadas hayan o no solicitado su supresión. Por personas afectadas entendemos todas aquellas cuyos datos biométricos fueran tratados en cualquier fase del tratamiento, continúen o no trabajando en la Diputación Provincial de Sevilla. Esta supresión alcanzaría a los datos utilizados para la identificación o autenticación mediante reconocimiento facial, de la palma de la mano u otros biométricos, incluyendo los códigos alfanuméricos generados cifrados o no o codificados con carácter irreversible o no. Dicha supresión no alcanza en cambio a los datos sobre día y hora de entrada y salida ni otros necesarios para el cumplimiento de las obligaciones y deberes laborales del responsable y el personal que no tengan carácter biométrico según se ha expuesto.

El artículo 5 RGPD en relación con los principios relativos al tratamiento establece que *"1.Los datos personales serán: a) tratados de manera lícita, leal y transparente en relación con el interesado."*

Por otro lado, el Considerando 39 RGPD expone que:

> *"Todo tratamiento de datos personales debe ser lícito y leal. Para las personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.[...]"*

Este Consejo considera, en el caso que nos ocupa, la supresión de los datos biométricos que debe efectuar el responsable es, en relación con los interesados, una información nueva y crucial respecto al tratamiento de sus datos biométricos. Por consiguiente, los principios de lealtad y transparencia y de responsabilidad

proactiva demostrable exigen que una vez suprimidos esos datos se comunique por el responsable dicha supresión a cada una de las persona afectadas.

c) Por otro lado, actividad de tratamiento "Servicio de personal"[8] del Inventario de Actividades de Tratamiento de la Diputación de Sevilla y siguen apareciendo en el apartado "Datos personales requeridos para el tratamiento" los denominados "Datos de reconocimiento biométrico a efectos de autenticación del control de presencia de su personal."

Por consiguiente, respecto a las medidas adoptar procede:

a) Ordenar a la Diputación Provincial de Sevilla que, de conformidad con el artículo 58.2.d) y g) RGPD y de acuerdo con el principio de transparencia recogido en el artículo 5.1.a) RGPD proceda, en el plazo de un mes a comunicar individualmente a todas las personas afectadas, trabajen actualmente o no en la Diputación Provincial de Sevilla, que se ha efectuado la mencionada supresión de sus datos biométricos de reconocimiento facial y de palma de la mano. Para acreditar el cumplimiento de esta medida la Diputación Provincial de Sevilla debe remitir al Consejo, en el plazo máximo de un mes tras la notificación de la resolución definitiva, la documentación acreditativa de haber efectuado dichas comunicaciones.

a) Ordenar a la Diputación Provincial de Sevilla que, de conformidad con el artículo 58.2.d) RGPD que, en el plazo de un mes a corregir las menciones hechas a "Datos de reconocimiento biométrico a efectos de autenticación del control de presencia de su personal." y que remita a este Consejo, en idéntico plazo, la documentación acreditativa de haber efectuado dichas correcciones.

En virtud de todo lo expuesto, el director del Consejo de Transparencia y Protección de Datos de Andalucía dicta la siguiente,

RESOLUCIÓN

Primero. Declarar la infracción responsabilidad de la Diputación Provincial de Sevilla con CIF *[NNNNN]*, por la comisión de las siguientes infracciones:

- Infracción tipificada en el art. 83.5. a RGPD y calificada a efectos de prescripción como muy grave en el artículo 72.1.e) LOPDGDD por vulneración sustancial del articulo 9 RGPD referido a el tratamiento de categorías especiales de datos en relación con la implantación de un sistema de control horario por datos biométricos (reconocimiento facial y de palma de la mano).

- Infracción tipificada el artículo 83.4.a RGPD y calificada a efectos de prescripción como grave en el artículo 73.t) LOPDGDD por vulneración sustancial del artículo 35 RGPD referido a la evaluación de impacto relativa a la protección de datos en relación el tratamiento de datos antes de llevar a cabo una evaluación de impacto relativa a la protección de datos cuando ésta era exigible.

Segundo. Ordenar a la Diputación Provincial de Sevilla en relación con las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido, que procede:

8 https://protecciondatos.dipusevilla.es/fichaactividad/9

a) Ordenar a la Diputación Provincial de Sevilla que, de conformidad con el artículo 58.2.d) y g) RGPD y de acuerdo con el principio de transparencia recogido en el artículo 5.1.a) RGPD proceda, en el plazo de un mes a comunicar individualmente a todas las personas afectadas, trabajen actualmente o no en la Diputación Provincial de Sevilla, que se ha efectuado la mencionada supresión de sus datos biométricos de reconocimiento facial y de palma de la mano. Para acreditar el cumplimiento de esta medida la Diputación Provincial de Sevilla debe remitir al Consejo, en el plazo máximo de un mes tras la notificación de la resolución definitiva, la documentación acreditativa de haber efectuado dichas comunicaciones.

b) Ordenar a la Diputación Provincial de Sevilla que, de conformidad con el artículo 58.2.d) RGPD que, en el plazo de un mes a corregir las menciones hechas a "Datos de reconocimiento biométrico a efectos de autenticación del control de presencia de su personal " en el registro de actividades de tratamiento y que remita a este Consejo, en idéntico plazo, la documentación acreditativa de haber efectuado dichas correcciones.

Tercero. Que se notifique la presente resolución al órgano infractor.

Cuarto. Que se comunique la presente resolución al Defensor del Pueblo Andaluz, de conformidad con lo establecido en el artículo 77.5 LOPDGDD.

En consonancia con lo establecido en el artículo 50 LOPDGDD, la presente Resolución se hará pública, disociando los datos que corresponda, una vez haya sido notificada a los interesados.

El incumplimiento de esta resolución podría comportar la comisión de la infracción considerada en el artículo 72.1.m) LOPDGDD, sancionable de acuerdo con el artículo 58.2 RGPD.

Contra esta Resolución, que pone fin a la vía administrativa, cabe interponer recurso potestativo de reposición ante este Consejo, en el plazo de un mes, o interponer directamente recurso contencioso-administrativo ante el Juzgado de lo Contencioso Administrativo de Sevilla que por turno corresponda, en el plazo de dos meses, en ambos casos a contar desde el día siguiente al de su notificación, de conformidad con lo dispuesto en los artículos 30.4, 123 y 124 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas y en los artículos 8.3 y 46.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

No obstante, al tratarse de un acto en materia de sanciones, el demandante podrá elegir alternativamente interponer el citado recurso contencioso-administrativo ante el juzgado o el tribunal en cuya circunscripción tenga aquél su domicilio, siempre entendiendo esta elección limitada a la circunscripción del Tribunal Superior de Justicia de Andalucía, de conformidad con lo dispuesto en los apartados segundo y tercero del artículo 14.1 de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa.

Conforme a lo previsto en el art. 90.3.a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta ante este Consejo su intención de interponer recurso contencioso-administrativo y traslada al mismo, una vez interpuesto, la documentación que acredite su presentación. Si el Consejo no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo correspondiente o en dicho recurso no se solicitara la suspensión cautelar de la resolución, se daría por finalizada la mencionada suspensión.

EL DIRECTOR DEL CONSEJO DE TRANSPARENCIA Y PROTECCIÓN DE DATOS DE ANDALUCÍA

JESÚS JIMÉNEZ LÓPEZ