- **Expediente Nº: EXP202304834**

RESOLUCIÓN DE TERMINACIÓN DEL PROCEDIMIENTO POR PAGO VOLUNTARIO

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

ANTECEDENTES

PRIMERO: Con fecha 30 de octubre de 2024, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a ***COLEGIO NOTARIAL DE ARAGÓN*** (en adelante, la parte reclamada), mediante el Acuerdo que se transcribe:

<<

- **Expediente N.º: EXP202304834**

ACUERDO DE INICIO DE PROCEDIMIENTO SANCIONADOR

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

HECHOS

PRIMERO: ***A.A.A.*** (en adelante, ***A.A.A.*** o parte reclamante) con fecha 7 de marzo de 2023 interpuso reclamación ante la Agencia Española de Protección de Datos por una posible infracción del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de datos, RGPD) imputable al ***COLEGIO NOTARIAL DE ARAGÓN*** con NIF ***Q5063003G*** (en adelante, ***COLEGIO NOTARIAL DE ARAGÓN*** o parte reclamada).

Los hechos que se pone en conocimiento a través de la reclamación son los siguientes:

El reclamante, ******PUESTO.1***, manifiesta que el 14/02/2023 se ha implantado un sistema de control horario mediante huella dactilar que no es conforme a la normativa de protección de datos, al no haberse efectuado una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Añade que cada trabajador debe marcarlo en todas las entradas y salidas del Colegio y no sólo las que se produzcan al comienzo y final de la jornada laboral y que, adicionalmente y cada viernes, los trabajadores deben enviar un informe del cumplimiento de los horarios,

con indicación de la hora de entrada y salida, a la dirección de correo de la Junta Directiva (***…***)

La parte reclamante manifiesta que la implantación del sistema es incorrecta, ya que no está basado en un sistema de almacenamiento descentralizado donde la huella dactilar recogida se incorpore a una tarjeta inteligente en poder del empleado.

Por otro lado, indica que, además de instalar el sistema referido, se han instalado cámaras de videovigilancia en zonas de uso exclusivo de los trabajadores.

SEGUNDO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación a ***COLEGIO NOTARIAL DE ARAGÓN***, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

El traslado, que se practicó conforme a las normas establecidas en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), fue recogido en fecha 21/04/2023, como consta en el acuse de recibo que obra en el expediente.
TERCERO: Con fecha 19/05/2023 tuvo entrada escrito de la Agencia Notarial de Certificación, S.L.U. (ANCERT), actuando en su condición de Delegado de Protección de Datos (DPD) de la parte reclamada, con el que daba respuesta a las cuestiones planteadas en el traslado de la reclamación y en el que se señala, resumidamente, lo siguiente:

- *El Colegio es una Corporación de Derecho público amparada por la Ley y reconocida por el Estado, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines, el cual tiene actualmente once empleados (aunque a fecha 14 de febrero dos de ellos se encontraban en situación de baja laboral.*

- Confirma que *es cierto que para controlar el horario de la asistencia y acceso de sus empleados a dichas dependencias recientemente dicho Colegio ha implantado un sistema de gestión del control horario mediante un sistema electrónico basado en la huella dactilar digitalizada, gestionado con el correspondiente software instalado en el servidor del Colegio, con la finalidad de dar cumplimiento al Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo*. Señala no obstante que el sistema todavía no emite correctamente los correspondientes informes sobre la recogida diaria por el lector de los datos horarios de los empleados.

- En la fecha señalada por el reclamante, *lo que se hizo fue acordar por la Junta-Directiva la necesidad de implantar dicho sistema y que, realmente, éste se comenzó a implementar en los días posteriores.*

- Califica de *manifiestamente falsa la afirmación de que el Colegio ha instalado cámaras de videovigilancia en zonas uso exclusivo de los trabajadores, pues únicamente existen dos cámaras instaladas, ubicadas en cada una de las dos puertas de acceso a las dependencias del mismo (una, ubicada en el acceso principal al*

Colegio y la otra instalada en la acceso por puerta lateral o de acceso a almacén) y otras dos en el acceso de la sala de "Archivo Histórico de Protocolos" en la primera planta del Colegio, todas ellas con fines de vigilancia y seguridad.

- En lo que respecta al informe semanal al que se refiere la reclamación, afirma que *el Colegio exigió el día 15 de febrero, en un comunicado, realizar dicho "informe del cumplimiento de los horarios, con indicación de la hora de entrada y salida de cada persona empleada", pero no a los empleados, sino al Oficial Mayor del Colegio, como medida temporal hasta que el sistema estuviera en funcionamiento, que sigue vigente porque todavía a fecha actual no está funcionando adecuadamente*. Dicho documento semanal *no es en verdad un registro manual de los horarios de entrada de los empleados, sino que únicamente anota cualquier hecho especialmente relevante o excepcional ocurrido durante la semana en relación a los horarios de los empleados (por ejemplo, un retraso no justificado, un solicitud de permiso especial para ausentarse, etc.), y lo remite a dicho correo electrónico*.

- El Colegio, en la toma de decisión previa de la instalación del sistema biométrico, sí tuvo en cuenta el impacto de la privacidad en los sistemas biométricos de control de acceso y horario laboral en los trabajadores, pues sí había llevado a cabo la correspondiente y obligatoria evaluación de impacto de protección de datos de dicho tratamiento, en su calidad de responsable del tratamiento.

- Desde el mismo momento de llevarse a cabo el tratamiento de datos biométricos, el Colegio había actualizado su Registro de Actividades de Tratamientos.

- Rechaza haber cometido alguna irregularidad y afirma que, si bien *es cierto que con anterioridad a la instalación de dicho sistema y también del Real Decreto-Ley 8/2019, el control horario de los empleados se había llevado a cabo manualmente mediante una hoja de papel en la que los empleados diariamente anotaban sus horas de entrada y salida de las oficinas, (…) dicho sistema de registro se consideró que no era objetivo y fiable como prueba acreditativa de los registros horarios, y por ello se implantó otro sistema más seguro que evitara cualquier posibilidad de subjetividad y arbitrariedad de los registros anotados en aras al estricto cumplimiento de la jornada laboral de los empleados*.

La parte reclamada considera que la reclamación presentada debiera ser inadmitida al carecer manifiestamente de fundamento y, por lo tanto, encontrarse entre los supuestos para la inadmisión a trámite de una reclamación previstos en el artículo 65.2 de la LOPDGDD. Y ello con base en los siguientes argumentos:

- Considera que el tratamiento de los datos biométricos está legitimado por el artículo 34.9 del Estatuto de los Trabajadores (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), en la redacción dada por el Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

- El Colegio llevó a cabo la correspondiente evaluación de impacto en la protección de datos (EIPD) incluyendo un análisis de la gestión de riesgos y la ponderación de los derechos concurrentes en los juicios de necesidad, idoneidad y proporcionalidad, emitiendo el correspondiente informe en fecha 6/2/2023 en el que se adoptaba la decisión favorable para la realización del tratamiento.

- Una vez adoptado el acuerdo de instalación del sistema por la Junta directiva celebrada el día 14 de febrero, los empleados fueron informados, por medio de la persona que entonces ocupaba temporalmente el cargo de ***PUESTO.3, ***B.B.B.*** (a la que la Junta directiva previamente le había comunicado el acuerdo), de cómo debían utilizar dicho nuevo sistema implantado para la gestión del control de la asistencia y acceso laboral a las dependencias del Colegio, y facilitándoles la información exigida por el artículo 13 del Reglamento general de protección de datos y el artículo 11 de la LOPDGDD.

- Se inició en los *posteriores días al referido 15 de febrero*, el proceso de configuración del sistema por parte del proveedor (grabación de huellas, horarios laborales para implementarlos en el sistema, etc.), *pero hasta la fecha, el sistema no ha estado operativo plenamente debido a diversas incidencias relacionadas con el software instalado y el servidor del propio Colegio*.

- Posteriormente, el día 22 de marzo, el Colegio volvió a facilitar información a los empleados que se encontraban en el mismo en dicho momento, pero esta vez por escrito. Se afirma que ninguno de los empleados del Colegio, desde el mismo 14/02/2023 hasta la fecha, ha ejercido ningún derecho de los regulados en los artículos 15 a 22 del RGPD, ni siquiera el de oposición a facilitar los datos biométricos.

- Desde el mismo momento de llevarse a cabo el tratamiento de datos biométricos el Colegio procedió a actualizar su Registro de Actividades de Tratamientos, que se encuentra publicado en su página web: https://aragon.notariado.org/portal/documents/1245687/1245718/Registro+de+ Actividades+ de+Tratamiento.pdf/e84343d3-0edb-e52d-e531-15f716ce135b?t=1629800170472).

- Señala que la STS de 2 de julio de 2007 (Rec. 5017/2003), ha entendido legitimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores. Y en el caso del Colegio Notarial se da la circunstancia de que la implantación del sistema de lectura de huella en el mismo está *especialmente justificada* porque los miembros de la Junta Directiva del Colegio, compuesta por nueve Notarios, cumplen sus jornadas de trabajo, no en el Colegio, sino en sus propias Notarías situadas en cualquier población de la Comunidad Autónoma de Aragón, y por ello no pueden ejercer *in situ* las funciones legales de control laboral al no cumplir su jornada laboral en el mismo.

- Considera que el tratamiento es conforme con la normativa en materia de protección de datos personales por cuanto:

  - El trabajador ha sido informado
  - Se respetan los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos. Insiste en que la finalidad del tratamiento es dar cumplimiento al Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, que únicamente se tratan los datos biométricos estrictamente necesarios para cumplir con la finalidad prevista por la normativa laboral aplicable para el control horario del acceso al Colegio por sus empleados (principio de minimización). En cuanto al principio de idoneidad, señala que el tratamiento de datos biométricos permite cumplir, con garantías de seguridad, las obligaciones del Colegio de la gestión laboral del control horario de la asistencia y acceso de sus empleados a las dependencias del mismo con la finalidad de dar cumplimiento al Real Decreto-Ley 8/2019, por lo que se considera que la medida es idónea. En lo que respecta al principio de necesidad indica que la necesidad del tratamiento por el Colegio se ampara en su obligación de asegurar y minimizar los riesgos de seguridad y fiabilidad en el registro horario de sus empleados, en base a su responsabilidad y obligación establecida por el Estatuto de los Trabajadores. Además, en el caso del Colegio, reitera la especial necesidad de la implantación del sistema de lectura de huella en el mismo también está justificada porque los miembros de la Junta Directiva del Colegio cumplen sus jornadas de trabajo, no en el Colegio, sino en sus propias Notarías situadas en cualquier población de la Comunidad Autónoma de Aragón, no pudiendo comprobar *in situ* el cumplimiento de las jornadas horarias en el Colegio. En lo relativo al principio de proporcionalidad, señala que *el Colegio ha analizado la aplicación de otras medidas de control horario de los empleados que pudieran minimizar los riesgos para los derechos y libertades de los empleados utilizando sistemas no biométricos, como por ejemplo el uso de tarjetas o aplicaciones mediante códigos alfanuméricos personales o contraseñas, constatando que estos no asegurarían al Colegio una comprobación segura y fiable de la identificación y autenticación unívoca de los usuarios porque permitirían ser fácilmente intercambiados*. *Por ello, ante la imposibilidad de aplicar otras medidas menos intrusivas que puedan proporcionar el mismo grado de efectividad, se puede afirmar que el tratamiento que se realiza mediante la utilización de sistemas de comprobación de las huellas dactilares de los empleados del Colegio*.

    Indican que se ha llevado a cabo una ponderación de los derechos en conflicto *por un lado, el derecho a la protección de datos, y por otro el derecho a las facultades de control laboral del Colegio establecidas por la normativa laboral -en concreto el art. 20.3 del Estatuto de los Trabajadores* (…) *considerando que prevalecen en todo momento el derecho al control laboral sobre el de protección de datos, sin perjuicio de que es imprescindible la aplicación de las garantías adecuadas de protección de datos, pues el RGPD requiere también en estos casos que la norma que permita este tratamiento ha de establecer también dichas garantías*.

- *Como se acredita y certifica la empresa instaladora, en el sistema instalado por el Colegio los datos biométricos se almacenan como plantillas biométricas. Es decir, el software de gestión del sistema almacena el hash (patrón o plantilla biométrica) que proporciona el terminal de huella dactilar, el cual se relaciona con el usuario final con el id de usuario del empleado en una tabla para los datos biométricos. El sistema biométrico utiliza dichos mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de los datos biométricos. Así, el sistema de huella dactilar asegura que sea imposible obtener la imagen real de la huella dactilar con el patrón guardado en el lector del terminal, ya que no se efectúa ninguna fotografía digital de la huella, sino que se establece una relación matemática entre determinados puntos de la misma (singularidades, puntos característicos o 'minucias') dando lugar a un conjunto de números que sirve después para identificar de manera inequívoca a cada persona. Por tanto, el sistema utilizado es adecuadamente fiable, al realizarse la captación de la huella digital, por parte del lector del terminal, mediante una lectura óptica de las singularidades (por ejemplo, un surco que se bifurca en dos, el núcleo de la huella, surcos formando una 'delta', etc...) presentes en la superficie de la huella. Dichos puntos singulares son relacionados entre sí a través de un algoritmo matemático de encriptación, generándose una plantilla de un número de bytes representativo de dicha huella. La característica de los sistemas biométricos está en asegurar la no aceptación de una muestra errónea (FAR- False Acceptance Rate) más que en la no aceptación de una muestra correcta (FRR- False Rejection Rate). Por lo tanto, descartando la posibilidad de la falsificación de una huella dactilar, la posibilidad de la aceptación de una huella no válida es un valor lo suficientemente bajo como para que sea más que razonablemente aceptable. Los datos biométricos se almacenan en la base de datos propia del software de control horario ubicada en un servidor en las instalaciones del Colegio así como en el terminal.*
- *El sistema biométrico del Colegio y las medidas de seguridad elegidas aseguran de que no es posible la reutilización de los datos biométricos para otra finalidad*.
- *El sistema biométrico del Colegio utiliza mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de los datos biométricos.*
- *El sistema biométrico está diseñado de modo que el Colegio puede revocar en cualquier momento el vínculo de identidad entre la plantilla generada y el empleado, en el caso, por ejemplo, de que un empleado cause baja en el Colegio*.
- *La tecnología específica utilizada por el sistema imposibilita dicha interconexión de la base de datos biométricos, pues estos se almacenan en el terminal y el servidor del Colegio, imposibilitando igualmente la divulgación de los datos*.
- *Los datos biométricos de los empleados del Colegio serán suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento conforme a la normativa laboral aplicable para el control horario del acceso al Colegio por sus empleados. Y así mismo serán objeto de tratamiento durante el*

tiempo requerido por la dicha normativa laboral, la cual establece que los registros deben conservarse durante cuatro años.

En lo que respecta a la base jurídica del tratamiento de datos personales, considera que el tratamiento de los datos biométricos (huella dactilar digitalizada o plantilla) tiene como base de legitimación los artículos 6.1.b) y 9.1 y 9.2b) del RGPD, en relación con el artículo 20 y 34 del Estatuto de los Trabajadores (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) y el Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

En cuanto a la finalidad del tratamiento, afirma que es la gestión del control de la asistencia y acceso laboral de sus trabajadores a las dependencias del Colegio Notarial de Aragón mediante huella dactilar digitalizada con la finalidad de dar cumplimiento al Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo. Se informa igualmente que *en caso de no facilitarse los referidos datos biométricos, esta circunstancia implica la imposibilidad de acceder a las dependencias del Colegio Notarial de Aragón*.

Entiende que las garantías del sistema implantado son las adecuadas, dado que los datos biométricos se almacenan como plantillas biométricas y reitera las características del sistema ya apuntadas anteriormente.

En lo que respecta a las categorías de interesados, confirma que son los trabajadores del Colegio y la información facilitada a éstos sobre el tratamiento de los datos es la siguiente:

- Información sobre la implantación del sistema de gestión del control de la asistencia y acceso laboral con la finalidad de cumplir con el Real Decreto-Ley 8/2029, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

- Se proporciona la información a la que se refiere el artículo 13 RGPD: responsable del tratamiento, legitimación, finalidad del tratamiento, posibles destinatarios de los datos, plazo de conservación y datos del delegado de protección de datos.

Señala asimismo que *habida cuenta de que esta es un proceso continuado, el Colegio ha establecido responsabilidades para la implementación de las medidas dentro de un plan de acción, realizándose controles periódicos hasta su implantación total, siendo el* ******PUESTO.2, C.C.C.****, la persona que la Junta Directiva del Colegio ha designado para asumir dichas responsabilidades en relación al sistema biométrico, de la cual es censor tercero. También hay que considerar, como se indica en dicho informe, que en el caso de que se produzcan cambios sustanciales en el tratamiento analizado a nivel técnico u organizativo se deberá proceder a revisar la EIPD o realizar una nueva EIPD si así corresponde*.

En relación con lo planteado por el reclamante respecto de la instalación de cámaras de videovigilancia en zonas de uso exclusivo de los trabajadores, rechaza dicha afirmación y señala que las cámaras han sido instaladas exclusivamente para vigilancia con la finalidad de preservar la seguridad de las personas y bienes, así como de sus instalaciones. Rechaza que las imágenes obtenidas sean utilizadas para el ejercicio de las funciones de control de los trabajadores, y que se hayan instalado sistemas de grabación de sonidos o de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos.

Confirma que únicamente existen dos cámaras de grabación de imágenes (no de sonido) instaladas, ubicadas en cada una de las dos puertas de acceso a las dependencias del mismo (una, ubicada en el acceso principal al Colegio y la otra instalada en el acceso por puerta lateral o de acceso a almacén) y otras dos cámaras en el acceso de la sala de “Archivo Histórico de Protocolos” en la primera planta del Colegio. En todos los cuatro casos se han colocado en las zonas videovigiladas donde se instalaron las cámaras los correspondientes carteles informativos con el fin de cumplir con el deber de información previsto en el artículo 12 del RGPD colocados en el mismo lado de las puertas y, por tanto, suficientemente visibles identificando, al menos, la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los artículos 15 a 22 del RGPD.

Indican que la instalación de las videocámaras ubicadas en el acceso principal y lateral del Colegio trae su causa en razones de estricta seguridad habiéndose valorado reiteradamente por la Junta directiva su instalación tras haberse producido ***(…)*** y con una finalidad claramente disuasoria.

Junto a dicho escrito, se aportó la siguiente documentación:

- Informe de evaluación de impacto en la protección de datos (EIPD) respecto al tratamiento de datos de datos biométricos mediante el uso de un sistema de control horario basado en huella dactilar del Ilustre Colegio Notarial de Aragón, fechado el 6/02/2023.

- Copia de los comunicados (un total de 9) dirigidos a los empleados con acuse de recibo en el que se incluye fecha, firma y DNI del receptor. En el escrito de respuesta a la actuación de traslado señala que eran 9 los empleados que en fecha 14 de febrero se encontraban en situación de alta laboral y dos en situación de baja laboral, situación que continúa en el momento en que se dirigió escrito de respuesta. Este hecho motiva, según indican, que en ese momento no habían recibido dicho documento pues tampoco han sido grabadas sus huellas en el sistema.

- Certificado de la entidad ***EMPRESA.1, con ******NIF.1***, fechado el 17/05/2023 en el que se indica que

  (…) *el sistema de control de presencia instalado en el colegio notarial no almacena ninguna huella como tal, se transforma en un código binario que, a través de un algoritmo, transforma esa huella en un código sólo comprensible por el dispositivo instalado. Cada una de las máquinas utiliza un algoritmo distinto por lo que no se puede traslada de una a otra y ninguna almacena huellas. Para trasladar los datos hay plantillas que solo*

sabe interpretar el software del sistema de gestión de la marca. En caso de eliminar un usuario se eliminan todos sus datos y solo quedan guardados los fichajes tal y como indica la ley.

- Documento con un cartel informativo de zona videovigilada en el que se indica como responsable al Ilustre Colegio Notarial de Aragón, la dirección en la que se pueden ejercer los derechos de protección de datos, información sobre la legitimación del tratamiento- cumplimiento de misión de interés público-, su finalidad- garantizar la seguridad-, indicación de que las imágenes no se ceden a terceros, referencia a los derechos reconocidos en los artículos 13 a 22 del RGPD y de la posibilidad de reclamar ante la *AGPD* y plazo de conservación de las imágenes durante un máximo de 30 días.

TERCERO: Con fecha 7/06/2023, de conformidad con el artículo 65 de la LOPDGDD, se admitió a trámite la reclamación presentada por la parte reclamante.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos en cuestión, en virtud de las funciones asignadas a las autoridades de control en el artículo 57.1 y de los poderes otorgados en el artículo 58.1 del RGPD, y de conformidad con lo establecido en el Título VIII, de la LOPDGDD.

De las actuaciones previas de investigación practicadas, pueden destacarse los siguientes extremos:

En fecha 13 de noviembre de 2023 se solicita a la parte reclamada ampliación de la información y en fecha 13 de diciembre de 2023 tiene entrada su respuesta, en la que se indica lo siguiente:

> *En relación a la información solicitada relativa al sistema de gestión del control horario basado en la huella dactilar, y en concreto respecto al estado actual del sistema, debemos afirmar que este Colegio recientemente ha adoptado la decisión, con carácter definitivo, de no implantar dicho sistema como herramienta del control horario de sus empleados.*
>
> *Dicha decisión ha sido adoptada por las razones que a continuación se exponen. La primera de ellas es que, como ya indicó el delegado de protección de datos en fecha 18 de mayo de 2023* (en el marco del procedimiento AT/01887/2023)*, una vez instalado el correspondiente software del sistema en el servidor del Colegio, no funcionaba correctamente la parte fundamental de las funcionalidades previstas por el producto al no emitir el sistema los correspondientes informes sobre la recogida diaria por el lector de los datos horarios de los empleados, es decir, los informes sobre los horarios de entrada y salida de los empleados, que evidentemente eran la razón principal de dicho sistema. Y, en segundo lugar, la instalación de dicho software, además interfirió en el funcionamiento de otras aplicaciones ya instaladas en dicho servidor, por lo cual el Colegio procedió primero a inhabilitar el software y posteriormente desinstalarlo de dicho servidor, y por ello, ante tales dificultades tras unos meses de su puesta en funcionamiento, ha decidido, con carácter definitivo, no*

volver a implantar dicho sistema biométrico del control horario ni del proveedor del mismo ni de ningún otro.

Así, en fecha 1 de diciembre de 2023, a instancias de dicho Colegio, un empleado del proveedor e instalador del sistema se ha personado en el mismo y ha retirado el lector de huella de dicho sistema y ha procedido a desinstalar el referido software de gestión del sistema.

Se aporta como Doc. N 1 de la entrada con n.º de registro REGAGE23e00084469463 el parte de trabajo del proveedor e instalador del sistema que acredita que se desmonta el sistema y se desinstala el software de gestión.

Además, dicha entidad, a continuación, ha procedido a la destrucción de los códigos binarios utilizados como plantillas biométricas obtenidos de las huellas dactilares para la autenticación de los empleados del Colegio, los cuales estaban almacenados en dicho lector por el software de gestión de dicho sistema.

Se aporta como Doc. N 2 de la entrada REGAGE23e00084469463 el certificado emitido por el proveedor e instalador del sistema que acredita lo anterior.

Asimismo, el Colegio añade:

A dicha decisión ha contribuido también que la entidad a la que nos dirigimos, el pasado mes de noviembre, ha emitido la "GUÍA SOBRE TRATAMIENTOS DE CONTROL DE PRESENCIA MEDIANTE SISTEMAS BIOMÉTRICOS", que entre sus conclusiones, se indica que con relación al tratamiento de control de presencia mediante técnicas biométricas de identificación o autenticación, los responsables del tratamiento han de tener en cuenta que la utilización de tecnologías biométricas de identificación y autenticación en el control de presencia supone un tratamiento de alto riesgo que incluye categorías especiales de datos, y que en la implementación del tratamiento de control de presencia hay que cumplir los principios de minimización y de protección de datos desde el diseño y por defecto, utilizando las medidas alternativas equivalentes, menos intrusivas, y que traten los menos datos adicionales.

Por este motivo, en lo sucesivo, el Colegio ha decidido que utilizará un sistema de control horario menos intrusivo para la protección de datos que consistirá en un programa de software para ordenador que permitirá al empleado fichar, mediante un código numérico, una vez que inicie sesión con el correspondiente ordenador asignado a cada empleado.

Cámaras de videovigilancia

En relación con lo que la parte reclamante manifiesta en su reclamación: "*además de instalar cámaras de videovigilancia en zonas uso exclusivo de los trabajadores*", en el marco de las actuaciones de investigación, en fecha 31 de octubre de 2023, se le solicita a la parte reclamante la siguiente información al respecto:

- *Documentos gráficos recientes, debidamente fechados, que permitan apreciar que los dispositivos afectados están actualmente en funcionamiento, sus características y su ubicación concreta*.
- *Si no se ha colocado un dispositivo informativo, en lugar suficientemente visible, que identifique la existencia del tratamiento, la identidad del responsable y la posibilidad de ejercitar los derechos previstos en los*

artículos 15 a 22 del Reglamento (UE) 2016/679 o que incluya un código de conexión o dirección de internet a esta información, se deberán acompañar documentos gráficos recientes, debidamente fechados, que permitan confirmar su ausencia en el entorno de la instalación.

- *Copia del documento facilitado a los trabajadores informando de la política de control laboral a través de estos dispositivos, si aplica. Se acompañarán asimismo las pruebas documentales de que se disponga sobre el tratamiento de los datos de los trabajadores captados por las cámaras. Igualmente, se hará constar si en base a dichos tratamientos de datos se ha producido algún expediente sancionador/disciplinario o despido de un trabajador y referencia de los mismos.*

En fecha 10 de noviembre de 2023 tiene entrada en la sede electrónica de la Agencia la respuesta de la parte reclamante (entradas con n.º de registro REGAGE23e00076322973, REGAGE23e00076430979 y REGAGE23e00076418762):

- Se incluyen las siguientes fotografías:
  - (…)
- Se indica que hay dos carteles informativos, uno en la puerta de acceso general, la de cristal que se ve en el patio (fotografía 7461) y otro en la calle lateral por acceso de la fotografía 7457, puerta que se señala que "*rara vez se abre, una vez al año*".
- Por último, la parte reclamante señala que a los empleados del colegio no se les ha facilitado documento alguno que informe de la política de control laboral a través de estos dispositivos, que no dispone de pruebas documentales sobre el tratamiento de los datos de los trabajadores captados por las cámaras y que tampoco tienen acceso a las imágenes captadas.

Asimismo, en fecha 13 de noviembre de 2023 se solicita al Colegio información relativa a las cámaras de videovigilancia instaladas en el mismo. En fecha 13 de diciembre de 2023 tiene entrada la respuesta y a continuación, se reproduce el contenido más relevante:

- ***(…)***
- Se aporta como Doc. N 3 de la entrada con n.º de registro REGAGE23e00084469463 y Doc. N 4, Doc. N 5 y Doc. N 6 de la entrada con n.º de registro REGAGE23e00084470034 las fotografías de la instalación y colocación de cada una de las cámaras.

Se aporta como Doc. N 10 de la entrada con n.º de registro REGAGE23e00084470495 la fotografía del cartel informativo colocado en el acceso a la sala "Archivo Histórico de Protocolos", Doc. N 11 de la entrada con n.º de registro REGAGE23e00084470495, y en los accesos por la puerta principal y por la puerta lateral al Colegio.

Las cámaras se han instalado en el Colegio exclusivamente para la vigilancia con la finalidad de preservar la seguridad de las personas y los bienes, así como de sus instalaciones, pues en ningún caso el Colegio ha tratado las imágenes obtenidas para el ejercicio de las funciones de control de los trabajadores, ni tampoco se han instalado sistemas de grabación de sonidos ni

de videovigilancia en lugares destinados al descanso o esparcimiento de los trabajadores, tales como vestuarios, aseos, comedores y análogos. Pues es necesario volver a indicar que la decisión de la instalación de las videocámaras ubicadas en el acceso principal y lateral del Colegio trae su causa en razones de estricta seguridad habiéndose valorado por la Junta directiva su instalación tras haberse producido un acceso no autorizado de dos personas un sábado por la noche del mes de marzo de este año ***(…)****.*

Se aporta como Doc. N 7 de la entrada con n.º de registro REGAGE23e00084470034 el albarán de suministro de las cámaras 1 y 2 instaladas en las puertas de acceso principal y lateral al Colegio. ***(…)***.

Se aporta como Doc. N 8 de la entrada con n.º de registro REGAGE23e00084470495 las dos capturas de pantalla de las zonas que quedan dentro del campo de visión de las cámaras 1 y 2.

(…) *por haberse instalado el software suministrado por el instalador de las cámaras, pues la Junta directiva del Colegio ha delegado en dicha persona la responsabilidad de la gestión de cualquier asunto relacionado con las cámaras y es la única persona autorizada al acceso de las imágenes.*

[…] Como medida de seguridad, ***(…)****.*

Se aporta como Doc. N 9 de la entrada REGAGE23e00084470495 fotografía de dicha mesa y se señala que tanto los ciudadanos que solicitan servicios al Colegio como el resto de los puestos de trabajo de los empleados se encuentran fuera de dicho despacho, que son las dependencias del Colegio (zona de atención al público y zona de oficina).

En relación con el plazo de conservación de las imágenes registradas, se reitera que ***(…)*** y se indica que, transcurridos treinta días, como máximo, desde la fecha de la grabación de las imágenes, el software instalado las elimina automáticamente.

Por último, se indica que la visualización y/o grabación de las imágenes no se ha encargado a ningún tercero ajeno al Colegio, que el Colegio únicamente contrató a la empresa ******EMPRESA.1*** la instalación física de las cámaras 1 y 2, no existiendo ningún contrato de mantenimiento y/o gestión del sistema de videovigilancia ni con dicha empresa ni con ninguna otra.

Respecto a las cámaras 3 y 4, la parte reclamante manifiesta que fueron instaladas hace más de diez años y por ello, no se ha guardado documentación (facturas, albaranes, etc.) de dicha instalación no existiendo tampoco ningún contrato de mantenimiento y/o gestión de dichas cámaras de videovigilancia con ninguna empresa.

QUINTO: De acuerdo con el informe recogido de la herramienta AXESOR, y que consta como diligencia expedida en el presente expediente, la entidad ***COLEGIO NOTARIAL DE ARAGÓN*** tiene un volumen de ventas de 1.131.754 € y cuenta con 9 empleados.

FUNDAMENTOS DE DERECHO

I
Competencia
De acuerdo con los poderes que el artículo 58.2 del RGPD, otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la LOPDGDD, es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

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

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

Si en el plazo estipulado no efectuara alegaciones a este acuerdo de inicio, el mismo podrá ser considerado propuesta de resolución, según lo establecido en el artículo 64.2.f) de la LPACAP.

III
Cuestiones previas

Ha de comenzarse indicando que, de acuerdo con el art. 4.1 RGPD, se entiende por «datos personales: *toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona*;

Por su parte, el artículo 4.2. del RGPD define el tratamiento como "*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 atención a lo anterior, en el presente caso y de acuerdo con lo establecido en los artículos señalados, consta la realización de un tratamiento de datos personales por

parte del ***COLEGIO NOTARIAL DE ARAGÓN***, que se concreta en el tratamiento de datos personales de sus trabajadores- su huella dactilar- como medio de control del cumplimiento de su jornada laboral- control de la asistencia y acceso laboral a las dependencias del Colegio- durante el período transcurrido entre el 15 de febrero de 2023 y el 1 de diciembre de ese mismo año.

El ***COLEGIO NOTARIAL DE ARAGÓN*** realiza esta actividad de tratamiento de datos personales en su condición de responsable del tratamiento, dado que es quien determina los fines y medios de tal actividad, en virtud del artículo 4.7 del RGPD según el cual es «responsable del tratamiento» o «responsable»: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.*

Como continuación de lo indicado, y de acuerdo con el artículo 70 de la LOPDGDD

1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:

a) Los responsables de los tratamientos. (…)

Sentado lo anterior, hay que tener en cuenta que los Colegios Profesionales, son corporaciones de Derecho Público, amparadas por la Ley y reconocidas por el Estado, con personalidad jurídica propia y plena capacidad para el cumplimiento de sus fines.

La Constitución establece en sus artículos 36 y 52, las bases normativas por medio de las cuales se han de regular las Corporaciones de derecho público. Por su parte, la LPACAP, señala en su artículo 2.4, que las Corporaciones de derecho público *"…se regirán por su normativa específica en el ejercicio de las funciones públicas que les hayan sido atribuidas por Ley o delegadas por una Administración Pública, y supletoriamente por la presente Ley".*

También la ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, deja por sentado el carácter público que se reconoce a una Corporación de derecho público, así como el alcance de tal consideración, cuando establece en su artículo 2.c), que el orden jurisdiccional contencioso-administrativo conocerá de las cuestiones que se susciten en relación con *"Los actos y disposiciones de las Corporaciones de Derecho público, adoptados en el ejercicio de las funciones públicas".*

Así, a pesar de calificarse como Corporación de *Derecho Público*, es necesario tener presente que, de igual forma que dichas entidades tienen atribuido el ejercicio de funciones públicas- a las que se refiere la normativa señalada con anterioridad- pueden ejercitar también funciones de naturaleza jurídico-privada, a las que se les aplica un régimen jurídico que tiene en cuenta la naturaleza privada- y no derivada del ejercicio de funciones públicas- de su actuación.

En definitiva, las Corporaciones de Derecho Público- entre las que se encuentra la parte reclamada, en su condición de Colegio Profesional, en este caso, Notarial- tienen una naturaleza mixta que implica que, si bien desarrollan funciones públicas, también llevan a cabo actividades y prestan servicios en régimen de derecho privado. Por ello, el régimen jurídico de estas organizaciones es necesariamente complejo, puesto que carece de uniformidad y ha de adaptarse a la naturaleza (pública o privada) de la actividad que lleve a cabo en cada momento. No obstante, puede señalarse que las funciones públicas a ejercer por los Colegios Profesionales son, esencialmente la ordenación del ejercicio profesional, que incluye el ejercicio de la potestad sancionadora y el control del cumplimiento de las normas deontológicas.

Por lo tanto, aplicado lo anterior y en lo que respecta a los hechos planteados en la reclamación presentada y de los que trae causa el presente acuerdo de inicio de procedimiento sancionador, cabe concluir que nos encontramos ante una actuación realizada por la parte reclamada de naturaleza privada.

IV
Datos biométricos y plantillas biométricas como categorías especiales de datos

El apartado 14 del artículo 4 del RGPD define datos biométricos como *datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos*;

En el caso que nos ocupa, afirma la parte reclamada que *en el sistema instalado por el Colegio los datos biométricos se almacenan como plantillas biométricas. El sistema biométrico utiliza dichos mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de los datos biométricos. Así, el sistema de huella dactilar asegura que sea imposible obtener la imagen real de la huella dactilar con el patrón guardado en el lector del terminal, ya que no se efectúa ninguna fotografía digital de la huella, sino que se establece una relación matemática entre determinados puntos de la misma (singularidades, puntos característicos o 'minucias') dando lugar a un conjunto de números que sirve después para identificar de manera inequívoca a cada persona.*
En este punto, ha de recordarse que la finalidad del tratamiento, según indica la parte reclamada, es la identificación del trabajador, al objeto de controlar el acceso a las dependencias donde desarrolla su jornada laboral y, por lo tanto, el cumplimiento de la misma. También, que la parte reclamada, al describir el sistema, confirma que sirve *para identificar de manera inequívoca a cada persona.* Por lo tanto, ha de concluirse que nos encontramos ante un tratamiento de datos de carácter personal de acuerdo con la definición antes transcrita del artículo 4.1 del RGPD.
Ha de señalarse, por otro lado, que el proceso de identificación incluye necesariamente la realización de varias operaciones de tratamiento (recogida o captura de datos, registro, almacenamiento, procesamiento, comparación, autenticación, conservación, supresión, limitación…etc)
De acuerdo con la definición dada por el artículo 4.14 del RGPD, los datos biométricos tratados se consideran datos de carácter personal siempre y cuando la finalidad del

tratamiento sea la identificación o autenticación de una persona- *que permitan o confirmen la identificación única de dicha persona*-, en el sentido previsto en el artículo 4.1 del RGPD; circunstancia que, como ya hemos señalado, se da en el presente supuesto.

Como ya señaló el Dictamen 4/2007 del Grupo de Trabajo del artículo 29, sobre el concepto de datos personales (WP136), de 20/06/2007, los datos biométricos pueden definirse como:

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

En el caso de las plantillas biométricas que se generan en el sistema instalado por el Consejo- *Es decir, el software de gestión del sistema almacena el hash (patrón o plantilla biométrica) que proporciona el terminal de huella dactilar, el cual se relaciona con el usuario final con el id de usuario del empleado en una tabla para los datos biométricos*- las mismas constituyen datos de carácter personal dado que el proceso se basa en asignar un identificador (la plantilla biométrica obtenida al recoger las muestras de huella dactilar de los trabajadores en el momento en que se produzca su acceso a las dependencias de la parte reclamada) que permite singularizar a un individuo- el trabajador- y, distinguirlo frente a otros, a través de "*elementos propios de la identidad física, fisiológica, genética, psíquica*", gracias a su cotejo con la muestra previamente guardada.

Es decir, una plantilla biométrica es una forma de escritura de una característica biométrica humana- en este caso, una huella dactilar- de manera que sea interpretable por una máquina de forma eficiente y eficaz para un propósito o propósitos determinados- en el caso que nos ocupa, el sistema de acceso instalado y el software que permite la identificación de la persona física cuya plantilla biométrica con el trabajador cuya huella dactilar ha sido previamente instalada en el sistema-.

Los sistemas biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación. Así, cada individuo tiene impresiones dactilares únicas que muestran características específicas que pueden medirse para decidir si una impresión dactilar se corresponde con una muestra registrada. Por lo tanto, son únicos, permanentes o definitivos en el tiempo, ya que permanecen invariablemente unidos a una persona. Debido a sus

especiales características, puede afirmarse que, cuando son comprometidos, estos datos tienen un impacto más significativo en el derecho fundamental a la protección de datos de su titular en comparación con otro tipo de datos personales. De ahí la especial relevancia que ha otorgarse a las garantías que se adopten en su tratamiento debido que la incidencia, especialmente significativa, en el derecho fundamental a la protección de datos personales de su titular.

Es desde esta perspectiva que se pronuncia el RGPD en su considerando 51, en el que afirma lo siguiente:

> *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. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, entendiéndose que el uso del término «origen racial» en el presente Reglamento no implica la aceptación por parte de la Unión de teorías que traten de determinar la existencia de razas humanas separadas. 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. Se deben establecer de forma explícita excepciones a la prohibición general de tratamiento de esas categorías especiales de datos personales, entre otras cosas cuando el interesado dé su consentimiento explícito o tratándose de necesidades específicas, en particular cuando el tratamiento sea realizado en el marco de actividades legítimas por determinadas asociaciones o fundaciones cuyo objetivo sea permitir el ejercicio de las libertades fundamentales.*

Por su parte, el artículo 9 del RGPD define las categorías especiales de datos como (…) *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*.

Así, cabe recordar que, i) al definir los datos biométricos, el artículo 4.14 RGPD se refiere a datos que *"permitan o confirmen la identificación única"* ii) que el artículo 9, a la hora de calificar como categoría especial de datos personales a los datos biométricos, establece como única "condición" que tengan como objetivo la identificación unívoca de una persona física y iii) que la confirmación de la identidad de un individuo se da tanto en los supuestos de identificación como de autenticación. Por lo tanto, ha concluirse que el tratamiento de datos biométricos constituye un

tratamiento de categorías especiales de datos. Una conclusión que ha sido incorporada por el Comité Europeo de Protección de Datos (CEPD) en sus Directrices 5/2022 sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley y por la propia AEPD en la guía sobre tratamientos de control de presencia mediante sistemas biométricos mencionada por la parte reclamada.

A este respecto, destacamos que el Tribunal de Justicia de la Unión Europea (TJUE), en su sentencia de 1 de agosto de 2022, en el asunto, C-184/20, fija una interpretación amplia del concepto categorías especiales de datos personales (el subrayado es nuestro):

> *125 Además, una interpretación amplia de los conceptos de «categorías especiales de datos personales» y de «datos sensibles» se ve respaldada por el objetivo de la Directiva 95/46 y del RGPD, a que se ha hecho mención en el apartado 61 de la presente sentencia, de asegurar un alto nivel de protección de las libertades y de los derechos fundamentales de las personas físicas, en particular, de su intimidad, en relación con el tratamiento de los datos personales que las afectan (véase, en este sentido, la sentencia de 6 de noviembre de 2003, Lindqvist, C-101/01, EU:C:2003:596, apartado 50).*
>
> *126 Más aún, la interpretación contraria se opondría a la finalidad del artículo 8, apartado 1, de la Directiva 95/46 y del artículo 9, apartado 1, del RGPD, que consiste en garantizar una mayor protección frente a tales tratamientos, que, en atención a la particular sensibilidad de los datos objeto de ellos, pueden constituir, como se desprende del considerando 33 de la Directiva 95/46 y del considerando 51 del RGPD, una injerencia especialmente grave en los derechos fundamentales al respeto de la vida privada y a la protección de los datos personales, garantizados por los artículos 7 y 8 de la Carta [véase, en este sentido, la sentencia de 24 de septiembre de 2019, GC y otros (Retirada de enlaces a datos sensibles), C-136/17, EU:C:2019:773, apartado 44]".*

Ha de concluirse, por lo tanto, que, en el caso analizado en el presente acuerdo de inicio de procedimiento sancionador, nos encontramos ante el tratamiento de una categoría especial datos personales- biométricos- del que es responsable la parte reclamada tal y como se ha argumentado con anterioridad.

V

Condiciones para el tratamiento de categorías especiales de datos

El artículo 9 del RGPD antes mencionado, al definir las categorías especiales de datos, parte del principio general de prohibición de su tratamiento

> *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*.

La prohibición de tratamiento que se aplica a las categorías especiales de datos se establece con carácter general, y a salvo de que pueda ser de aplicación algunas de las circunstancias previstas en el apartado 2 de dicho precepto (el subrayado es nuestro):

> *2. El apartado 1 no será de aplicación cuando concurra una de las circunstancias siguientes:*

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;
c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional,
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo

esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado. (…)

De acuerdo con lo manifestado por la parte reclamada, ésta considera que el tratamiento de las huellas dactilares de sus empleados con fines de control laboral se encuentra amparado en la letra b del artículo 9.2 antes transcrito, y ello en el marco de las obligaciones de registro de la jornada laboral que se derivan de los artículos 20 y 34 del Estatuto de los Trabajadores, adoptado por el Real Decreto Legislativo 2/2015, de 23 de octubre, en su redacción dada Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo. Dichos preceptos, en lo que aquí interesa, se pronuncian en los siguientes términos:

Artículo 20. Dirección y control de la actividad laboral.

1. El trabajador estará obligado a realizar el trabajo convenido bajo la dirección del empresario o persona en quien este delegue.

2. En el cumplimiento de la obligación de trabajar asumida en el contrato, el trabajador debe al empresario la diligencia y la colaboración en el trabajo que marquen las disposiciones legales, los convenios colectivos y las órdenes o instrucciones adoptadas por aquel en el ejercicio regular de sus facultades de dirección y, en su defecto, por los usos y costumbres. En cualquier caso, el trabajador y el empresario se someterán en sus prestaciones recíprocas a las exigencias de la buena fe.

3. El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad.

4. El empresario podrá verificar el estado de salud del trabajador que sea alegado por este para justificar sus faltas de asistencia al trabajo, mediante reconocimiento a cargo de personal médico. La negativa del trabajador a dichos reconocimientos podrá determinar la suspensión de los derechos económicos que pudieran existir a cargo del empresario por dichas situaciones.

Artículo 34. Jornada.

(…)

9. La empresa garantizará el registro diario de jornada, que deberá incluir el horario concreto de inicio y finalización de la jornada de trabajo de cada persona trabajadora, sin perjuicio de la flexibilidad horaria que se establece en este artículo.

Mediante negociación colectiva o acuerdo de empresa o, en su defecto, decisión del empresario previa consulta con los representantes legales de los trabajadores en la empresa, se organizará y documentará este registro de jornada.

La empresa conservará los registros a que se refiere este precepto durante cuatro años y permanecerán a disposición de las personas trabajadoras, de sus representantes legales y de la Inspección de Trabajo y Seguridad Social.

Analizando los preceptos señalados, debemos indicar los términos en los que se pronuncia el art. 9.2 b) del RGPD a la hora de prever la circunstancia descrita y que permitiría el levantamiento de la prohibición de tratar categorías especiales de datos:

1. El tratamiento ha de ser <u>necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del</u>

interesado en el ámbito del Derecho laboral y de la seguridad y protección social

2. El tratamiento ha de ser autorizado – *en la medida en que así lo autorice*- por el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros
3. El instrumento a través del cual se articule dicha autorización deberá establecer *garantías adecuadas* del respeto de los derechos fundamentales y de los intereses del interesado.

Además de levantar la prohibición sobre su tratamiento, el responsable debe acreditar también que su tratamiento se puede realizar porque concurre una de las bases jurídicas legitimadoras del tratamiento contenidas en el artículo 6.1 del RGPD, que son requisito general para el tratamiento de cualquier dato de carácter personal. Esto es, la concurrencia de una excepción que hipotéticamente permita levantar la prohibición de tratar datos biométricos no será suficiente, no sustituye a la necesidad de que a su vez exista una base de licitud en el caso de los biométricos. El responsable debe estar en disposición de acreditar que concurren ambas.
La parte reclamada entiende que el tratamiento realizado encuentra su base de licitud en el artículo 6.1 b) del RGPD, cuyos términos son los siguientes:

> *1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones (…)*
> *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 este de medidas precontractuales;*

En el caso que nos ocupa, si bien puede entenderse que existiría la base de legitimación prevista en el artículo 6.1 b), la existencia de una base de legitimación del tratamiento sólo podría tenerse en consideración en caso de que se apreciara una circunstancia que levantase la prohibición del tratamiento de categorías especiales de datos personales, en este caso biométricos.

VI
Obligación incumplida. Artículo 9 RGPD

De acuerdo con lo que venimos analizando, nos encontramos ante un tratamiento de categorías especiales de datos- huellas dactilares de los empleados de la parte reclamada-, para el que es de aplicación la prohibición general de tratamiento prevista en el artículo 9.1 del RGPD.
No obstante lo anterior, como ya se ha indicado, esta prohibición general de tratamiento puede ser levantada por alguna de las circunstancias de las previstas en el apartado 2 del mismo artículo 9 RGPD.

En el análisis de la aplicación de dichas circunstancias es importante recordar que el TJUE ya se ha pronunciado sobre el carácter restrictivo que debe otorgarse a las excepciones a la prohibición de tratamiento de las categorías especiales de datos. Por ejemplo, en su sentencia de 4 de julio de 2023, dictada en el asunto C-252/21, en la que indica lo siguiente (el subrayado es nuestro):

> *76 Por otra parte, en la medida en que establece una excepción al principio de prohibición del tratamiento de categorías especiales de datos personales, el artículo 9, apartado 2, del RGPD debe interpretarse de manera restrictiva (véanse,*

en este sentido, las sentencias de 17 de septiembre de 2014, Baltic Agro, C-3/13, EU:C:2014:2227, apartado 24 y jurisprudencia citada, y de 6 de junio de 2019, Weil, C-361/18, EU:C:2019:473, apartado 43 y jurisprudencia citada).

La parte reclamada alega como circunstancia que permite el tratamiento de los datos biométricos de sus trabajadores 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;* (artículo 9.2 b)

Teniendo en cuenta los términos en los que se pronuncia este precepto y que la normativa estatal que la parte reclamada considera como habilitante para el tratamiento de una categoría especial de datos biométricos de sus trabajadores- la huella dactilar- tan sólo prevé la consecución de un objetivo- el control de la jornada laboral a través del registro de la misma- y no indica que se deba o pueda hacer mediante el tratamiento de datos biométricos, además de que no cabe apreciar la necesidad del mismo para la consecución del objetivo pretendido, ha de entenderse que, sin perjuicio de lo que resulte de la instrucción, no se cumpliría con lo dictaminado por el artículo 9.2 b) RGPD.

VII

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

El artículo 83.5 del RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 20.000.000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

> *"a) los principios básicos para el tratamiento, incluidas las condiciones para el consentimiento a tenor de los artículos 5, 6, 7 y 9; (…)*

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

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

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

> *"En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*
>
> > *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.

VIII
Propuesta de sanción

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

"1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;
j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, y a las circunstancias que se dan en el presente expediente, correspondería la imposición de multa.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que en la sanción a imponer ha de tenerse en cuenta las circunstancias previstas en el artículo 83.2 a), b) y g):

a) *la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido.* A este respecto, y tal y como se argumenta, se ha producido un tratamiento de datos biométricos- incluidos dentro de las categorías especiales de datos- que, por su naturaleza, afectan de una forma más incisiva en el derecho fundamental a la protección de datos de los afectados que, en consecuencia, merece una respuesta acorde con el perjuicio.

a) *la intencionalidad o negligencia en la infracción.* Como se ha indicado, la decisión de iniciar el tratamiento de datos biométricos no ha venido precedida de una adecuada valoración de los riesgos en atención a la finalidad del tratamiento y a la categoría de los datos objeto del mismo, de lo que se concluye en una actuación negligente por la parte reclamada. De igual forma, y a pesar de las deficiencias en el funcionamiento del sistema instalado,

detectadas desde su comienzo, el sistema ha permanecido en vigor durante varios meses, siendo esta una decisión consciente de la parte reclamada.

g) *las categorías de los datos de carácter personal afectados por la infracción*. En el presente caso, nos encontramos ante un tratamiento de datos biométricos, considerados categorías especiales de datos, merecedores de un nivel especialmente elevado de protección debido a los riesgos que para su titular se derivan del tratamiento.

No se tienen en consideración circunstancias agravantes.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 9 del RGPD, permite fijar inicialmente una sanción de multa administrativa de 10.000,00 euros, (DIEZ MIL EUROS).

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada por vulneración del precepto señalado anteriormente.

IX
Sobre la necesidad de realizar y superar una evaluación de impacto previa y adecuada al tratamiento

a) Obligación de realizar una Evaluación de Impacto de Datos Personales (EIDP)

Según lo dispuesto por el considerando 84 del RGPD (el subrayado es nuestro)

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

A continuación, el RGPD, en su considerando 90, se refiere a EIPD en los siguientes términos:

> *En tales casos, el responsable debe llevar a cabo, antes del tratamiento, una evaluación de impacto relativa a la protección de datos con el fin de valorar la particular gravedad y probabilidad del alto riesgo, teniendo en cuenta la naturaleza, ámbito, contexto y fines del tratamiento y los orígenes del riesgo. Dicha evaluación de impacto debe incluir, en particular, las medidas, garantías*

y mecanismos previstos para mitigar el riesgo, garantizar la protección de los datos personales y demostrar la conformidad con el presente Reglamento.

Por su parte, el artículo 35 RGPD- *Evaluación de impacto relativa a la protección de datos*- señala lo siguiente (el subrayado es nuestro):

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

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

3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en caso de:

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

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

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

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

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

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

7. La evaluación deberá incluir como mínimo:

a)una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;

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

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

d)las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta

los derechos e intereses legítimos de los interesados y de otras personas afectadas.

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

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

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

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

La EIPD aparece desde la entrada en vigor del RGPD como una nueva herramienta exigible al responsable de tratamientos de “alto riesgo”. En este sentido, el tratamiento de datos biométricos se considera de alto riesgo de acuerdo con lo previsto en el apartado 4 del artículo 35 y consta entre los tratamientos incluidos en el documento “Listas de tipos de tratamiento de datos que requieren evaluación de impacto relativa a protección de datos”, hecho público por la AEPD en desarrollo de dicha previsión.

Así, la consideración de alto riesgo del tratamiento de estos datos se ve refrendada por el hecho de que los datos biométricos cumplen con los criterios correspondientes a los números 4, 5 y 10 del mencionado listado (tratamientos que impliquen el uso de categorías especiales de datos; el uso de datos biométricos y los que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas). Ha de recordarse que dicho listado fue publicado el 18/05/2019; por lo tanto, con bastante anterioridad al tratamiento del que trae causa el presente acuerdo de inicio de procedimiento sancionador.

Las EIPD tienen como objetivo último la identificación de los riesgos que llevan aparejados determinados tratamientos personales en atención a su incidencia en el derecho fundamental a la protección de datos personales de sus titulares y, en tal sentido, ha de entenderse que se configura como una obligación del responsable- en atención al principio de responsabilidad proactiva- que, por sus propias características- ha de optarse por un enfoque de análisis de riesgos desde el diseño y por defecto, para poder identificarlos, determinar la probabilidad de materialización y su impacto, y prever medidas y garantías que eliminen o, cuando menos, mitiguen los riesgos detectados, evitando su materialización- debe realizarse con carácter previo al tratamiento y adaptarse continuamente en atención a la evolución de los riesgos y amenazas que puedan afectar al tratamiento.

Con esta misma lógica, no basta con realizar formalmente una EIPD, sino que la misma, además de contener como mínimo la información del art. 35.7 del RGPD, deberá superarse y ser considerada válida. Es decir, no se trata de una obligación formal, que se entienda cumplida con la mera realización de una EIPD, sino material, garantizando que la misma contenga un análisis sólido y exhaustivo del tratamiento previsto, de los riesgos que el mismo puede implicar y de las medidas que se consideren convenientes para evitarlos o, al menos, minimizarlos. Y todo ello, con carácter previo al tratamiento, de tal manera que las conclusiones de la EIPD puedan tenerse en cuenta en su diseño, cumpliendo así el principio de protección de datos desde el diseño y por defecto que contempla el artículo 25 RGPD.
Especialmente relevante será el análisis que la EIPD haga de la concurrencia de los preceptivos criterios de necesidad, idoneidad y proporcionalidad del tratamiento. Y ello por cuanto el responsable que pretenda instaurar un tratamiento de datos personales de esta naturaleza ha de asegurarse que se supera lo que se ha denominado en la jurisprudencia “el triple juicio de proporcionalidad”, planteándose en especial si el tratamiento de datos biométricos es necesario, idóneo y proporcional.
Si existen otros sistemas no biométricos que permitan conseguir la misma finalidad de identificar-verificar la identidad de las personas con eficacia, no será necesario iniciar tratamientos biométricos, y, por tanto, implantar este sistema se considerará contrario al RGPD. Este juicio debe ser el punto de partida de su análisis, pues sólo en caso de que estos métodos superen el citado triple juicio, se exigirá el cumplimiento de otros requisitos o garantías.
En definitiva, el tratamiento de datos biométricos nunca podrá iniciarse de no haber elaborado una EIPD válida y previa al tratamiento.

a) La EIDP realizada por la parte reclamada

Según ha quedado acreditado por la parte reclamada, consta la realización de una EIPD fechada el 6 de febrero de 2023 que, si bien previa, es muy próxima a la decisión acerca de la implantación del sistema acordada por la Junta Directiva de la parte reclamada, el 14 de febrero. Asimismo, según lo indicado por la propia reclamada, es en los días posteriores que comienza el proceso de configuración del sistema por parte del proveedor (grabación de huellas, horarios laborales para implementarlos en el sistema, etc.). Estas circunstancias llevarían a plantearse, como cuestión previa de relevancia, si la decisión acerca de la implantación de un sistema como el analizado ya estuviera avanzada en la fecha en la que se elaboró la EIPD y que incluso ya estuviera identificado el proveedor – y, por lo tanto, conocidas las características del sistema-. Y ello por cuanto sólo así parecería razonable que la instalación del sistema pudiera haberse realizado de forma prácticamente inmediata tras la toma de la decisión. De igual forma, siguiendo con este mismo razonamiento, parecería al menos dudoso que la EIPD hubiera sido elaborada desconociendo totalmente estos hechos- decisión mínimamente avanzada y proveedor identificado- de tal manera que podría cuanto menos plantearse que la EIPD no se realizara atendiendo a las consideraciones que han de tenerse en cuenta y que han sido señaladas con anterioridad.
Sentado lo anterior, de la EIPD realizada consideramos conveniente destacar los siguientes extremos:

- En el análisis del denominado *Escenario de Riesgo R02* - hay violación de la confidencialidad de los datos personales- se señala como medida propuesta la *Necesidad de realizar una evaluación de impacto en la protección de datos*

- En lo que respecta al Escenario de Riesgo R04- Los datos biométricos se mantienen almacenados por tiempo no definido-, se proponen como medidas las siguientes:
    - *Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento conforme a la normativa aplicable (los registros deben conservarse cuatro años) y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.*
    - *Mantener documentación sobre datos biométricos únicamente durante el tiempo requerido por la normativa laboral aplicable*
- En relación con el análisis de la necesidad del tratamiento, destacamos los siguientes aspectos:

    a. Juicio de idoneidad

    En relación al juicio de idoneidad, hay que dilucidar si el tratamiento de datos biométricos es necesario para responder a una necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable, y viniendo determinada dicha idoneidad del tratamiento por su efectividad en minimizar el riesgo para el que se aplica.

    A este respecto se considera que este tratamiento de datos biométricos permite cumplir, con garantías de seguridad, las obligaciones del Colegio de la gestión laboral del control horario de la asistencia y acceso de sus empleados a las dependencias del mismo con la finalidad de dar cumplimiento al Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo, por lo que se considera que la medida es idónea.

    b. Juicio de necesidad

    En relación al juicio de necesidad, hay que dilucidar la probabilidad de que el tratamiento sea eficaz para responder a la necesidad en cuestión del tratamiento de la huella dactilar para minimizar riesgos de incumplimiento de las obligaciones del Colegio de la gestión laboral del control horario de sus empleados.

    Así, la necesidad del tratamiento por el Colegio se ampara en su obligación de asegurar y minimizar los riesgos de seguridad, objetividad y fiabilidad en el registro horario de sus empleados, en base a su responsabilidad y obligación establecida por el Estatuto de los Trabajadores. Debe tenerse en cuenta que con anterioridad al Real Decreto-Ley 8/2019, el control horario laboral en el Colegio se lleva a cabo manualmente mediante una hoja de papel en la que los empleados diariamente anotan sus horas de entrada y salida de las oficinas, pero dicho sistema de registro se ha considerado que no es objetivo y fiable para acreditar dichos horarios, máxime cuando en el caso del Colegio, que es el empleador, la especial necesidad de la implantación del sistema de lectura de huella en el mismo también está justificada porque los miembros de la Junta Directiva del Colegio, compuesta por nueve Notarios, cumplen sus jornadas laborales de trabajo, no en el Colegio, sino en sus propias Notarías donde están destinados, situadas en cualquier población de la Comunidad Autónoma de Aragón.

Además, dicha necesidad se ampara igualmente en que el sistema de huella dactilar asegurará que sea imposible obtener la imagen real de la huella dactilar con el patrón guardado en el lector del terminal, ya que no se efectuará ninguna fotografía digital de la huella, sino que se deberá establecer una relación matemática entre determinados puntos de la misma (singularidades, puntos característicos o 'minucias') dando lugar a un conjunto de números que servirá después para identificar de manera inequívoca a cada empleado.

c. Juicio de proporcionalidad: análisis del balance entre riesgo-beneficio

En relación al juicio de proporcionalidad del tratamiento, este viene determinado por la posibilidad de aplicar otras medidas menos intrusivas que puedan proporcionar el mismo grado de efectividad.

A tal efecto se ha analizado la aplicación de otras medidas de control horario de los empleados que pudieran minimizar los riesgos para los 28 derechos y libertades de los empleados utilizando sistemas no biométricos, como por ejemplo el uso de tarjetas o aplicaciones mediante códigos alfanuméricos personales o contraseñas, constatando que estos no asegurarían al Colegio una comprobación fiable de la identificación y autenticación unívoca de los usuarios porque permitirían ser fácilmente intercambiados. Por ello, ante la imposibilidad de aplicar otras medidas menos intrusivas que puedan proporcionar el mismo grado de efectividad, se puede afirmar que el tratamiento que se realice mediante la utilización de sistemas de comprobación de las huellas dactilares de los empleados del Colegio, aplicando las correspondientes medidas de protección de datos, es una medida proporcional para responder a la necesidad del tratamiento. Para llegar a esta conclusión se ha llevado a cabo una ponderación de los derechos en conflicto que concurrirán en el caso de la captura de huellas dactilares como medida de control de la jornada horaria de los empleados del Colegio. Por un lado, el derecho a la protección de datos, y por otro el derecho a las facultades de control laboral del Colegio establecidas por la normativa laboral -en concreto el art. 20.3 del Estatuto de los Trabajadores que establece que "El empresario podrá adoptar las medidas que estime más oportunas de vigilancia y control para verificar el cumplimiento por el trabajador de sus obligaciones y deberes laborales, guardando en su adopción y aplicación la consideración debida a su dignidad y teniendo en cuenta, en su caso, la capacidad real de los trabajadores con discapacidad"-, considerando que prevalecen en todo momento el derecho al control laboral sobre el de protección de datos, sin perjuicio de que es imprescindible la aplicación de las garantías adecuadas de protección de datos, pues el RGPD requiere también en estos casos que la norma que permita este tratamiento ha de establecer también dichas garantías.

X
Obligación incumplida. Art. 35 RGPD

La obligación de evaluar la idoneidad, necesidad y proporcionalidad del tratamiento en la EIPD según el artículo 35.7 b) del RGPD, debe interpretarse de conformidad con lo previsto por la reiterada jurisprudencia de nuestro Tribunal Constitucional respecto a la necesidad de constatar que toda medida restrictiva de derechos fundamentales (operaciones de tratamiento que comprenden datos biométricos en este caso) supera lo que se denomina como "el triple juicio de proporcionalidad".

Ello implica que, antes que nada, sea necesario constatar si cumple los tres siguientes requisitos o condiciones a los que se refiere el Tribunal Constitucional en su sentencia 14/2003, de 28 de enero: « *para comprobar si una medida restrictiva de un derecho fundamental supera el juicio de proporcionalidad, es necesario constatar si cumple los tres requisitos o condiciones siguientes: si tal medida es susceptible de conseguir el objetivo propuesto (juicio de idoneidad); si, además, es necesaria, en el sentido de que no exista otra medida más moderada para la consecución de tal propósito con igual eficacia (juicio de necesidad); y, finalmente, si la misma es ponderada o equilibrada, por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto (juicio de proporcionalidad en sentido estricto)*".

- Idoneidad. En relación con el juicio de idoneidad, el mismo debe partir de la adecuación del sistema implantado para alcanzar las finalidades del tratamiento, en este caso, el control de la asistencia y acceso laboral a las dependencias del Colegio por parte de sus empleados. Cabe destacar que, de acuerdo a lo afirmado por la parte reclamada, el sistema dio fallos desde el momento de su implantación; a la fecha en que se respondió al traslado de la reclamación se indicó que *hasta la fecha, el sistema no ha estado operativo plenamente debido a diversas incidencias relacionadas con el software instalado y el servidor del propio Colegio* y, durante las actuaciones de traslado, afirmó que *una vez instalado el correspondiente software del sistema en el servidor del Colegio, no funcionaba correctamente la parte fundamental de las funcionalidades previstas por el producto al no emitir el sistema los correspondientes informes sobre la recogida diaria por el lector de los datos horarios de los empleados, es decir, los informes sobre los horarios de entrada y salida de los empleados, que evidentemente eran la razón principal de dicho sistema. Y, en segundo lugar, la instalación de dicho software, además interfirió en el funcionamiento de otras aplicaciones ya instaladas en dicho servidor, por lo cual el Colegio procedió primero a inhabilitar el software y posteriormente desinstalarlo de dicho servidor.*

  Podemos afirmar, por lo tanto, que el sistema instalado no resultaba idóneo para el cumplimiento de la finalidad prevista, destacando su interferencia con aplicaciones que ya se encontraban en funcionamiento en la parte reclamada; circunstancia que podría haber sido detectada antes de proceder a la instalación del sistema
- Necesidad. Argumenta la parte reclamada que el tratamiento era necesario para realizar con efectividad el control del cumplimiento horario de los trabajadores. Todo ello teniendo en cuenta las especiales características del **COLEGIO NOTARIAL DE ARAGÓN**, en cuyas dependencias no se encuentran físicamente con regularidad los miembros de la Junta Directiva. A este respecto, ha de recordarse que necesidad no debe confundirse con conveniencia y que no puede articularse una medida consistente en un tratamiento de datos personales de alto riesgo con base en la satisfacción

de los intereses de una sola de las partes. Por otro lado, y aunque la parte reclamada parece vincular la ausencia regular de los miembros de su Junta Directiva en sus dependencias con las dificultades para controlar el cumplimiento por parte de los trabajadores de su jornada laboral, consta en el expediente la figura del puesto de Oficial Mayor del Colegio que, se entiende, desarrolla su jornada laboral en las dependencias del mismo, precisamente para poder realizar las funciones que se vinculan a dicho tipo de puestos.

- Proporcionalidad. Afirma la parte reclamada haber analizado otras opciones menos intrusivas que permitieran alcanzar con igual nivel de efectividad el objetivo propuesto. Ha de destacarse a este respecto que el Real Decreto-ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo que introdujo el apartado 9 del artículo 34 del Estatuto de los Trabajadores- referido al registro de la jornada laboral y que se utiliza como base legal para la implementación de la medida- entró en vigor, según su Disposición final sexta, el 12/05/2019

  4. El registro de jornada establecido en el apartado 9 del artículo 34 del texto refundido de la Ley del Estatuto de los Trabajadores, aprobado por el Real Decreto Legislativo 2/2015, de 23 de octubre, según la redacción dada al mismo por el artículo 10 de este real decreto-ley, será de aplicación a los dos meses de su publicación en el «Boletín Oficial del Estado»

  Teniendo en cuenta que la implantación del tratamiento objeto del presente acuerdo de inicio de procedimiento sancionador se acordó casi cuatro años después, puede considerarse que, hasta ese momento se consideró adecuado el sistema hasta entonces implantado. Destaca también que, en el marco de las actuaciones de investigación llevadas a cabo, la parte reclamada afirma que *el Colegio ha decidido que utilizará un sistema de control horario menos intrusivo para la protección de datos que consistirá en un programa de software para ordenador que permitirá al empleado fichar, mediante un código numérico, una vez que inicie sesión con el correspondiente ordenador asignado a cada empleado.*

XI

Tipificación de la infracción del artículo 35 del RGPD y calificación a efectos de prescripción

El artículo 83.4 el RGPD tipifica como infracción administrativa la vulneración de los artículos siguientes, que se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

a) *las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43*; *(…)*

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

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

A los solos efectos del plazo de prescripción, el artículo 73 de la LOPDGDD establece lo siguiente:

" En función de lo que establece el artículo 83.4 del Reglamento (UE) 2016/679 se consideran graves y prescribirán a los dos años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes

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

XII

Propuesta de sanción

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

“1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 9 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:
a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;
b) la intencionalidad o negligencia en la infracción;
c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;
d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;
e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;
f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;
g) las categorías de los datos de carácter personal afectados por la infracción;
h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;
i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;

j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y
k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción".

Por su parte, el artículo 76 *"Sanciones y medidas correctivas"* de la LOPDGDD dispone:

"1. Las sanciones previstas en los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679 se aplicarán teniendo en cuenta los criterios de graduación establecidos en el apartado 2 del citado artículo.

2. De acuerdo a lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:
a) El carácter continuado de la infracción.
b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.
c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.
d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.
e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.
f) La afectación a los derechos de los menores.
g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.
h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado".

En el presente caso, considerando la gravedad de la posible infracción, atendiendo especialmente a las consecuencias que su comisión provoca en los afectados, correspondería la imposición de multa, además de la adopción de medidas, si procede.

A efectos de decidir sobre la imposición de una multa administrativa y su cuantía, de conformidad con las evidencias de que se dispone en el presente momento de acuerdo de inicio de procedimiento sancionador, y sin perjuicio de lo que resulte de la instrucción, se considera que en la sanción a imponer ha de tenerse en cuenta las circunstancias previstas en el artículo 83.2 a), b) y g).

a) *la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido.* A este respecto, y tal y como se argumenta, se ha producido un tratamiento de datos biométricos- incluidos dentro de las categorías especiales de datos- que, por su naturaleza, afectan de una forma más incisiva en el derecho fundamental a la protección de datos de los afectados que, en consecuencia, merece una respuesta acorde con el perjuicio.

a) *la intencionalidad o negligencia en la infracción.* Como se ha indicado, la decisión de iniciar el tratamiento de datos biométricos no ha venido precedida de una adecuada valoración de los riesgos en atención a la finalidad del tratamiento y a la categoría de los datos objeto del mismo, de lo que se concluye en una actuación negligente por la parte reclamada. De igual forma, y a pesar de las deficiencias en el funcionamiento del sistema instalado, detectadas desde su comienzo, el sistema ha permanecido en vigor durante varios meses, siendo esta una decisión consciente de la parte reclamada

g) *las categorías de los datos de carácter personal afectados por la infracción*: En el presente caso, nos encontramos ante un tratamiento de datos biométricos, considerados categorías especiales de datos, merecedores de un nivel especialmente elevado de protección debido a los riesgos que para su titular se derivan del tratamiento.

No se tienen en consideración circunstancias agravantes.

El balance de las circunstancias contempladas en el artículo 83.2 del RGPD, con respecto a la infracción cometida al vulnerar lo establecido en el artículo 35 del RGPD, permite fijar inicialmente una sanción de multa administrativa de 10.000,00 euros, (DIEZ MIL EUROS).

Por tanto, de conformidad con las evidencias de las que se dispone en este momento de acuerdo de inicio de procedimiento sancionador, se considera que los hechos conocidos podrían ser constitutivos de una infracción, imputable a la parte reclamada por vulneración de los preceptos señalados anteriormente.

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

SE ACUERDA:

PRIMERO: INICIAR PROCEDIMIENTO SANCIONADOR a ***COLEGIO NOTARIAL DE ARAGÓN***, con NIF ***Q5063003G***, por la presunta infracción de los artículos 9 y 35 del RGPD, tipificadas, respectivamente, en el artículo 83.5 a) y 83.4 a) del RGPD.

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

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

CUARTO: QUE a los efectos previstos en el art. 64.2 b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, la sanción que pudiera corresponder sería de multa administrativa de 10.000,00 euros por la infracción del artículo 9 del RGPD y de multa administrativa de 10.000,00 euros por la infracción del artículo 35 del RGPD, sumando un total de 20.000,00 euros, sin perjuicio de lo que resulte de la instrucción.

QUINTO: NOTIFICAR el presente acuerdo a ***COLEGIO NOTARIAL DE ARAGÓN***, con NIF ***Q5063003G***, otorgándole un plazo de audiencia de diez días hábiles para que formule las alegaciones y presente las pruebas que considere convenientes. En su escrito de alegaciones deberá facilitar su NIF y el número de procedimiento que figura en el encabezamiento de este documento.

De conformidad con lo dispuesto en el artículo 85 de la LPACAP, podrá reconocer su responsabilidad dentro del plazo otorgado para la formulación de alegaciones al presente acuerdo de inicio; lo que llevará aparejada una reducción de un 20% de la sanción que proceda imponer en el presente procedimiento. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000,00 euros, resolviéndose el procedimiento con la imposición de esta sanción.

Del mismo modo podrá, en cualquier momento anterior a la resolución del presente procedimiento, llevar a cabo el pago voluntario de la sanción propuesta, lo que supondrá la reducción de un 20% de su importe. Con la aplicación de esta reducción, la sanción quedaría establecida en 16.000,00 euros y su pago implicará la terminación del procedimiento, sin perjuicio de la imposición de las medidas correspondientes.

La reducción por el pago voluntario de la sanción es acumulable a la que corresponde aplicar por el reconocimiento de la responsabilidad, siempre que este reconocimiento de la responsabilidad se ponga de manifiesto dentro del plazo concedido para formular alegaciones a la apertura del procedimiento. El pago voluntario de la cantidad referida en el párrafo anterior podrá hacerse en cualquier momento anterior a la resolución. En este caso, si procediera aplicar ambas reducciones, el importe de la sanción quedaría establecido en **12.000,00 euros**.

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

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

En caso de que optara por proceder al pago voluntario de cualquiera de las cantidades señaladas anteriormente (**16.000,00 euros o 12.000,00 euros**), deberá hacerlo efectivo mediante su ingreso en la cuenta nº ***IBAN: ES00-0000-0000-0000-0000-0000 (BIC/Código SWIFT: CAIXESBBXXX)*** abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A., indicando en el concepto el número de referencia del procedimiento que figura en el encabezamiento de este documento y la causa de reducción del importe a la que se acoge.

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

En cumplimiento de los artículos 14, 41 y 43 de la LPACAP, se advierte de que, en lo sucesivo, las notificaciones que se le remitan se realizarán exclusivamente de forma electrónica, a través de la Dirección Electrónica Habilitada única (dehu.redsara.es) y de la Sede electrónica (sedeagpd.gob.es), y que, de no acceder a ellas, se hará constar su rechazo en el expediente, dando por efectuado el trámite y siguiéndose el procedimiento. Se le informa que puede identificar ante esta Agencia una dirección de correo electrónico para recibir el aviso de puesta a disposición de las notificaciones y que la falta de práctica de este aviso no impedirá que la notificación sea considerada plenamente válida.

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

1479-031024
Mar España Martí
Directora de la Agencia Española de Protección de Datos

>>

SEGUNDO**:** En fecha 22 de noviembre de 2024, la parte reclamada ha procedido al pago de la sanción en la cuantía de **12000 euros** haciendo uso de las dos reducciones previstas en el Acuerdo de inicio transcrito anteriormente, lo que implica el reconocimiento de la responsabilidad.

TERCERO**:** El pago realizado, dentro del plazo concedido para formular alegaciones a la apertura del procedimiento, conlleva la renuncia a cualquier acción o recurso en vía administrativa contra la sanción y el reconocimiento de responsabilidad en relación con los hechos a los que se refiere el Acuerdo de Inicio y su calificación jurídica.

FUNDAMENTOS DE DERECHO

I

Competencia

De acuerdo con los poderes que el artículo 58.2 del Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), otorga a cada autoridad de control y según lo establecido en los artículos 47, 48.1, 64.2 y 68.1 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), es competente para iniciar y resolver este procedimiento la Directora de la Agencia Española de Protección de Datos.

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

II
Terminación del procedimiento

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

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

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

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

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

De acuerdo con lo señalado,
la Directora de la Agencia Española de Protección de Datos RESUELVE**:**

PRIMERO: DECLARAR la terminación del procedimiento **EXP202304834**, de conformidad con lo establecido en el artículo 85 de la LPACAP.

SEGUNDO: NOTIFICAR la presente resolución a ***COLEGIO NOTARIAL DE***

ARAGÓN.

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

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

936-151024
Mar España Martí
Directora de la Agencia Española de Protección de Datos