- **Expediente N.º: EXP202202960**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO:

A.A.A. (en adelante, la parte reclamante) con fecha 14 de febrero de 2022 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **CTC EXTERNALIZACIÓN, S*.L.*** con NIF ***B60924131*** (en adelante, la parte reclamada). Los motivos en que basa la reclamación son los siguientes:

Se reclama que en la entidad CTC EXTERNALIZACIÓN, S.L. se han solicitado datos biométricos, en concreto la huella dactilar, a los empleados con la finalidad de implantar un sistema de fichaje basado en ese dato.

Se expone que en el momento de tomar los datos biométricos no se comunicó que la información se encontraba en el portal del empleado, localizada en la parte más recóndita de la aplicación a la que no tienen acceso todos los trabajadores que emplean el nuevo sistema de fichaje.

Junto a la reclamación se aporta Impresión de correos electrónicos intercambiados entre la parte reclamante y reclamada

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 la parte reclamada 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 14/03/2022 como consta en el acuse de recibo que obra en el expediente.

Con fecha 22/03/2022 se recibe en esta Agencia escrito de respuesta indicando básicamente lo siguiente:

1. Se trata de un sistema de verificación/autenticación (uno a uno), No de Identificación (uno a varios).

2. No se almacena la huella dactilar. El lector genera un identificador numérico que es el que coincide con la huella. Se almacenan los identificadores y no la huella. Se utiliza un sistema de cifrado para el almacenamiento. Es imposible reproducir la huella dactilar a partir del identificador numérico.

3. El sistema no compara huellas, compara el código que se genera en la lectura con el código que está almacenado.

4. El sistema relaciona un número con un identificador numérico que se ha creado a través de un hash.

5. No se solicitan ni se tratan más datos de los estrictamente necesarios para la finalidad de este tratamiento.

6. No pueden reutilizarse los datos para otras finalidades y se suprimen cuando ya no son necesarios.

7. Los datos tratados son nombre, apellidos, código de empleado y huella dactilar de inicio que se transforma en un código de identificación. La huella como tal se elimina.

8. Almacenan solo un template biométrico que es registrado en un repositorio central para su distribución al resto de dispositivos biométricos.

9. El repositorio central está ubicado en un servidor interno no accesible públicamente y con acceso restringido exclusivamente al administrador del sistema.

10. Se ha informado sobre el tratamiento de datos de carácter personal, concretamente: la identidad del Responsable del tratamiento, la base de legitimación, finalidades del tratamiento, contacto del delegado de protección de datos, derechos y procedimiento para ejercitarlos, que no se realizan cesiones de datos y plazo de conservación previsto. Además, la información se facilita a través del Portal del Empleado al que tienen acceso todos los Empleados. Se entregan las cláusulas de protección de datos de la empresa con las altas laborales. e envió en octubre 2021 un correo electrónico a los empleados informando de la actualización de las políticas de protección de datos y de su publicación en el Portal del Empleado. El sistema de acceso con la huella dactilar se activó a finales de diciembre 2021.

11. Tienen protección de datos desde el diseño: se ha seleccionado un proveedor con un software que ofrece todas las garantías en cumplimiento de las normativas de protección de datos, con el que se tiene firmado un contrato como Encargado del tratamiento.

12. No se realizan transferencias internacionales de datos. La ubicación está en el EEE.

13. Se aporta la Evaluación de impacto realizada, donde entre otras cuestiones:

    Consta que sí se cumple el principio de minimización de datos porque "*La finalidad que se pretende cubrir requiere de todos los datos a recabar y para todas las personas/interesados afectados (principio de minimización de datos).”*. No consta justificación de cómo se cumple este principio.

    Consta que se responde afirmativamente a la cuestión de que "*Los datos recogidos se van a usar exclusivamente para la finalidad declarada y no para ninguna otra no informada ni incompatible con la legitimidad de su uso (principio de limitación de la finalidad).”.* No consta justificación de cómo se cumple este principio.

    Consta en el apartado Resultado que "*Tras el análisis de la necesidad y proporcionalidad de este tratamiento, el análisis de riesgos realizado y la valoración del riesgo Residual tras la aplicación de las correspondientes*

medidas de seguridad, el resultado de este estudio de Evaluación de impacto de protección de datos EIPD es: ACEPTABLE."

14. Se ha instalado un cartel informativo junto al aparato de fichajes sobre el tratamiento de datos con la finalidad que sea perfectamente visible por todos los trabajadores. También se ha ampliado la información de protección de datos relativa al uso de la huella dactilar para control de la jornada laboral y se ha comunicado a los empleados, a través del Portal del Empleado.

15. Con motivo de esta reclamación se ha enviado email a todos los empleados la cláusula informativa.

16. Han implantado las siguientes medidas para evitar que se produzcan incidencias similares:

    - Cartel informativo junto al aparato de fichajes sobre el tratamiento de datos.

    Aporta copia del cartel informativo donde consta información del responsable, finalidad, legitimación, destinatarios, derechos y lugar donde localizar información adicional (Portal del Empleado).

    Se aporta captura de pantalla del Portal del Empleado donde consta un enlace a la cláusula informativa, pero no consta fecha de publicación, ni *url* del Portal del Empleado.

    - Ampliación de la información de protección de datos relativa al uso de la huella dactilar para control de la jornada laboral y comunicación a los empleados, a través del Portal del Empleado.

    - Envío de un correo electrónico a los empleados con la información actualizada de protección de datos relativa al uso de la huella dactilar para control de la jornada laboral y como canal para todas las dudas o aclaraciones que necesiten.

    - Se realizará el seguimiento de la recepción de las nuevas cláusulas publicadas por todos los empleados.

1. Se aporta el Registro de actividades de tratamiento de la huella dactilar en el que consta que se usa la huella dactilar como sistema de verificación/autenticación, no de Identificación.

2. Han descartado otros sistemas p.e el fichaje con tarjeta porque tras la experiencia con el mismo, se dieron situaciones conflictivas. Se trata de un servicio en el que existe una gran rotación de personal. Cuando se utilizaba el sistema de tarjeta para el fichaje, en ocasiones se cedía a otras personas que no eran las titulares de la misma, presenciándose en la zona

de trabajo personal ajeno al mismo con todos los riesgos que supone de seguridad laboral. La utilización de la huella dactilar es el sistema que permite evitar estas situaciones delictivas y garantiza el correcto cumplimiento de la normativa laboral e impedir el acceso no autorizado.

TERCERO:

Con fecha 14 de mayo de 2022, 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 Reglamento (UE) 2016/679 (Reglamento General de Protección de Datos, en adelante RGPD), y de conformidad con lo establecido en el Título VII, Capítulo I, Sección segunda, de la LOPDGDD, teniendo conocimiento de los siguientes extremos:

ANTECEDENTES

Junto a la reclamación la parte reclamación aporta los siguientes correos electrónicos:

- Copia de correo electrónico enviado por soliobrera.seccionTourline@gmail.com a ***USUARIO.1@grupoctc.com y a ***USUARIO.2@grupoctc.com con fecha 31/01/2022 con el texto:

  "El pasado viernes cuando me dispuse a firmar la salida de mi jornada laboral (método implantado desde un inicio para el registro y control de entrada-salida de trabajadores en centro de trabajo Madrid-Coslada), me informan que se va empezar a fichar con un control de acceso mediante huella dactilar y que tienen que tomarme las muestras, a lo que pregunto que sino van a darme información y algún documento en el que consienta el tratamiento de este tipo de datos y me dicen (para mi sorpresa) que no hay[…]"

- Aporta copia de correo electrónico enviado por ***USUARIO.1@grupoctc.com con fecha 02/02/2022 con el texto:

  "En primer lugar, no te informaron debidamente cuando preguntaste en el servicio si existía información sobre el tratamiento de los datos, pues sí que tenemos dicha información. En concreto, se encuentra en el portal del empleado de CTC, portal al que tienes acceso desde que te incorporaste en la compañía.
  Por otro lado, y atendiendo al artículo 9 sobre la Licitud del tratamiento, no es necesario el consentimiento expreso porque el tratamiento es necesario para el cumplimiento de obligaciones por parte del empresario, así como para el cumplimiento del ejercicio de los derechos del responsable del tratamiento.
  Cierto es que el artículo 13 prevé un deber de información, y este deber se cumple perfectamente al encontrarse la información colgada en el portal del

Empleado (en la política de protección de datos). Ahí verás toda la información relativa al responsable del tratamiento, finalidades de la recogida de los datos, destinatarios, conservación de los datos y el procedimiento para el ejercicio de los derechos.

En segundo lugar, comentas que el artículo 64.5.f) os faculta a emitir un informe previo. En este caso, lamento comunicarte que el punto 5 del mencionado artículo, está relacionado con el control de trabajo (en un sentido de contenido). De hecho, el literal del artículo estipula Io siguiente: "la implementación y revisión de sistemas de organización y control de trabajo, estudios de tiempos, establecimientos de primas e incentivos y valoración de puestos de trabajo". En este caso, se trata de un sistema de fichaje mediante huella dactilar, y la licitud de este tratamiento está amparada, no solo por el artículo 6 RGPD 2016/679 UE, sino también por cumplimiento de una obligación legal como es la del registro horario, regulada en el artículo 34.9 del Estatuto de los Trabajadores.
Para mayor tranquilidad, comentarte que la huella dactilar, en este caso, no adquiere la categoría de dato especial porque se utiliza únicamente para autentificar que la persona es quien dice ser. Además, no se almacena la huella, sino solo una serie de puntos que, vía algoritmo, provee una firma única para esa huella. Es decir, por si sola no representa la huella dactilar, y se guarda en un sistema centralizado con acceso restringido.
Con respecto al motivo de este sistema de fichaje, es el que se está implementando en la mayoría de servicios de CTC, incluidas oficinas centrales.
Por último, y si después de esta explicación aún lo consideras necesario, enviaremos los resultados del estudio de la evaluación de impacto (EIPD) que nos solicitabas.
[…]"

Durante las actuaciones se investigó a la siguiente entidad:

CTC EXTERNALIZACIÓN, S.L. con NIF B60924131 con domicilio en PLAZA EUROPA, 30 32. - 08902 L'HOSPITALET DE LLOBREGAT (BARCELONA) (en adelante CTC)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

Cuestiones generales:

1. Que en caso de que el empleado decline el uso de su huella para el proceso de marcaje o la huella resulte insuficientemente buena, se podrá realizar el marcaje mediante tarjeta RFID.
2. Que el tratamiento de huella dactilar comenzó en la fecha 29/12/2021 y finaliza cuando termine la relación laboral con el empleado. En ese caso, el hash de la huella es eliminado.
3. Que hay 208 lectoras de huellas instaladas en 117 centros de trabajo, todos en España.

Respecto a la información sobre protección de datos proporcionada:

4. Aportan capturas de pantalla donde consta que el documento con nombre "*POL RGPD CTC EXTER_2021.pdf*" fue publicado con fecha 28/10/2021 asociado a un "*cluster_id*" = 66 que, según manifiestan, hace referencia a los empleados a los que se les publica el documento.

5. Aportan captura de pantalla de sus sistemas donde consta "*cluster_id*" = 66 asociado al campo "*description*"="*Empleados sociedad CTC*".

6. Aportan copia de email enviado a ctc@grupoctc.com en fecha 28/10/2021 con asunto "*Actualización Políticas de protección de datos CTC EXTERNALIZACIÓN S.L.U."* donde consta:

"[…]
Por medio de la presente comunicación queremos informar que CTC EXTERNALIZACIÓN S.L.U., en su obligación de cumplimiento normativo, ha procedido a la actualización de sus Políticas de protección de datos respecto al tratamiento de los datos de carácter personal. Pueden acceder a través del Portal del Empleado, a la publicación de las nuevas políticas:
POL/RGPD CTC EXTER_2021: Cláusula Protección de datos de Empleados
Debe leer atentamente las presentes cláusulas y pulsar su aceptación. En caso de cualquier duda puede contactar con el Departamento de Protección de Datos, a través del correo electrónico: dpo@grupoctc.com
[…]"

7. Se aporta la cláusula informativa referida anteriormente donde consta como Fecha: 02/03/2018, fecha de Actualización: 26/10/2021 y el código "*POL/RGPD CTC EXTER_2021*". Asimismo, consta información sobre:

a. El marco legal
b. El responsable del tratamiento
c. La legitimación, siendo ésta la relación contractual laboral.
d. Finalidades del tratamiento, siendo éstas, gestionar la relación laboral con los empleados, gestión contable administrativa, confección de nóminas, prevención de riesgos laborales, formación. Se informa de que está instalado un lector de huellas dactilar para acceso a oficinas.
e. Destinatarios, donde consta:

"Los datos se comunicarán a las Administraciones públicas (Seguridad Social y Agencia Tributaria) en cumplimiento de la normativa laboral, mutuas laborales, a la empresa de asesoría laboral, a empresas de formación y a entidades bancarias para la domiciliación y pago de nóminas.
También entre empresas del Grupo, a empresas Clientes a las que prestamos nuestros servicios, así como a Proveedores que actúan como encargados del tratamiento y con quien se tienen debidamente firmados contratos de protección de datos.
En el caso de subcontrataciones, el trabajador autoriza a ceder los datos incluidos en los TC's, a todas aquellas empresas que sean necesarias para llevar a cabo la subcontratación.
Si la tarea del Empleado implica la conducción de vehículos, se cederán los datos del Empleado a la empresa de alquiler de vehículos, así como a la Administración en el caso de multa por infracción de tráfico."

f. Deber de confidencialidad del empleado.
g. Conservación de los datos, donde consta:

"Los datos proporcionados se conservarán mientras dure la relación contractual y durante los años necesarios para cumplir con las obligaciones legales.
Se recuerda que el uso de la cuenta de correo electrónico facilitada por la empresa, es estrictamente y está limitado para fines profesionales y no para temas personales.
El Empleado se compromete a la utilización del correo electrónico y de Internet sólo para temas profesionales de carácter laboral, reconociendo expresamente que la cuenta de correo electrónico es dominio de la empresa.
También se informa que la empresa, en el caso de extinción laboral, tendrá acceso al correo corporativo y equipo utilizado por el Exempleado."
h. Derechos.

En ese documento "*POL/RGPD CTC EXTER_2021*" consta exclusivamente la siguiente referencia específica al tratamiento de huellas dactilares:

"[…]
Está instalado un lector de huella dactilar para acceso a oficinas.
[…]"

8. Se aportan capturas de pantalla de sus sistemas donde consta que el reclamante ha accedido a ***(…)"*** en fechas entre 23/08/2021 y el 16/12/2021. Consta asimismo que el reclamante ha ejecutado la acción "*sign*" respecto del objeto "*POL06 2018 CLAUSULA PROTECCION DATOS*" en fecha 23/08/2021 10:20. Consta asimismo que existe un "*agreement_date*" relacionado con el reclamante y el documento "*POL06_2018_CLAUSULA.pdf*" en fecha 23/08/2021 10:20:16. Consta que la última "*agreement_date*" asociada al reclamante fue en fecha 23/08/2021.

9. Se aporta captura de pantalla del portal del empleado donde consta la "*Cláusula informativa uso huella dactilar para control de la jornada laboral*" y "*Cláusula Protección de datos de Empleados*". Que consta un botón a la derecha de cada documento con el texto "Recibida" que mediante su pulsación queda marcado el documento como "Recibido".

10. Que tras recibir el traslado de la reclamación por parte de la AEPD publicaron la cláusula más detallada "*Cláusula informativa uso huella dactilar para control de la jornada laboral*", la cual se envió por correo electrónico.
Aporta correo electrónico enviado en fecha 22/03/2022 con esta cláusula informativa.
En dicha cláusula informativa consta información específica sobre el tratamiento de huella dactilar con los apartados de responsable, legitimación, finalidad, destinatarios, plazo de conservación, derechos y medidas de seguridad. Que consta en esta información proporcionada "*Se trata de un sistema de autenticación/verificación no de identificación.*"

En relación a las características técnicas del sistema y a los contratos:

11. Que se utiliza un único servidor Windows Server 2016 como máquina virtual gestionada por CTC. ***(…).*** Que el servidor está ubicado en España.

Aporta copia de contrato de encargo firmado y fechado a 27/01/2023 entre CTC e ******EMPRESA.1)*** siendo éste el encargado del tratamiento. En dicho contrato consta

que CTC ha contratado con ***EMPRESA.1** el servicio de implantación y mantenimiento del sistema de control de acceso y control de jornada laboral mediante huella dactilar.

Consta asimismo otro contrato fechado a 29/09/2020 y firmado entre CTC e ***EMPRESA.1** como proveedor de software de control y acceso y presencia ***(…).***

Aporta contrato con el proveedor de hosting ***EMPRESA.2.** donde consta fecha 27/11/2019. No consta el objeto del contrato ni consta aportado el contrato completo. Consta en el apartado "*12 Datos de carácter personal*" en el subapartado "*5) Tratamiento de datos responsabilidad del Cliente, **EMPRESA.2** como encargado del tratamiento*" que:

> *"5) Tratamiento de datos responsabilidad del Cliente. **EMPRESA.2** como encargado del tratamiento*
> *Únicamente en el supuesto que **EMPRESA.2** tuviera acceso a datos de carácter personal responsabilidad del Cliente, y la prestación de los servicios contratados implique un tratamiento de datos personales por cuenta de un responsable del tratamiento, ya sea el Cliente o un tercero que contrata los servicios del Cliente directa o indirectamente, **EMPRESA.2** será considerado, "encargado del tratamiento" comprometiéndose a cumplir las obligaciones que le correspondan en función de la naturaleza y alcance de los servicios contratados y en virtud de Io establecido en la normativa vigente en materia de protección de datos, nacional o supranacional.*
> *[…]"*

12. Que las lectoras de huellas son ***(…).***

Aporta documento de especificaciones técnicas de la lectora donde consta que soporta ***(…)***.

13. Que el lector de huella es un dispositivo que se ubica en una zona accesible y de paso en el cual los empleados registran los diferentes marcajes a lo largo de la jornada laboral. Que para ello pueden utilizar su huella dactilar y el sistema calcula el hash que se comparará con el registrado en el momento de su activación en el sistema (registro del hash inicial de la huella y asociación al empleado).

14. Que el sistema está configurado para realizar una comparación de huellas 1:N. Que ***(…)*** calcula el template y lo compara con los que tiene almacenados. Que si existe correspondencia con algún patrón almacenado da por buena la lectura.

Aporta un diagrama donde consta que tras detectar el dedo en el sensor y calcular el patrón, existe el proceso de "*Comparar con los patrones almacenados*".

15. Que el template se genera en el módulo biométrico por lo que la imagen de la huella no se almacena ni se propaga a otros sistemas. Que en ningún momento se guarda la huella dactilar del empleado. Que la respuesta obtenida por el módulo es el template. Que la plantilla biométrica es según ***(…).***

16. Que el template se registra en la base de datos. Que se envía una señal para propagar el template solo a los dispositivos donde el empleado realiza su jornada laboral.

17. Que en relación a cómo se garantiza que la huella dactilar captada se borra al finalizar el proceso de captación, manifiesta lo siguiente:

> *"En ningún caso se guarda la imagen de la huella dactilar ya que no se obtiene, la respuesta obtenida por el módulo es el template.*
> *Todos estos procedimientos y criterios están basados en la especifica la norma* ***(...)."***

No se aporta el estándar ***(...).***

18. Que en respuesta a la información requerida sobre la descripción detallada paso a paso del proceso completo seguido por un empleado para acceder a su centro de trabajo y fichar el inicio de la jornada laboral usando los dispositivos lectores de huella dactilar y, en su caso, sin utilizarlos, CTC manifiesta:

> *"El lector de huella es un dispositivo que se ubica en una zona accesible y de paso en el cual los empleados registran los diferentes marcajes a lo largo de la jornada laboral, para ello pueden utilizar su huella dactilar y el sistema calcula el hash que se comparará con el registrado en el momento de su activación en el sistema (registro del hash inicial de la huella y asociación al empleado). Una vez el sistema reconoce el hash se presenta opción de tipo de marcaje, ej: entrada, salida o pausa, los marcajes son sincronizados con el servidor central a través de una red privada. No se recoge ninguna información más.*
> *El empleado puede necesitar otras vías para el uso del dispositivo (ej. lectura de huella insuficientemente buena) o declinar el uso de su huella para el proceso de marcaje, en ambos casos podrás realizarlo mediante tarjeta RFID."*

En relación al contenido de la base de datos:

19. Aporta extracción de su base de datos donde constan, para 100 registros, los datos ***(…)***. Se comprueba que el "código" está compuesto de números y letra. ***(…)***. En la extracción de estos datos consta que el hash de la huella se encuentra en una tabla diferente a la tabla donde se encuentran los datos identificativos de los empleados.

Sin embargo, no se ha podido constatar las posibles medidas de seguridad que pudieran estar implantadas para separar el acceso a ambas tablas.

20. Aporta captura de pantalla de sus sistemas donde constan un total de ******CANTIDAD.1*** huellas dactilares de empleados almacenadas.

21. Aporta un extracto de la base de datos con todos los usuarios dados de baja del sistema con ******CANTIDAD.2*** así como otro extracto con las fechas de borrado de cada huella con ******CANTIDAD.3***.

Se comprueba que la tabla de bajas de empleados tiene el campo *ID* extraído del campo *usuario.id* y la tabla de borrado de huellas tiene el campo *USER_ID.* Se comprueba que buscando coincidencias por los campos *ID* y *USER_ID,* para

***CANTIDAD.4** empleados coincide exactamente la fecha de baja con la fecha de borrado de huella.

Se comprueba asimismo que existen borrados de huella anteriores a la fecha 29/12/2021. En total son ***CANTIDAD.5** borrados de huella anteriores al 29/12/2021:

Finalmente se comprueba que el primer borrado de huella ocurre en la fecha 25/03/2020

22. Que en relación al borrado de huellas manifiesta que las plantillas biométricas se eliminan completamente del sistema en un proceso automático de sincronización de empleados (4 veces al día). Que al tratarse de un proceso automático se garantiza que se cumple el objetivo de eliminación del dato.

En relación a la evaluación de impacto:

23. Que justifican el cumplimiento con la minimización de datos, así como el análisis de necesidad y proporcionalidad y el proceso seguido para garantizar que los datos recabados no se usen para otra finalidad, manifestando lo siguiente:

> *"Justificamos la aplicación del principio de minimización, en el sentido de que en cada una de las operaciones que constituyen el tratamiento, los datos y operaciones son las mínimas y necesarias para abordar los fines del tratamiento. Para realizar las consultas de fichaje, es necesario tener el hash de la huella dactilar asociado al código y por relación al nombre y apellido del Empleado, en caso contrario, no hay manera de saber a quién corresponde la jornada laboral. Por otra parte, y en relación a la finalidad de control de acceso asociada a temas de prevención de riesgos laborales, en caso de una emergencia (P.E. incendio, ...) es necesario saber qué personas se encuentran dentro de la instalación.*
> *Respecto a la ponderación de la proporcionalidad del tratamiento, atendiendo a los siguientes criterios:*
> *Juicio de idoneidad: para conseguir el objetivo de control de acceso y de la jornada laboral, el sistema a través del hash de la huella dactilar, nos ha resultado el adecuado para el fin que se persigue. El umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento, debe ser prácticamente del 100%, se trata del cumplimiento de una obligación legal y de garantizar la seguridad en el ámbito laboral. La eficacia de este sistema, consideramos que nos ayuda a alcanzar este umbral.*
> *Juicio de necesidad: El correcto control de la jornada laboral, así como el control de acceso al servicio, es relevante y para alcanzar la finalidad perseguida, este sistema nos ofrece una mayor fiabilidad respecto a otros. Se habían utilizado otros sistemas, p.e el fichaje con tarjeta, pero tras la experiencia con el mismo, no nos proporcionaba la suficiente eficacia para el objetivo perseguido. Utilizando el sistema de tarjeta para el fichaje, experimentamos que, en determinadas ocasiones, se cedía la tarjeta a otra persona que no era la titular de la misma, con todos los riesgos que suponen para la seguridad laboral y la inexactitud del registro de jornada.*

Consideramos que no existe un tratamiento alternativo que sea igualmente eficaz para el logro de la finalidad perseguida, atendiendo a facilitar al máximo el uso del sistema al empleado, veracidad de los registros y seguridad laboral
Juicio de proporcionalidad en sentido estricto: Cuando realizamos la valoración inicial de implementar este sistema, consideramos que la gravedad del riesgo para los derechos y libertades de los empleados y la intromisión en su privacidad, era nula. No se almacenan las huellas dactilares de los Empleados tampoco pueden reproducirse las mismas desde los hash.
Por otra parte, ponderando el beneficio del social para los Empleados, valoramos que resultaba más positivo y cómodo para ellos, evitando situaciones p.e. en que se extravía la tarjeta, o la olvidan en el vehículo... , produciendo retrasos en los fichajes que a quién más perjudica es a los propios interesados.
Respecto a la Caducidad: el tratamiento desaparece, en el momento en que se suspende la relación laboral con el Empleado. Los hashes son eliminados.
Respecto al uso para otras finalidades: La única función que permite el sistema con el uso de la huella es el registro de marcaje y/o acceso al centro, no habilita ningún otro acceso a datos del empleado, ni se utiliza como parte de identificación para otros sistemas o funcionalidades."

En relación al acceso a las lectoras, servidor de la aplicación y servidor de bases de datos y a la seguridad en general:

24. Que a las lectoras no se puede acceder directamente sino a través de la aplicación o bien accediendo a la web embebida en el dispositivo, con unas únicas credenciales de administración. Que no se puede acceder a las lectoras desde ningún otro punto de la red que no sea desde el servidor, ya que tienen implantadas restricciones de red.

25. Que el servidor de la aplicación está aislado del dominio. Que solo dispone de 3 usuarios de acceso; "CLI.gruntc", "CLI.***EMPRESA.1", "PRV.gruntc".

Aporta logs de acceso a dicho servidor donde constan autenticación exitosa exclusivamente dos de esos usuarios.

26. Aporta logs de acceso al servidor de base de datos donde constan que acceden usuarios "*Account Name*" de los que no se han aportado datos, como "*DWM-12*", "*SRVINTEMO$*" o "-".

27. Aporta logs de acceso a la aplicación que controla el sistema así como los usuarios con permisos de acceso a esta aplicación y los usuario eliminados. En estos listados constan accesos a la aplicación de los usuarios "*CTT*", "*CTT Valencia*", "*Gestamp*", "*...*", "*Makro*" los cuales no constan en el listado de usuarios con permiso de acceso a la aplicación ni tampoco constan en el listado de usuarios eliminados.

28. Aporta documentos de Procedimiento de acceso a servidores y aplicaciones, así como Procedimiento de altas y bajas de usuarios de sistemas.

29. Que en contestación al requerimiento de justificación de por qué no puede prescindir de la asociación directa entre el hash de la huella dactilar y el nombre y apellidos, manifiestan:

> *"El hash de la huella se relaciona con un código de empleado que podría ser suficiente para completar el registro de jornada, pero claramente insuficiente para poder realizar el seguimiento de los marcajes en tiempo real por parte de los responsables del centro. Igualmente, no permitiría tener control sobre la localización de las personas (dentro-fuera) a efectos de prevención de riesgos laborales.*
> *Cabe destacar que el módulo del dispositivo, al comparar el hash en tiempo real, lo que retorna es el código. Y es a partir de éste, donde se realizan todas las funcionalidades, el hash no vuelve a intervenir de ninguna manera en el proceso."*

30. Que en contestación a que acredite cómo evita que los datos de huellas sean reutilizados para otros fines o por otros responsables, manifiesta:

> *"Los dispositivos biométricos están inventariados con sus datos correspondientes a instalación, ubicación, así como su estado. Dispositivos retirados por cierre son recuperados, eliminado el contenido y almacenados para posterior uso.*
> *Los datos biométricos no tienen ningún sentido en la instalación, no aportan información interpretable ni relevante. El uso de los datos biométricos también está totalmente descartado en cualquier otro uso, su uso como identificación no nos aporta valor más allá de la recogida de los marcajes de una forma ágil, fácil para el empleado y que permita evitar marcajes fraudulentos. El hardware es dedicado y tampoco se le puede dar un uso diferente al que el fabricante diseñó."*

CONCLUSIONES DEL INFORME DE ACTUACIONES PREVIAS DE INVESTIGACIÓN

1. Hay claros indicios de que el usuario accedió a una Url que podría ser la del portal del empleado, pero no consta tal evidencia. Sí consta que el reclamante aceptó el documento de información sobre protección de datos, pero lo hizo en fecha anterior a la última actualización del documento informativo. En esta última actualización del documento consta información específica al tratamiento de huella, aunque solo haciendo mención a dicho tratamiento con una frase.

2. Consta un email enviado en octubre 2021 a la organización con la actualización del documento de información en protección de datos.

3. Consta otro email enviado, aunque ya en marzo 2022, con información más específica del tratamiento de huellas.

4. En relación al funcionamiento del sistema, éste funciona con una comparación de huellas 1:N, sin embargo en la información de protección de datos proporcionada consta que se trata de un sistema de autenticación, no de identificación.

5. En relación al borrado de huellas, constan hash de huellas borradas con fecha anterior al primer envío de información sobre protección de datos con información del tratamiento de huellas y anterior también a la fecha en la que manifiestan que comenzó el tratamiento.

6. En relación a la seguridad del sistema:

a. Constan almacenados y relacionados los datos identificativos del empleado y su hash de huella. No se le ha llegado a requerir a CTC la justificación de las medidas de seguridad implantadas para impedir una eventual asociación no deseada de estos datos, aunque sí se le ha requerido justificación de por qué necesitan la asociación directa entre los datos identificativos y el hash de huella cuya contestación parece insuficiente.

b. En la información aportada por CTC se constata el acceso de algunos usuarios que no constan en los listados de usuarios con privilegios de acceso facilitados, tanto a la aplicación como al servidor de base de datos.

c. CTC no ha acreditado cómo queda garantizado el borrado de la huella tras su captura.

QUINTO:

Con fecha 12 de mayo de 2023, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la parte reclamada, por la presunta infracción del Artículo 35 del RGPD, Artículo 32 del RGPD y Artículo 13 del RGPD, tipificadas en los Artículos 83.5 del RGPD y Artículo 83.4 del RGPD.

SEXTO:

Notificado el citado acuerdo de inicio 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), la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifiesta lo siguiente:

En relación con la imputación del artículo 13 del RGPD por la falta de información a los trabajadores en relación con la puesta en marcha de un sistema de fichaje mediante el tratamiento de datos biométricos, la parte reclamada se limita a reafirmar argumentos ya expuestos en la fase de actuaciones previas de investigación: (haber corregido la cláusula informativa; la parte reclamante habría accedido al contenido informativo de la cláusula; la adopción de medidas informativas adicionales y posteriores; y la existencia de sistemas alternativos a la huella dactilar para el fichaje

En relación con la vulneración del artículo 32 alega que la huella dactilar no se almacena. Lo que hace el sistema es convertir la huella en un identificador numérico; y que ya se habría acreditado que los usuarios que no deberían acceder a los datos se encontraban dados de baja, sin que pudieran tener acceso a la aplicación.

Finalmente, nada se alegó en relación con el incumplimiento del artículo 35 del RGPD, relativo a la ausencia de una verdadera evaluación de impacto.

SÉPTIMO:

Con fecha 2 de noviembre de 2023 se formuló propuesta de resolución, proponiendo

*"PRIMERO Que por la Directora de la Agencia Española de Protección de Datos se sancione a **CTC EXTERNALIZACIÓN, S.L.**, con NIF **B60924131**,*

- *Por una infracción del Artículo 13 del RGPD, tipificada en el Artículo 83.5 del RGPD, con una multa de 200.000€ (DOSCIENTOS MIL EUROS).*

- *Por una infracción del artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD con una multa de 100.000€ (CIEN MIL EUROS).*

- *Por una infracción del artículo 35 del RGPD, tipificada en el Artículo 83.4 del RGPD, con una multa de 100.000,00 € (CIEN MIL EUROS)*

*SEGUNDO Que por la Directora de la Agencia Española de Protección de Datos se ordene a **CTC EXTERNALIZACIÓN, S.L.**, con NIF **B60924131**, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 6 meses, acredite haber procedido al cumplimiento de las siguientes medidas:*

- *Informar a todos los trabajadores de manera adecuada, incluyendo todos los extremos que no se han incluido hasta ahora, conforme a lo detallado en los fundamentos de derecho de esta propuesta*

- *Establecer las medidas de seguridad necesarias para evitar el acceso por personal no expresamente autorizado, así como para garantizar el borrado de la huella tras su captura. También para separar el acceso a las tablas que contienen el hash de las huellas y los datos identificativos de los trabajadores.*

- *Elaborar una evaluación de impacto de protección de datos que contenga todos los extremos previstos en el artículo 35 del RGPD, en particular teniendo en cuenta los defectos señalados en esta propuesta. "*

OCTAVO:

Notificada la citada propuesta de resolución 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), la parte reclamada presentó escrito de alegaciones en el que, en síntesis, manifiesta lo siguiente:

En relación con la imputación del artículo 13 RGPD: a este respecto, el reclamado se limita a reiterar alegaciones ya presentadas al acuerdo de inicio:

- Reitera que CTC efectuó correcciones a la versión inicial de la cláusula de protección de datos (fecha octubre 2021) para una adecuada información a los trabajadores.

- En caso de haberse ocasionado algún perjuicio, el derecho de los posibles afectados habría quedado plenamente garantizado mediante la aplicación de las medidas posteriores informativas adoptadas por CTC
- La información sobre el tratamiento del dato personal relativo a la huella dactilar de los empleados de CTC habría estado disponible con carácter previo a la puesta en funcionamiento, que se produjo en diciembre de 2021.
- CTC estableció un cartel informativo junto a los dispositivos de fichaje y también envió un e-mail informativo.
- En todo caso no habría habido una falta total de información, sino aspectos que necesitarían aclaración

En relación con la imputación del artículo 32 RGPD:

- También reitera lo ya alegado en fase de instrucción, acerca de haber identificado a las empresas intervinientes en el establecimiento del sistema y haber aportado documentos sobre la tecnología utilizada
- Indica que en su momento se aportó una declaración responsable de la empresa INTEMO acreditativa del hecho de que no se almacena la huella dactilar
- Como novedad respecto a anteriores alegaciones, CTC aportan un informe sobre registros de usuarios en el sistema.
- El acceso al sistema, afirma, solo se llevaría a cabo por “usuarios técnicos con finalidad de controlar” el sistema

En relación con la imputación del artículo 35 RGPD

- CTC reproduce lo que considera que es el reproche que en el expediente se le dirige, que sería únicamente, a su juicio, que el documento de evaluación de impacto aportado por el reclamado no constituiría una “evaluación de impacto” en los términos del RGPD, al adolecer de defectos sustanciales como no determinarse la finalidad del tratamiento o no contener un juicio acerca de la necesidad y proporcionalidad del sistema.

- Invoca diversos precedentes de resoluciones de esta AEPD:

    - E/00793/2016: el reclamado interpreta esta resolución en el sentido de que, si se ha informado a los trabajadores sobre la implantación del sistema, la AEPD no entraría a evaluar la idoneidad del mismo.
    - E/10900/2019: conforme a esta resolución, el sistema biométrico de acceso puede implantarse si hay una base jurídica, aun sin consentimiento trabajadores
    - E/03925/2020. La AEPD, a juicio del reclamado, estaría dando por bueno un supuesto “similar” en que no existiría Evaluación de impacto.

- En relación con el principio de proporcionalidad, alega que en el expediente anterior PS/00050/2021 se impuso una multa de 20.000€ por la infracción de carencia de evaluación de impacto, mientras que en este caso se estaría sancionando con 100.000€.

De las actuaciones practicadas en el presente procedimiento y de la documentación obrante en el expediente, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO.

A.A.A. (en adelante, la parte reclamante) con fecha 14 de febrero de 2022 presentó reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra **CTC EXTERNALIZACIÓN, S*.L.*** con NIF ***B60924131***. Los motivos en que basa la reclamación son los siguientes:

Se reclama que en la entidad CTC EXTERNALIZACIÓN, S.L. se han solicitado datos biométricos, la huella dactilar, a los empleados con la finalidad de implantar un sistema de fichaje basado en ese dato.

Se expone que en el momento de tomar los datos biométricos no se comunicó que la información se encontraba en el portal del empleado, localizada en la parte más recóndita de la aplicación a la que no tienen acceso todos los trabajadores que emplean el nuevo sistema de fichaje.

SEGUNDO.

Se envió un email enviado a ctc@grupoctc.com en fecha 28/10/2021 con asunto "*Actualización Políticas de protección de datos CTC EXTERNALIZACIÓN S.L.U.*" donde consta:

> *"[…]*
> *Por medio de la presente comunicación queremos informar que CTC EXTERNALIZACIÓN S.L.U., en su obligación de cumplimiento normativo, ha procedido a la actualización de sus Políticas de protección de datos respecto al tratamiento de los datos de carácter personal. Pueden acceder a través del Portal del Empleado, a la publicación de las nuevas políticas:*
> *POL/RGPD CTC EXTER_2021: Cláusula Protección de datos de Empleados*
> *Debe leer atentamente las presentes cláusulas y pulsar su aceptación. En caso de cualquier duda puede contactar con el Departamento de Protección de Datos, a través del correo electrónico:* ***dpo@grupoctc.com***
> *[…]"*

TERCERO.

Por parte de CTC se aporta cláusula informativa donde consta como Fecha: 02/03/2018, fecha de Actualización: 26/10/2021 y el código "POL/RGPD CTC EXTER_2021". En ese documento consta exclusivamente la siguiente referencia específica al tratamiento de huellas dactilares:

> *"[…]*
> *Está instalado un lector de huella dactilar para acceso a oficinas.*
> *[…]"*

CUARTO.

Constan capturas de pantalla de los sistemas de CTC donde consta que el reclamante ha accedido a una aplicación codificada como “com.ctc.portal[…]” en fechas entre 23/08/2021 y el 16/12/2021. Consta asimismo que el reclamante ha ejecutado la acción “sign” respecto del objeto “POL06 2018 CLAUSULA PROTECCION DATOS” en fecha 23/08/2021 10:20. Consta asimismo que existe un “agreement_date” relacionado con el reclamante y el documento “POL06_2018_CLAUSULA.pdf” en fecha 23/08/2021 10:20:16. Consta que la última “agreement_date” asociada al reclamante fue en fecha 23/08/2021.

QUINTO.

Tras recibir el traslado de la reclamación por parte de la AEPD, CTC publicó una cláusula informativa más detallada “Cláusula informativa uso huella dactilar para control de la jornada laboral”, la cual se envió por correo electrónico.

Aporta correo electrónico enviado en fecha 22/03/2022 con esta cláusula informativa.

En dicha cláusula informativa consta información específica sobre el tratamiento de huella dactilar con los apartados de responsable, legitimación, finalidad, destinatarios, plazo de conservación, derechos y medidas de seguridad. Que consta en esta información proporcionada “Se trata de un sistema de autenticación/verificación no de identificación.”

SEXTO.

El lector de huella es un dispositivo que se ubica en una zona accesible y de paso en el cual los empleados registran los diferentes marcajes a lo largo de la jornada laboral. Para ello pueden utilizar su huella dactilar y el sistema calcula el *hash* que se comparará con el registrado en el momento de su activación en el sistema (registro del hash inicial de la huella y asociación al empleado).

El sistema está configurado para realizar una comparación de huellas 1:N. Dispone del módulo biométrico CBM que calcula el *template* y lo compara con los que tiene almacenados. En caso de existir correspondencia con algún patrón almacenado da por buena la lectura.

SÉPTIMO.

La parte reclamada aporta extracción de su base de datos donde constan, para 100 registros, los datos de nombre, apellidos, id de usuario, código, fecha de alta, fecha de baja, hash de la huella dactilar. Se comprueba que el “código” está compuesto de números y letra. Se comprueba que la letra cumple la regla ***(…)***. En la extracción de estos datos consta que el hash de la huella se encuentra en una tabla diferente a la tabla donde se encuentran los datos identificativos de los empleados. Sin embargo, no se ha podido constatar las posibles medidas de seguridad que pudieran estar implantadas para separar el acceso a ambas tablas.

OCTAVO.

En los sistemas de CTC constan un total de ***CANTIDAD.1 huellas dactilares de empleados almacenadas. CTC aporta un extracto de la base de datos con todos los usua-

rios dados de baja del sistema con ***CANTIDAD.2 así como otro extracto con las fechas de borrado de cada huella con ***CANTIDAD.3.

Se comprueba que la tabla de bajas de empleados tiene el campo ID extraído del campo usuario.id y la tabla de borrado de huellas tiene el campo USER_ID. Se comprueba que buscando coincidencias por los campos ID y USER_ID, para ***CANTIDAD.4 empleados coincide exactamente la fecha de baja con la fecha de borrado de huella.

Se comprueba asimismo que existen borrados de huella anteriores a la fecha 29/12/2021. En total son ***CANTIDAD.5 borrados de huella anteriores al 29/12/2021.Finalmente se comprueba que el primer borrado de huella ocurre en la fecha 25/03/2020

NOVENO.

A las lectoras no se puede acceder directamente sino a través de la aplicación o bien accediendo a la web embebida en el dispositivo, con unas únicas credenciales de administración. No se puede acceder a las lectoras desde ningún otro punto de la red que no sea desde el servidor, ya que tienen implantadas restricciones de red.

DÉCIMO.

EL servidor de la aplicación está aislado del dominio, y solo dispone de 3 usuarios de acceso; “CLI.gruntc”, “CLI.***EMPRESA.1”, “PRV.gruntc”.v CTC aporta logs de acceso a dicho servidor donde constan autenticación exitosa exclusivamente dos de esos usuarios.

DÉCIMOPRIMERO.

El documento de evaluación de impacto aportado por CTC contiene lo siguiente:

> *“Justificamos la aplicación del principio de minimización, en el sentido de que en cada una de las operaciones que constituyen el tratamiento, los datos y operaciones son las mínimas y necesarias para abordar los fines del tratamiento. Para realizar las consultas de fichaje, es necesario tener el hash de la huella dactilar asociado al código y por relación al nombre y apellido del Empleado, en caso contrario, no hay manera de saber a quién corresponde la jornada laboral. Por otra parte, y en relación a la finalidad de control de acceso asociada a temas de prevención de riesgos laborales, en caso de una emergencia (P.E. incendio, ...) es necesario saber qué personas se encuentran dentro de la instalación.*
> *Respecto a la ponderación de la proporcionalidad del tratamiento, atendiendo a los siguientes criterios:*
> *Juicio de idoneidad: para conseguir el objetivo de control de acceso y de la jornada laboral, el sistema a través del hash de la huella dactilar, nos ha resultado el adecuado para el fin que se persigue. El umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento, debe ser prácticamente del 100%, se trata del cumplimiento de una obligación legal y de garantizar la seguridad en el ámbito laboral. La eficacia de este sistema, consideramos que nos ayuda a alcanzar este umbral.*

Juicio de necesidad: El correcto control de la jornada laboral, así como el control de acceso al servicio, es relevante y para alcanzar la finalidad perseguida, este sistema nos ofrece una mayor fiabilidad respecto a otros. Se habían utilizado otros sistemas, p.e el fichaje con tarjeta, pero tras la experiencia con el mismo, no nos proporcionaba la suficiente eficacia para el objetivo perseguido. Utilizando el sistema de tarjeta para el fichaje, experimentamos que, en determinadas ocasiones, se cedía la tarjeta a otra persona que no era la titular de la misma, con todos los riesgos que suponen para la seguridad laboral y la inexactitud del registro de jornada.
Consideramos que no existe un tratamiento alternativo que sea igualmente eficaz para el logro de la finalidad perseguida, atendiendo a facilitar al máximo el uso del sistema al empleado, veracidad de los registros y seguridad laboral
Juicio de proporcionalidad en sentido estricto: Cuando realizamos la valoración inicial de implementar este sistema, consideramos que la gravedad del riesgo para los derechos y libertades de los empleados y la intromisión en su privacidad, era nula. No se almacenan las huellas dactilares de los Empleados tampoco pueden reproducirse las mismas desde los hash.
Por otra parte, ponderando el beneficio del social para los Empleados, valoramos que resultaba más positivo y cómodo para ellos, evitando situaciones p.e. en que se extravía la tarjeta, o la olvidan en el vehículo... , produciendo retrasos en los fichajes que a quién más perjudica es a los propios interesados.
Respecto a la Caducidad: el tratamiento desaparece, en el momento en que se suspende la relación laboral con el Empleado. Los hashes son eliminados.
Respecto al uso para otras finalidades: La única función que permite el sistema con el uso de la huella es el registro de marcaje y/o acceso al centro, no habilita ningún otro acceso a datos del empleado, ni se utiliza como parte de identificación para otros sistemas o funcionalidades."

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 Cuestiones previas

En el presente caso, de acuerdo con lo establecido en el artículo 4.1 del RGPD, consta la realización de un tratamiento de datos personales, toda vez que CTC EXTERNALIZACIÓN, S.L. realiza esta actividad 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: «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.

Conforme a los datos obtenidos en AXESOR, el volumen de negocio de la parte reclamada para el ejercicio de 2020 fue ***(…).***

Adicionalmente el artículo 4.2 del Reglamento define el "tratamiento" de datos personales 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"

A este respecto conviene referirse a la distinción que realiza el interesado en sus alegaciones acerca de la diferencia entre "identificación" y "autenticación" en relación con el tratamiento de datos biométricos. Afirma que no se estaría utilizando un sistema de "identificación" (es decir, uno que determinara la identidad del sujeto partiendo de su huella), sino de "autenticación" (esto es, uno que verifica que la huella dactilar se corresponde con la previamente aportada).

A este respecto deben significarse dos cosas. En primer, lugar, que resulta más que dudoso que el sistema utilizado en este caso se trate de uno de "autenticación". Los lectores de huella dactilar instalados no comparan la huella del sujeto con algún documento o soporte que el mismo utilice en el momento de fichar, sino que lo que hace es comparar dicha huella, leída en el momento del fichaje, con el total de huellas previamente registradas por los trabajadores. Con ello, la comparación es 1:N.

Pero, lo más importante es que ya desde las Directrices 05/2022, del CEPD, sobre Tecnologías de Reconocimiento facial, se deja claro que ambos sistemas (identificación y autenticación) constituyen un tratamiento de categorías especiales de datos personales. En efecto, el epígrafe 12 de las Directrices establecen lo siguiente:

> *(12) While both functions – authentication and identification – are distinct, they both relate to the processing of biometric data related to an identified or identifiable natural person and therefore constitute a processing of personal data, and more specifically a processing of special categories of personal data.*
>
> *(12) Mientras ambas funciones – autenticación e identificación- son distintas, las dos se refieren al tratamiento de datos biométricos relacionados con una persona identificada o identificable, y con ello constituyen un tratamiento de*

datos personales, y más concretamente el tratamiento de categorías especiales de datos personales. (la traducción es nuestra)

De lo antedicho resulta que el régimen previsto en el RGPD para las categorías especiales de datos personales es aplicable al presente supuesto.

III Contestación a las alegaciones relativas al incumplimiento del artículo 13 RGPD

En respuesta a las alegaciones presentadas por la entidad reclamada tanto al acuerdo de inicio como a la propuesta de resolución se debe señalar lo siguiente:

En relación con la imputación del artículo 13 del RGPD por la falta de información a los trabajadores en relación con la puesta en marcha de un sistema de fichaje mediante el tratamiento de datos biométricos, la parte reclamada reitera argumentos ya expuestos en la fase de actuaciones previas de investigación:

- El hecho de haber corregido la cláusula informativa a los trabajadores. A este respecto, CTC reconoce expresamente haber efectuado la corrección en fecha posterior a haber recibido la reclamación a través de esta Agencia.

- La parte reclamante habría accedido al contenido informativo de la cláusula

- La adopción de medidas informativas adicionales y posteriores. También, haber ubicado carteles informativos junto a los dispositivos de fichaje.

- La existencia de sistemas alternativos a la huella dactilar para el fichaje de los empleados, particularmente mediante el uso de una tarjeta RFID.

En el caso que nos ocupa, se ha acreditado que la parte reclamada no informó correctamente sobre el tratamiento. La cláusula informativa a que hace referencia y que habría sido incluida en el “portal del empleado” de la empresa en octubre de 2021 adolece de importantes defectos. Estos además corroborados por la subsanación que se hizo la versión de la cláusula informativa, sin fecha, pero elaborada tras el requerimiento de información de esta Agencia y, conforme afirma el informe de actuaciones previas, enviado a los trabajadores en marzo de 2022:

- No incluye cuál/es son los tratamientos objeto de dicha cláusula informativa. De hecho, la única referencia específica al tratamiento de la huella viene de una muy escueta mención en el apartado 3 “Está instalado un lector de huella dactilar para acceso a oficinas”. No indica si está activado ni si recoge la huella y, desde luego, no incluye el dato de la huella dactilar entre los que son objeto de tratamiento.

  Por el contrario, la cláusula posterior (marzo de 2022) contiene una referencia específica al tratamiento de la “huella dactilar para control de la jornada laboral”

  A este respecto es importante señalar que la cláusula informativa parece referirse a una pluralidad de tratamientos, a los que engloba en un solo documento redactado de manera muy escueta. No se relacionan los

tratamientos realizados, y para todos ellos aplica una base legitimadora, que sería la ejecución del contrato. Además, afirma que el tratamiento de datos personales se realiza con múltiples finalidades:

- Gestionar la relación laboral con los empleados de la compañía.
- Gestión contable administrativa de datos de empleados.
- Confección de nóminas.
- Prevención de riesgos laborales.
- Formación

- En la primera cláusula informativa se realizaba una información conjunta para lo que se supone que eran múltiples tratamientos de datos personales que realizaba la empresa. Pues bien, para todos ellos el documento original informaba como base de legitimación sencillamente la expresión "Relación contractual laboral".

  Sin embargo, en la versión posterior, esto se ha corregido y, refiriéndose específicamente al tratamiento de la huella dactilar, se afirma que la legitimación vendría del *"cumplimiento de una obligación legal (artículo 34.9 del Estatuto de los trabajadores), referente al control de la jornada laboral*." Como se observa, una base legitimadora totalmente diferente.

  De hecho, consultado el Registro de Actividades de tratamiento aportado por la parte reclamada, en el tratamiento "Control de acceso y jornada laboral mediante huella dactilar", en el campo "Legitimación de las operaciones de tratamiento" figura "cumplimiento de una obligación legal (artículo 34.9 del Estatuto de los trabajadores)".

  Por todo ello, no se cumplió en este aspecto con el deber de información a los trabajadores en la información inicial que se suministró. A este respecto, debe recordarse que el mencionado artículo 13.2.e) del RGPD establece que debe informarse sobre "*si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos".*

- En relación con el período de conservación de los datos, en la versión inicial de la cláusula informativa se indicaba *"Los datos proporcionados se conservarán mientras dure la relación contractual y durante los años necesarios para cumplir con las obligaciones legales*". Ello además, como se ha indicado más arriba, en relación con los múltiples tratamientos que se realizaban. Sin embargo, en la versión posterior se aclara cuáles son los períodos de conservación y bloqueo, concretando además el plazo total en años *"Los datos se conservarán mientras dure la relación laboral. Los datos respecto a la jornada laboral se conservarán bloqueados y pseudonimizados durante lo exigido por cumplimiento legal (4 años.)*"

- Ni en la versión inicial de la cláusula ni en la posterior se informa sobre el derecho a presentar reclamación ante la Autoridad de control (art. 13.2.d) del RGPD).

En relación con el presunto carácter voluntario del uso del sistema de fichaje con huella dactilar, recordar que no es objeto de este expediente dilucidar si se encontraban, o no, los trabajadores obligados al uso de ese sistema. Con independencia de la legitimación respecto del tratamiento de los datos personales o de la posible obligatoriedad respecto de su suministro, era obligación del responsable del tratamiento cumplir con sus deberes de información establecidos en el artículo 13 del RGPD.

Por todo ello, no puede considerarse que la parte reclamada haya cumplido con sus obligaciones de información del artículo 13 del RGPD. Llama la atención, además, que el texto del correo electrónico enviado por la empresa haga únicamente una referencia a la "actualización de sus políticas de protección de datos", sin referencia ninguna a la implantación de un sistema de fichaje mediante huella dactilar (lo que a buen seguro habría fomentado la consulta de la cláusula informativa que, por lo que se ha visto, era totalmente defectuosa).

IV Contestación a las alegaciones relativas al incumplimiento del artículo 32 RGPD

En relación con esta infracción, relativa a la falta de medidas de seguridad en el tratamiento de los datos biométricos, CTC alega lo siguiente:

En primer lugar, respecto al tratamiento del dato de la huella, se afirma que la imagen de la huella dactilar no se almacena. Lo que hace el sistema es convertir la huella en un identificador numérico. De este modo, cuando el trabajador ficha, se compara ese identificador con el previamente asignado a dicha huella. Con ello, la huella dactilar no podría reproducirse a partir de ese identificador numérico. A este respecto, Aporta un certificado de la empresa IDEMIA IDENTITY & SECURITY FRANCE SAS que afirma que "*no hay forma de recuperar las plantillas en caso de robo, ya que es imposible recrear una imagen de una huella a partir de los puntos típicos*".

En relación con esta alegación debe señalarse que la imputación de la infracción del artículo 32 no se basa en el factor alegado por el reclamado, sino en lo reflejado en el acuerdo de inicio, esto es:

> *"b. En la información aportada por CTC se constata el acceso de algunos usuarios que no constan en los listados de usuarios con privilegios de acceso facilitados, tanto a la aplicación como al servidor de base de datos.*
>
> *c. CTC no ha acreditado cómo queda garantizado el borrado de la huella tras su captura.*
>
> *d. Conforme se detalla en el informe de actuaciones previas de investigación, en la extracción de los datos consta que el hash de la huella se encuentra en una tabla diferente a la tabla donde se encuentran los datos identificativos de los empleados. Sin embargo, no se ha podido constatar las posibles medidas de*

seguridad que pudieran estar implantadas para separar el acceso a ambas tablas."

En relación con los accesos a la aplicación que controla el sistema, de los que esta Agencia ha deducido que se podrían producir accesos por usuarios que no tenían permisos para ello, se afirma en las alegaciones que en los documentos que se facilitaron durante el período de inspección ya se habría acreditado que dichos usuarios se encontraban dados de baja, sin que pudieran tener acceso a la aplicación. Aparte, señalan que también fue aportada por su parte las políticas de seguridad e información.

En cuanto a la cuestión del acceso por usuarios que no dispondrían de permisos, puede señalarse lo siguiente, analizada la documentación aportada por el interesado en sus alegaciones al acuerdo de inicio.

- Se constata que sí están eliminados, como afirma CTC, los usuarios "CTT", "CTT Valencia", "Gestamp", "..." y "Makro". Con ello, no puede afirmarse que respecto a esos usuarios se produjeran accesos indebidos.

- En relación con el usuario "DWM-12", consta en una captura de pantalla aportada por el interesado, con membrete "Log File Viewer – SRVINTEMO" pero NO aparece en el fichero que denominan "21.a.3 AccesosSQLSERVER.log". con ello, es posible que este usuario conste en el log del servidor pero NO el log de la base de datos. Por tanto, podría darse por válida la explicación aportada relativa a tratarse de una cuenta que se genera automáticamente cuando se inicia una sesión de escritorio remoto y por tanto deducirse que no tiene por qué ser una cuenta que esté accediendo realmente a la base de datos.

- Por el contrario, los Usuarios "SRVINTEMO$" o "-" sí aparecen en el fichero denominado "21.a.3 AccesosSQLSERVER.log", esto es, donde se supone que están los accesos al servidor de la base de datos y además aparecen asociados al mensaje "An account was successfullly logged on". Estos usuarios no habían sido identificados en la contestación al requerimiento de licencias inspección. En todo caso, en las alegaciones no se explica con el suficiente detalle y claridad el asunto. Únicamente incluyen una frase algo ambigua sobre el carácter del usuario ("*En el caso de usuarios de los que no se han aportado datos, como "SRVINTEMO$" o "-" no son cuentas de usuario ni de sistema, simplemente es información que aparece en el log generado por el propio sistema operativo.*")

  No se aporta ninguna evidencia a este respecto, como por ejemplo el listado de usuarios que están dados de alta con acceso a la base de datos o confirmación de que el fichero "21.a.3 AccesosSQLSERVER.log" se refiere a logs de acceso a la base de datos.

Con posterioridad, en sus alegaciones a la propuesta de resolución, el reclamado ha aportado un informe técnico acerca de los accesos y usuarios. De ello se concluye lo siguiente:

El reclamado afirma que, en la respuesta al requerimiento de la Inspección, lo que se adjuntó habría sido una extracción del registro de eventos de Windows que incluía todos los accesos. Se entiende que lo que aportaron como respuesta al requerimiento no eran los accesos específicos a SQL Server, aunque sí lo identificaron como tal en su día. Además, parece que la información aportada como respuesta al requerimiento estaba cortada ya que era una captura de pantalla y en este informe se haría aportado de forma más completa.

Pues bien, del conjunto de la documentación aportada a lo largo del expediente (relativo a los usuarios “DWM-12”, “-“, “SRVINTEMO$” respecto a los cuales no se determinaba con claridad quiénes eran, parece, según explicación dada en alegaciones y asociada a capturas de pantalla aportadas también ahora, que están vinculados con accesos del usuario “CLI.gruntc”, sí declarado previamente como legitimado para el acceso.

Asimismo, también se adjuntan algunos accesos específicos a SQL Server y en estos se ven accesos de los usuarios “sa” y “SRVINTEMO$” y “SQLTELEMETRY”. Los usuarios están declarados, según captura de pantalla aportada también ahora, excepto la cuenta “SRVINTEMO$”. Pero respecto a esta cuenta “SRVINTEMO$” puede presumirse que ocurrirá algo similar a lo ya explicado respecto al otro log del servidor aportado, y donde se podía ver que esa misma cuenta estaba realmente vinculada a un usuario que sí estaba declarado.

Por tanto, tras el análisis de toda la información y documentación aportada ahora, no puede determinarse con total certeza el acceso de algunos usuarios que no constan en los listados de usuarios con privilegios de acceso facilitados, tanto a la aplicación como al servidor de base de datos. Como se verá más adelante, este factor es tenido en cuenta para la disminución de la cuantía de la sanción por la vulneración del artículo 32.

Finalmente, es preciso constatar que nada se ha alegado en relación con el resto de hechos imputados que se contenían en el acuerdo de inicio de este expediente. A este respecto recordamos que se indicaba lo siguiente:

> *“c. CTC no ha acreditado cómo queda garantizado el borrado de la huella tras su captura.*
>
> *d. Conforme se detalla en el informe de actuaciones previas de investigación, en la extracción de los datos consta que el hash de la huella se encuentra en una tabla diferente a la tabla donde se encuentran los datos identificativos de los empleados. Sin embargo, no se ha podido constatar las posibles medidas de seguridad que pudieran estar implantadas para separar el acceso a ambas tablas.”*

V Contestación a las alegaciones relativas al incumplimiento del artículo 35 RGPD

En relación con este incumplimiento CTC alega lo siguiente: en primer lugar invoca diversos precedentes de resoluciones de esta AEPD:

- E/00793/2016: el reclamado interpreta esta resolución en el sentido de que, si se ha informado a los trabajadores sobre la implantación del sistema, la AEPD no entraría a evaluar la idoneidad del mismo.

  En relación con este supuesto, debe resaltarse que enjuicia un caso producido antes de la entrada en vigor del actual RGPD. Y en este Reglamento se encuentran perfectamente establecidas y diferenciadas dos obligaciones. Por una parte, la información a los titulares de los datos personales de los datos que van a ser tratados y sus condiciones (art. 13). Y por otra, de la necesidad de superación de una evaluación de impacto relativa a la protección de datos, en la que se incluye "una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad" (art. 35.7.b).

  En todo casono puede afirmarse que la mera información a los trabajadores pudiera ser base legitimadora para la instalación del sistema biométrico. Y todo ello sin perjuicio de que en el presente expediente también se sanciona por la ausencia de información, con lo que ni siquiera ese requisito, que indican que sería suficiente, se habría cumplido.

- E/10900/2019: conforme a esta resolución, se alega que el sistema biométrico de acceso podría implantarse si hay una base jurídica, aun sin consentimiento trabajadores.

  A este respecto se señala que el artículo 6.1 del RGPD establece cuáles son las distintas bases de legitimación para el tratamiento de los datos personales. El consentimiento (letra a) de dicho artículo) es solo una de ellas, pudiendo concurrir efectivamente otras como la ejecución de un contrato, el cumplimiento de una obligación legal o incluso la existencia de un interés legítimo que debe ponderarse.Y que además, para el tratamiento de categorías especiales de datos personales se requiere que concurra una excepción de las del apartado 2 del artículo 9 del RGPD.

  No obstante, la concurrencia de una excepción del artículo 9.2 del RGPD junto con una base de legitimación de las del artículo 6 del RGPD, en modo alguno exime del cumplimiento del resto de obligaciones que establezca el RGPD. Y una de ellas consiste en la elaboración y superación de una evaluación de impacto de protección de datos en los supuestos establecidos en dicho Reglamento, entre los cuales se encuentra el tratamiento que está siendo objeto de este expediente.

  Con ello, no puede afirmarse que la mera existencia de una base legitimadora exima de la necesaria realización y superación de la evaluación de impacto de protección de datos en los supuestos legalmente previstos.

  Por lo demás, la resolución que pone fin a ese expediente basa su motivación en la antigua diferenciación, a efectos de determinar el tratamiento de categorías especiales de datos personales, entre "identificación" y "autenticación" para la determinación de la identidad en sistemas de fichaje con huella dactilar

Como ha quedado suficientemente explicado en el fundamento segundo de esta resolución, a partir de las Directrices 05/2022 del CEPD, sobre reconocimiento facial, la distinción entre ambos tipos de tratamientos ha desaparecido, considerándose en todo caso la existencia de un tratamiento de categorías especiales de datos personales.

- E/03925/2020. La AEPD, a juicio del reclamado, estaría dando por bueno un supuesto "similar" en que no existiría EIPD.

  Analizado el procedimiento invocado, se observa que se trata de una resolución de archivo de actuaciones, en la que el mencionado archivo obedeció a que la evaluación de impacto de protección de datos sí había sido elaborada y superada. Así, la resolución afirma lo siguiente:

  "*La reclamada ha acompañado copia de la amplia Evaluación de impacto realizada para el tratamiento de la huella digital.*

  Por lo tanto, se ha acreditado que la actuación de la reclamada, como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores."

  En consecuencia, nada tiene que ver este supuesto, en que sí se elaboró y superó la evaluación de impacto, con el enjuiciado en el presente expediente.

En relación con el principio de proporcionalidad, el reclamado alega que en el expediente de esta Agencia PS/00050/2021 se impuso una multa de 20.000€ por la infracción de carencia de evaluación de impacto, mientras que en este caso se estaría sancionando con 100.000€.

Es preciso indicar a este respecto que el artículo 83.4 del RGPD establece que la cuantía de la sanción tendrá en cuenta el volumen de negocio del reclamado. A este respecto, tal y como queda reflejado en esta resolución, se ha constatado que el volumen de negocio de la parte reclamada es de ***(…).***l mientras que los ingresos del sancionado en el PS/00050/2021 eran considerablemente inferiores Por lo demás, el resto de circunstancias tenidas en cuenta para la graduación de la sanción, son diferentes en ambos casos.

Adicionalmente debe señalarse que conforme a lo establecido en el artículo 83.1 del RGPD, las autoridades de control garantizarán que la imposición de las multas administrativas con arreglo a dicho Reglamento deberán ser en cada caso individual efectivas, proporcionadas y disuasorias.

Su apartado 2 añade que "*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:"*

VI Obligación de información incumplida. Artículo 13 RGPD

El artículo 13 del RGPD establece lo siguiente:

> *Información que deberá facilitarse cuando los datos personales se obtengan del interesado*
>
> *1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:*
>
> *a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;*
>
> *b) los datos de contacto del delegado de protección de datos, en su caso;*
>
> *c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;*
>
> *e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;*
>
> *f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al lugar en que se hayan puesto a disposición.*
>
> *2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:*
>
> *a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;*
>
> *b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;*
>
> *c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;*
>
> *d) el derecho a presentar una reclamación ante una autoridad de control;*

e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos;

f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.

4. Las disposiciones de los apartados 1, 2 y 3 no serán aplicables cuando y en la medida en que el interesado ya disponga de la información.

En ese sentido, el Considerando 60 del RGPD dice que "*Los principios de tratamiento leal y transparente exigen que se informe al interesado de la existencia de la operación de tratamiento y sus fines. El responsable del tratamiento debe facilitar al interesado cuanta información complementaria sea necesaria para garantizar un tratamiento leal y transparente, habida cuenta de las circunstancias y del contexto específicos en que se traten los datos personales. Se debe, además, informar al interesado de la existencia de la elaboración de perfiles y de las consecuencias de dicha elaboración. Si los datos personales se obtienen de los interesados, también se les debe informar de si están obligados a facilitarlos y de las consecuencias en caso de que no lo hicieran."*

En el caso que nos ocupa, puede comprobarse que la parte reclamada no informó correctamente sobre el tratamiento. La cláusula informativa a que hace referencia y que habría sido incluida en el "portal del empleado" de la empresa en octubre de 2021 adolece de importantes defectos. Estos además corroborados por la subsanación que se hizo la versión de la cláusula informativa, sin fecha, pero elaborada tras el requerimiento de información de esta Agencia y conforme afirma el informe de actuaciones previas enviado a los trabajadores en marzo de 2022:

- No incluye cuál/es son los tratamientos objeto de dicha cláusula informativa. De hecho, la única referencia específica al tratamiento de la huella viene de una muy escueta mención en el apartado 3 "Está instalado un lector de huella dactilar para acceso a oficinas". No indica si está activado ni si recoge la huella y, desde luego, no incluye el dato de la huella dactilar entre los que son objeto de tratamiento.

  Por el contrario, la cláusula posterior contiene una referencia específica al tratamiento de la "huella dactilar para control de la jornada laboral"

A este respecto es importante señalar que la cláusula informativa parece referirse a una pluralidad de tratamientos, a los que engloba en un solo documento redactado de manera muy escueta. No se relacionan los tratamientos realizados, y para todos ellos aplica una base legitimadora, que sería la ejecución del contrato. Además, afirma que el tratamiento de datos personales se realiza con múltiples finalidades:

- Gestionar la relación laboral con los empleados de la compañía.
- Gestión contable administrativa de datos de empleados.
- Confección de nóminas.
- Prevención de riesgos laborales.
- Formación

- En la primera cláusula informativa se realizaba una información conjunta para los que se supone que eran múltiples tratamientos de datos personales que realizaba la empresa. Pues bien, para todos ellos el documento original informaba como base de legitimación sencillamente la expresión "Relación contractual laboral".

  Sin embargo, en la versión posterior, esto se ha corregido y, refiriéndose específicamente al tratamiento de la huella dactilar, se afirma que la legitimación vendría de *"cumplimiento de una obligación legal (artículo 34.9 del Estatuto de los trabajadores), referente al control de la jornada laboral*." Como se observa, una base legitimadora totalmente diferente.

  De hecho, consultado el Registro de Actividades de tratamiento aportado por la parte reclamada, en el tratamiento "Control de acceso y jornada laboral mediante huella dactilar", en el campo "Legitimación de las operaciones de tratamiento" figura "cumplimiento de una obligación legal (artículo 34.9 del Estatuto de los trabajadores)".

  Por todo ello, no se cumplió en este aspecto con el deber de información a los trabajadores en la información inicial que se suministró. A este respecto, debe recordarse que el mencionado artículo 13.2.e) del RGPD establece que debe informarse sobre "*si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de no facilitar tales datos"*

- En relación con el período de conservación de los datos, en la versión inicial de la cláusula informativa se indicaba "Los datos proporcionados se conservarán mientras dure la relación contractual y durante los años necesarios para cumplir con las obligaciones legales". Ello además, como se ha indicado más arriba, en relación con los múltiples tratamientos que se realizaban. Sin embargo, en la versión posterior se aclara cuáles son los períodos de conservación y bloqueo, concretando además el plazo total en años "Los datos se conservarán mientras dure la relación laboral. Los datos respecto a la jornada laboral se conservarán bloqueados y pseudonimizados durante lo exigido por cumplimiento legal (4años.)"

- Ni en la versión inicial de la cláusula ni en la posterior se informa sobre el derecho a presentar reclamación ante la Autoridad de control (art. 13.2.d)

Por todo ello, no puede considerarse que la parte reclamada haya cumplido con sus obligaciones de información del artículo 13 del RGPD. Llama la atención, además, que el texto del correo electrónico enviado por la empresa haga únicamente una referencia a la "actualización de la actualización de sus políticas de protección de datos", sin referencia ninguna a la implantación de un sistema de fichaje mediante huella dactilar (lo que a buen seguro habría fomentado la consulta de la cláusula informativa que, por lo que se ha visto, era totalmente defectuosa)

VII Falta de información. Artículo 13 RGPD Tipificación y calificación de la infracción

De conformidad con las evidencias de las que se dispone en el presente momento del procedimiento sancionador, se considera que la parte reclamada ha omitido la información relativa al tratamiento de datos que efectúa, vulnerando con ello el artículo 13 del RGPD.

Los hechos conocidos son constitutivos de una infracción, imputable a la parte reclamada tipificada en el artículo 83.5 del RGPD que estipula lo siguiente:

"5. Las infracciones de las disposiciones siguientes 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:

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

A efectos del plazo de prescripción de las infracciones, la infracción imputada prescribe a los tres años, conforme al artículo 72.h). de la LOPDGDD, que califica de muy grave la siguiente conducta:

"h) La omisión del deber de informar al afectado acerca del tratamiento de sus datos personales conforme a lo dispuesto en los artículos 13 y 14 del Reglamento (UE) 2016/679 y 12 de esta ley orgánica."

VIII Falta de información. Artículo 13 RGPD. Sanción

Esta infracción puede ser sancionada con multa de 20 millones de € 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, de acuerdo con el artículo 83.5 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

- La duración de la infracción. La misma se habría prolongado como mínimo desde octubre de 2021 (fecha del envío de la cláusula original) hasta marzo de 2022 (que contiene la versión revisada) (art. 83.2.a) del RGPD).

- La categoría de datos personales afectados por la infracción. Debe tenerse en cuenta que la huella dactilar es un dato biométrico y conforme al artículo 9 del RGPD se consideran como categorías especiales de datos "el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física," (artículo 83.2.g) del RGPD)

Conforme a dichos criterios se estima que la sanción que corresponde es de una multa de DOSCIENTOS MIL EUROS (200.000€)

IX Falta de medidas de seguridad. Artículo 32 RGPD. Obligación incumplida

En lo que respecta a la aplicación de la normativa de protección de datos al supuesto planteado, debe tenerse en cuenta que el RGPD, en su artículo 32, exige a los responsables del tratamiento, la adopción de las correspondientes medidas de seguridad necesarias que garanticen que el tratamiento es conforme a la normativa vigente, así como garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales, solo los pueda tratar siguiendo instrucciones del responsable.

El Artículo 32 "*Seguridad del tratamiento*" del RGPD establece:

"*1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:*

a) la seudonimización y el cifrado de datos personales;

a) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

a) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

b) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

2. Al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros".

El artículo 32 no establece medidas de seguridad estáticas, sino que corresponderá al responsable determinar aquellas medidas de seguridad que son necesarias para incorporar la capacidad de garantizar la confidencialidad, la integridad y la disponibilidad de los datos personales, por lo tanto, un mismo tratamiento de datos puede implicar medidas de seguridad distintas en función de las especificidades concretas en las que tiene lugar dicho tratamiento de datos.

En consonancia con estas previsiones, el Considerando 75 del RGPD establece: *Los riesgos para los derechos y libertades de las personas físicas, de gravedad y probabilidad variables, pueden deberse al tratamiento de datos que pudieran provocar daños y perjuicios físicos, materiales o inmateriales, en particular en los casos en los que el tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo; en los casos en los que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales; en los casos en los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas; en los casos en los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales; en los casos en los que se traten datos personales de personas vulnerables, en particular niños; o en los casos en los que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados*.

Asimismo, el Considerando 83 del RGPD establece: *A fin de mantener la seguridad y evitar que el tratamiento infrinja lo dispuesto en el presente Reglamento, el responsable o el encargado deben evaluar los riesgos inherentes al tratamiento y aplicar medidas para mitigarlos, como el cifrado. Estas medidas deben garantizar un nivel de seguridad adecuado, incluida la confidencialidad, teniendo en cuenta el estado de la técnica y el coste de su aplicación con respecto a los riesgos y la naturaleza de los datos personales que deban protegerse. Al evaluar el riesgo en relación con la seguridad de los datos, se deben tener en cuenta los riesgos que se derivan del tratamiento de los datos personales, como la destrucción, pérdida o*

alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos, susceptibles en particular de ocasionar daños y perjuicios físicos, materiales o inmateriales. (el subrayado es nuestro)

En definitiva, el primer paso para determinar las medidas de seguridad será la evaluación del riesgo. Una vez evaluado será necesario determinar las medidas de seguridad encaminadas para reducir o eliminar los riesgos para el tratamiento de los datos.

El principio de seguridad de los datos requiere la aplicación de medidas técnicas u organizativas apropiadas en el tratamiento de los datos personales para proteger dichos datos contra el acceso, uso, modificación, difusión, pérdida, destrucción o daño accidental, no autorizado o ilícito. En este sentido, las medidas de seguridad son claves a la hora de garantizar el derecho fundamental a la protección de datos. No es posible la existencia del derecho fundamental a la protección de datos si no es posible garantizar la confidencialidad, la integridad y la disponibilidad de estos.

No debe olvidarse que, de conformidad con el artículo 32.1 del RGPD citado, las medidas técnicas y organizativas a aplicar para incorporar la capacidad de garantizar un nivel de seguridad adecuado al riesgo deben tener en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Por tanto, la parte reclamada, a la hora de evaluar los riesgos y determinar las medidas técnicas y organizativas apropiadas para incluir la capacidad de garantizar un nivel de seguridad adecuado al riesgo, está obligada a tener en cuenta la concreta actividad que se realiza y la tipología de datos tratados.

Por ello, derivado de la actividad a la que se dedica, la parte reclamada está obligada a realizar de forma muy especializada un análisis de los riesgos y una implantación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo de su actividad para los derechos y libertades de las personas.

En el presente caso, en el curso de la investigación realizada por esta Agencia, se ha podido constatar lo siguiente en relación a la seguridad del sistema:

a. Constan almacenados y relacionados los datos identificativos del empleado y su hash de huella.

b. CTC no ha acreditado cómo queda garantizado el borrado de la huella tras su captura.

c. Conforme se detalla en el informe de actuaciones previas de investigación, en la extracción de los datos consta que el hash de la huella se encuentra en una tabla diferente a la tabla donde se encuentran los datos identificativos de los empleados. Sin embargo, no se ha podido constatar las posibles medidas de seguridad que pudieran estar implantadas para separar el acceso a ambas tablas.

Con ello, la parte reclamada no ha acreditado la existencia de medidas técnicas y organizativas en relación con la seguridad del tratamiento de datos personales.

X Tipificación y calificación a los efectos de la prescripción de la infracción del artículo 32 del RGPD

La citada infracción del artículo 32 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece 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 efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"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:

f) La falta de adopción de aquellas medidas técnicas y organizativas que resulten apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos por el artículo 32.1 del Reglamento (UE) 2016/679."

XI Falta de medidas de seguridad artículo 32 RGPD.

Esta infracción puede ser sancionada con multa de 10 millones de € 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, de acuerdo con el artículo 83.4 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

- Duración de la infracción. La misma se habría prolongado como mínimo desde octubre de 2021 (fecha del envío de la cláusula origina), sin que el inspector hubiera constatado su cese en momento alguno. (art. 83.2.a) del RGPD).

- La categoría de datos personales afectados por la infracción. Debe tenerse en cuenta que la huella dactilar es un dato biométrico y conforme al artículo 9 del RGPD se consideran como categorías especiales de datos "el tratamiento de datos biométricos dirigidos a identificar de manera unívoca a una persona física,". A este respecto, la situación de riesgo creada por la falta de medidas de seguridad es superior respecto a datos que no tienen la consideración de especiales (artículo 83.2.g) del RGPD).

Tanto en el acuerdo de inicio como en la propuesta de resolución de este expediente se incluía como uno de los incumplimientos dentro de esta infracción el hecho de que en la información aportada por CTC se constataba el acceso de algunos usuarios que no constaban en los listados de usuarios con privilegios de acceso facilitados, tanto a la aplicación como al servidor de base de datos.

No obstante, a lo largo de este expediente, el reclamado ha facilitado información y documentación que han hecho concluir que no puede determinarse con total certeza el acceso de algunos usuarios que no constan en los listados de usuarios con privilegios de acceso facilitados, tanto a la aplicación como al servidor de base de datos.

En consecuencia, si bien en el acuerdo de inicio de esta resolución se proponía una sanción de 100.000€ para el incumplimiento del artículo 32, tras la apreciación mencionada la cuantía queda fijada en SESENTA Y CINCO MIL EUROS (65.000€).

XII Evaluación de impacto relativa a la protección de datos. Artículo 35 RGPD Obligación incumplida

Obligación de realizar y superar una evaluación de impacto de protección de datos.

El artículo 35.1 del RGPD establece que "*Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación 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.*"

En el apartado 3 de dicho artículo 35 figuran los supuestos en que es preceptiva la elaboración de la evaluación de impacto:

"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."

En este procedimiento, la necesidad de elaboración de una evaluación de impacto de protección de datos no es cuestionada por el reclamado, que además ha remitido la elaborada en relación con este tratamiento. El artículo 35.7 RGPD recoge el contenido mínimo que debe tener:

"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."

Antes de implantar un tratamiento de datos basado en esta tecnología tan intrusiva, es preciso también auditar previamente su funcionamiento, no de forma aislada sino en el marco del tratamiento concreto en que se va a emplear.

La evaluación de impacto de protección de datos personales, EIPD, aparece entonces como la herramienta exigida por el RGPD para garantizar que se cumple con esta vertiente del tratamiento, según lo establecido en el ya mencionado apartado 1 del artículo 35 del RGPD.

El tratamiento de datos biométricos es un tratamiento de alto riesgo, en virtud de lo previsto en el artículo 35.4 del RGPD, por lo que debe partirse de la base de que el tratamiento realizado en este supuesto por CTC debió estar precedido de la realización y superación de una evaluación de impacto válida, que incluyese como mínimo los apartados previstos en el artículo 35.7 del RGPD. Ello implica que no basta con realizar una EIPD, sino que habrá que superarla para cumplir con el RGPD.

A estos efectos, esta Agencia tiene publicada el documento denominado "Listas de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos". Esta lista se basa en los criterios establecidas por el Grupo de Trabajo del Artículo 29 en la guía WP248 "Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD", los complementa y debe entenderse como una lista no exhaustiva. Dentro de ella se encuentra:

“5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.”

Esta evaluación se hará con carácter previo al inicio del tratamiento, sin perjuicio de que deba entenderse como una evaluación continua o periódica, en el sentido establecido por el artículo 35.11 del RGPD, que dispone: “En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.”

Una EIPD debe cumplir con los requisitos o contenido mínimo relacionado en el artículo 35.7 del RGPD, que dispone:

“La evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas”.

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

Para analizar el cumplimiento de esta obligación por parte de CTC debe partirse de la consideración realizada por el responsable, y ya rebatida en anteriores apartados de esta resolución, de que el responsable no estaba tratando datos calificados como especiales en el artículo 9 del RGPD. Como ha quedado acreditado, el tratamiento de datos biométricos encaja en esa categoría de datos, sin que quepa aplicar distinción alguna, a estos efectos, entre identificación y autenticación

Establecido este factor, desde un principio debe descartarse la validez del documento presentado por el responsable como “evaluación de impacto” relativa a los datos personales. Y ello porque en ningún momento este documento tiene como base el tratamiento de datos personales de categoría especial como son los biométricos. Y en

consecuencia, la evaluación no ha podido tener cuenta aspectos cruciales que debieron analizarse, entre ellos:

- Si concurre alguna de las causas de levantamiento de la prohibición de tratamiento de esas categorías de datos personales de entre las previstas en el artículo 9.2 del RGPD.

- Una correcta identificación y análisis de riesgos en lo relativo al tratamiento referenciado respecto también de estas categorías de datos personales, que han de ser tomadas en consideración junto con el resto de elementos que intervienen en el tratamiento de datos personales, y cómo pueden afectar a los derechos y libertades de los titulares de los datos.

- Las medidas técnicas y organizativas de todo tipo, con mención expresa a las medidas de seguridad específicas e inherentes al tratamiento de estos datos.

Lo expuesto lleva a la conclusión, necesariamente, de que en modo alguno puede considerarse como una evaluación de impacto relativa a la protección de datos válida, cuando parte de premisas en las que el responsable del tratamiento no tienen en consideración que se encuentra ante un tratamiento de categorías especiales de datos personales, con todo lo que ello supone en cuanto al cumplimiento del RGPD y la gestión del riesgo.

Una de las obligaciones que corresponden a todo responsable de tratamiento de datos personales está asegurarse de que el tratamiento respeta los Principios previstos en el artículo 5 del RGPD. En el caso de datos biométricos, por ser de categoría especial y alto riesgo, cabe destacar la importancia esencial de respetar el principio de minimización del tratamiento/datos, previsto en el artículo 5.1.c) que indica:

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

El respeto de este principio deberá ser el punto de partida del inicio de todo tratamiento, debiendo plantearse el responsable primero que nada si este tratamiento será realmente necesario, idóneo, y proporcional antes de iniciarlo. Y si este tratamiento es de alto riesgo -caso de los biométricos- deberá reflejar esta evaluación previa de necesidad y proporcionalidad en un documento especifico denominado evaluación de impacto de protección de datos personales, de acuerdo con lo previsto en el artículo 35.7.b) del RGPD, que dispone que deberá realizarse y superarse "una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad ".

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

En la misma línea, el Grupo de Trabajo del artículo 29, en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas, indica que "*Al analizar la proporcionalidad de un sistema biométrico propuesto, es preciso considerar previamente si el sistema es necesario para responder a la necesidad identificada, es decir, si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable. Un segundo factor que debe tenerse en cuenta es la probabilidad de que el sistema sea eficaz para responder a la necesidad en cuestión a la luz de las características específicas de la tecnología biométrica que se va a utilizar. Un tercer aspecto para ponderar es si la pérdida de intimidad resultante es proporcional a los beneficios esperados. Si el beneficio es relativamente menor, como una mayor comodidad o un ligero ahorro, entonces la pérdida de intimidad no es apropiada. El cuarto aspecto para evaluar la adecuación de un sistema biométrico es considerar si un medio menos invasivo de la intimidad alcanzaría el fin deseado*".

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

Puesto que el tratamiento de datos biométricos, implica restringir derechos y libertades de los interesados, la obligación de tratar únicamente "los datos personales que sean adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados" prevista por el principio de minimización de datos/tratamiento del artículo 5.1.c) 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 (tratamiento biométrico en este caso) supera lo que se denomina como "el triple juicio de proporcionalidad".

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

Documento aportado por el reclamado.

Analizada la evaluación de impacto proporcionada por el reclamado, puede observarse que adolece de importantes defectos:

En primer lugar, es preciso dejar claro que una evaluación de impacto de protección de datos no es un mero documento de carácter formal que se incluya como un trámite previo a la realización del tratamiento. Por el contrario, se trata del documento que plasma un análisis que debe comenzar por un criterio tan básico como si para la realización de la actividad de que se trate es preciso realizar un tratamiento de datos personales. En caso de no superarse ese primer análisis, no debería realizarse o continuarse con el tratamiento.

A continuación, en caso de ser imprescindible realizar un tratamiento de datos personales, debe realizarse un análisis respecto de la tipología de datos personales tratados. Y ello, porque junto con otros elementos, determinarán los riesgos que tal tratamiento implica y que debe de ser evaluados por el responsable del tratamiento. Y a la vista de los mismos proceder al análisis de la necesidad, idoneidad y proporcionalidad, de modo que se obtenga un resultado conforme al cual se determine si los riesgos que implica el tratamiento, y en función de las medidas establecidas, organizativas y de seguridad, aconsejan o no su realización.

Esto nos devuelve al concepto de evaluación de impacto de protección de datos como un concepto material a la vez que formal.

Formal porque es precisa la existencia de un documento que la sintetice, acompañado de un conjunto de documentos que, por mor de la responsabilidad proactiva, acrediten su realización. Entre otros debe estar presente la documentación previa a la EIPD en la que se haya plasmado la necesidad de la decisión de realizar la EIPD; asimismo se precisa toda la documentación elaborada con ocasión de la realización de la EIPD y justificativa de los resultados obtenidos en la EIPD y de las medidas adoptadas al respecto, incluyendo la documentación relativa a participación del Delegado de Protección de Datos, en su caso, en la elaboración de la misma.

Y material porque debe realizar los análisis más arriba citados y contener un veredicto que permita la realización del tratamiento. Es decir, la evaluación de impacto no es solo un documento que debe elaborarse, sino un juicio que debe superarse. Solo si se produce dicha superación, esto es, si se llega a la convicción de que los riesgos existentes son asumibles en función de las medidas técnicas y organizativas, de todo tipo, establecidas, podrá realizarse el tratamiento en las condiciones previstas.

Y, en caso de que se produzca la superación, adicionalmente deberán preverse medidas reactivas, para que, en caso de materialización de riesgos, se evite o minimice el impacto en los derechos y libertades de los titulares de los datos personales.

Pues bien, en relación con el documento aportado por la parte reclamada, no se describen las finalidades del tratamiento. A estos efectos, la única referencia contenida en el documento es indicar que el tratamiento estaría legitimado por el cumplimiento de una obligación legal (Estatuto de los Trabajadores) y una indicación de “La finalidad que se pretende cubrir requiere de todos los datos a recabar y para todas las personas/interesados afectados (principio de minimización de datos).”, seguida de la expresión “SÍ”

Necesidad y proporcionalidad

a. Necesidad

La evaluación de impacto proporcionada por el responsable no contiene un verdadero juicio sobre la necesidad y proporcionalidad en la realización del tratamiento objeto del expediente. A estos efectos, dicho documento contiene únicamente la siguiente explicación:

"Se han descartado otros sistemas p.e el fichaje con tarjeta porque tras la experiencia con el mismo, se dieron situaciones conflictivas. Se trata de un servicio en el que existe una gran rotación de personal. Cuando se utilizaba el sistema de tarjeta para el fichaje, en ocasiones se cedía a otras personas que no era la titular de la misma, presenciándose en la zona de trabajo personal ajeno al mismo con todos los riesgos que suponen de seguridad laboral. La utilización de la huella dactilar es el sistema que permite evitar estas situaciones delictivas y garantiza el correcto cumplimiento de la nomativa laboral e impedir el acceso no autorizado"

La necesidad implica que se requiere una evaluación combinada, basada en hechos, sobre la eficacia de la medida para el objetivo perseguido y sobre si resulta menos intrusiva en comparación con otras opciones para lograr el mismo objetivo.

La necesidad no debe confundirse con utilidad del sistema. Puede que la detección de huella dactilar facilite el no tener que llevar una tarjeta, que se tarde unos segundos menos en su acceso, que sea automático e instantáneo y no excesivamente costoso. Obviamente, un sistema de huella dactilar puede ser útil, pero no tiene por qué ser objetivamente necesario (siendo esto último lo que realmente debe estar presente). Como establece el dictamen 3/2012 sobre la evolución de las tecnologías biométricas-del GT 29-, debe examinarse "si es esencial para satisfacer esa necesidad, y no solo el más adecuado o rentable". Se han de analizar las opciones y alternativas antes de instaurar un sistema nuevo que supone una exagerada limitación del derecho de cada usuario, cuando pueden existir medios menos invasivos de la intimidad, y no optar por lo práctico o ágil y cómodo, cuando están en juego derechos de sus titulares.

Que un sistema previamente establecido para la consecución de una finalidad no sea eficaz, como afirma la parte reclamada respecto a su sistema de fichaje con tarjeta, no significa que no haya otros sistemas que sean eficaces sin la necesidad de realizar un tratamiento biométrico. Y todos ellos han de ser considerados, atendiendo a una descripción pormenorizada de los mismos, y no sólo el que previamente aseveran que no era eficaz.

La jurisprudencia del TJUE aplica una evaluación de la necesidad estricta para cualquier limitación del ejercicio de los derechos a la protección de datos de carácter personal y al respeto de la vida privada en relación con el tratamiento de datos de carácter personal: «las excepciones y limitaciones en relación con la protección de datos de carácter personal deben aplicarse únicamente en la medida en que sean estrictamente necesarias». El TEDH aplica una evaluación de la necesidad estricta en función del contexto y de todas las circunstancias existentes, como en el caso de las medidas secretas de control.

A este respecto, nada de eso se realiza en el documento suministrado. Este se limita a afirmar que el sistema de fichaje con huella dactilar estaría justificado por presuntos problemas que podrían producirse por la cesión de tarjetas entre trabajadores. En relación con este aspecto, nada explica sobre por qué no resulta factible algún otro sistema de supervisión que evitara ese problema y por qué, en definitiva, el tratamiento de la huella dactilar es imprescindible y no pueden utilizarse otros sistemas menos intrusivos que el tratamiento de un dato biométrico.

En consecuencia, si existen alternativas disponibles para que en un momento dado todos los aficionados opten por un acceso no biométrico, y se articula un consentimiento libre, expreso y específico que permita optar entre estos otros métodos menos intrusivos y los biométricos, ello implica que el tratamiento de datos biométricos no es necesario para la finalidad de controlar la identidad de los que acceden a la grada de animación. **En ningún caso se supera el juicio de necesidad porque el tratamiento biométrico no es necesario**.

b. Idoneidad.

El principio de idoneidad implica la necesidad de evaluar que exista un vínculo lógico y directo entre el tratamiento y el objetivo perseguido. En este sentido, la única explicación aportada al respecto por la parte reclamada es la siguiente:

“Juicio de idoneidad: para conseguir el objetivo de control de acceso y de la jornada laboral, el sistema a través del hash de la huella dactilar, nos ha resultado el adecuado para el fin que se persigue. El umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento, debe ser prácticamente del 100%, se trata del cumplimiento de una obligación legal y de garantizar la seguridad en el ámbito laboral. La eficacia de este sistema, consideramos que nos ayuda a alcanzar este umbral”

Nada más añade la parte reclamada al respecto, limitándose a afirmar la eficacia de un sistema como el establecido para el fichaje. No detalla por qué es este el sistema idóneo, particularmente en función de los riesgos que conlleva, ni tampoco explicita por qué considera que la eficacia del sistema es total. De hecho, no afirma que dicha eficacia sea completa sino que “El umbral de efectividad que se debería alcanzar para cumplir con los fines del tratamiento, debe ser prácticamente del 100”. Es decir no acredita su eficacia, sino que se limita a declarar un objetivo a conseguir).

c. Proporcionalidad

Una vez que se considera que una medida legislativa es necesaria, debe analizarse en función de su proporcionalidad. Una evaluación de la proporcionalidad implica, por lo general, evaluar qué «salvaguardias» deben acompañar a una medida (por ejemplo, sobre la vigilancia) para reducir los riesgos que plantea la medida prevista para los derechos y libertades fundamentales de las personas afectadas, a un nivel «aceptable» /proporcional.

Otro factor que debe tenerse en cuenta en la evaluación de la proporcionalidad de una medida propuesta es la eficacia de las medidas existentes por encima de la propuesta.

Si ya existen medidas para un propósito similar o idéntico, su eficacia debe evaluarse de forma sistemática como parte de la evaluación de la proporcionalidad. Sin esa evaluación de la eficacia de las medidas existentes que persiguen un objetivo similar o el mismo, no se puede considerar que se haya realizado debidamente la evaluación de la proporcionalidad de una nueva medida.

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

Como puede fácilmente observarse, de la evaluación de impacto aportada no se deduce juicio alguno sobre la proporcionalidad. A este respecto, la Guía de Protección de datos en las relaciones laborales, de esta AEPD (mayo de 2021), aclara lo siguiente en su apartado de “Datos biométricos”:

“4. El almacenamiento se realizará preferentemente en un dispositivo personal, antes que acudirse a un almacenamiento centralizado. Deberá utilizarse una clave de encriptado específica para los dispositivos de lectura a fin de proteger efectivamente estos datos contra todo acceso no autorizado.”

En el supuesto que nos ocupa, nos encontramos ante un sistema centralizado. Y, por lo demás, nada sobre el juicio de proporcionalidad esto aparece en la evaluación de impacto aportada por el responsable.

Análisis de riesgos

El artículo 35.7.d) del RGPD establece como parte del contenido mínimo de la evaluación de impacto de protección de datos lo siguiente:

“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.”

Observando el apartado correspondiente del documento de evaluación de impacto aportado, se concluye que se ha incluido una visión muy parcial de los riesgos, incluyendo (aparte del riesgo genérico de “no llevar a cabo una evaluación de impacto”, los relativo a la seguridad de los sistemas de información (posibles ciberataques, brechas, etc).

Por el contrario, nada se incluye sobre las garantías, y mecanismos que garanticen la protección de los datos personales. Nada referido al posible trato de la información almacenada en relación con datos biométricos ni ningún otro aspecto distinto del de la seguridad de la información. Ni mucho menos un análisis de los riesgos desde la perspectiva de los derechos e intereses de los interesados y afectados.

En función de lo anteriormente descrito, no puede considerarse que el responsable haya cumplido su obligación de realizar y superar una evaluación de impacto relativa a la protección de datos en relación con el tratamiento de la huella.

XIII Tipificación de la infracción del artículo 35 RGPD

La citada infracción del artículo 35 del RGPD supone la comisión de las infracciones tipificadas en el artículo 83.4 del RGPD que bajo la rúbrica *"Condiciones generales para la imposición de multas administrativas"* dispone:

"Las infracciones de las disposiciones siguientes se sancionarán, de acuerdo con el apartado 2, con multas administrativas de 10 000 000 EUR como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía:

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

A este respecto, la LOPDGDD, en su artículo 71 "*Infracciones*" establece 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 efectos del plazo de prescripción, el artículo 73 "*Infracciones consideradas graves*" de la LOPDGDD indica:

"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"

XIV Falta de evaluación de impacto artículo 35 RGPD.

Esta infracción puede ser sancionada con multa de 10 millones de € 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, de acuerdo con el artículo 83.4 del RGPD.

Asimismo, se considera que procede graduar la sanción a imponer de acuerdo con los siguientes criterios que establece el artículo 83.2 del RGPD:

- Duración de la infracción. La misma se habría prolongado como mínimo desde octubre de 2021 (fecha del envío de la cláusula origina), sin que el inspector hubiera constatado su cese en momento alguno. (art. 83.2.a)

- La categoría de datos personales afectados por la infracción. Debe tenerse en cuenta que la huella dactilar es un dato biométrico y conforme al artículo 9 del RGPD se consideran como categorías especiales de datos “el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física,”. A este respecto, la situación de riesgo creada por la falta de medidas de seguridad es agravada respecto a datos que no tienen la consideración de especiales (artículo 83.2.g)

Conforme a dichos criterios se estima que la sanción que corresponde es de una multa de CIEN MIL EUROS (100.000 €)

XV Adopción de medidas

Confirmada la infracción, se acuerda imponer al responsable la adopción de medidas adecuadas para ajustar su actuación a la normativa mencionada en este acto, de acuerdo con lo establecido en el citado artículo 58.2 d) del RGPD, según el cual cada autoridad de control podrá “*ordenar al responsable o encargado del tratamiento que las operaciones de tratamiento se ajusten a las disposiciones del presente Reglamento, cuando proceda, de una determinada manera y dentro de un plazo especificado…”.* La imposición de esta medida es compatible con la sanción consistente en multa administrativa, según lo dispuesto en el art. 83.2 del RGPD.

En concreto, en función de las infracciones observadas, se establecen las siguientes medidas, estableciéndose el plazo para su cumplimiento en el plazo de SEIS MESES:

- Informar a todos los trabajadores de manera adecuada, incluyendo todos los extremos que no se han incluido hasta ahora, conforme a lo detallado en los fundamentos de derecho de esta resolución

- Establecer las medidas de seguridad necesarias para evitar el acceso por personal no expresamente autorizado, así como para garantizar el borrado de la huella tras su captura. También para separar el acceso a las tablas que contienen el hash de las huellas y los datos identificativos de los trabajadores.

- Elaborar una evaluación de impacto de protección de datos que contenga todos los extremos previstos en el artículo 35 del RGPD, en particular teniendo en cuenta los defectos señalados en esta resolución .

Adicionalmente, y conforme a los artículos 90.3 de la LPCAP, y 58. 2.f), del RGPD, en esta resolución se acuerda que en el plazo de diez días desde su notificación, el reclamado limite temporal o definitivamente el tratamiento del sistema de control horario mediante la huella dactilar, en tanto no informe adecuadamente a los trabajadores, hasta que realice y supere una evaluación de impacto de protección de datos del tratamiento válida, que tenga en cuenta los riesgos para los derechos y libertades de los empleados y las medidas y garantías adecuadas para su tratamiento, o incluso si se realizara, precisara efectuar la previsión de consulta que se establece

en el artículo 36 del RGPD y en definitiva, hasta que sea conforme a la normativa de protección de datos. En este sentido, la Agencia ha publicado recientemente una guía sobre el control de presencia mediante sistemas de tratamientos biométricos que se encuentra disponible en su página web donde se indican los requisitos necesarios para establecer un sistema de estas características.

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

Por lo tanto, de acuerdo con la legislación aplicable y valorados los criterios de graduación de las sanciones cuya existencia ha quedado acreditada,

la Directora de la Agencia Española de Protección de Datos

RESUELVE:

PRIMERO: IMPONER a **CTC EXTERNALIZACIÓN, S.L.**, con NIF ***B60924131***, las siguientes multas:

- Por una infracción del Artículo 13 del RGPD, tipificada en el Artículo 83.5 del RGPD una multa de 200.000 euros (DOSCIENTOS MIL euros).

- Por una infracción del Artículo 32 del RGPD, tipificada en el Artículo 83.4 del RGPD, una multa de 65.000 euros (SESENTA Y CINCO MIL euros)

- Por una infracción del Artículo 35 del RGPD, tipificada en el Artículo 83.4 del RGPD, una multa de 100.000 euros (CIEN MIL euros).

Ello hace un total de 365.000€ (TRESCIENTOS SESENTA Y CINCO MIL euros).

SEGUNDO: ORDENAR a **CTC EXTERNALIZACIÓN, S.L.**, con NIF ***B60924131***, que en virtud del artículo 58.2.d) del RGPD, en el plazo de 6 meses, acredite haber procedido al cumplimiento de las siguientes medidas:

- Informar a todos los trabajadores de manera adecuada, incluyendo todos los extremos que no se han incluido hasta ahora, conforme a lo detallado en los fundamentos de derecho de esta resolución

- Establecer las medidas de seguridad necesarias para evitar el acceso por personal no expresamente autorizado, así como para garantizar el borrado de la huella tras su captura. También para separar el acceso a las tablas que contienen el hash de las huellas y los datos identificativos de los trabajadores.

- Elaborar una evaluación de impacto de protección de datos que contenga todos los extremos previstos en el artículo 35 del RGPD, en particular teniendo en cuenta los defectos señalados en esta resolución, y superarla.

- Cumplir con la normativa de protección de datos.

TERCERO. ORDENAR, conforme a los artículos 90.3 de la LPCAP, y 58. 2.f), del RGPD, a **CTC EXTERNALIZACIÓN, S.L.**, con NIF ***B60924131*** que, en el plazo de diez días desde la notificación de esta resolución, limite temporal o definitivamente el tratamiento del sistema de control horario mediante la huella dactilar, en tanto no informe adecuadamente a los trabajadores, hasta que realice y supere una evaluación de impacto de protección de datos del tratamiento válida, que tenga en cuenta los riesgos para los derechos y libertades de los empleados y las medidas y garantías adecuadas para su tratamiento, o incluso si se realizara, precisara efectuar la previsión de consulta que se establece en el artículo 36 del RGPD y en definitiva, hasta que sea conforme a la normativa de protección de datos

CUARTO: NOTIFICAR la presente resolución a **CTC EXTERNALIZACIÓN, S.L.**.

QUINTO: Esta resolución será ejecutiva una vez finalice el plazo para interponer el recurso potestativo de reposición (un mes a contar desde el día siguiente a la notificación de esta resolución) sin que el interesado haya hecho uso de esta facultad. Se advierte al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida 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.. En caso contrario, se procederá a su recaudación en período ejecutivo.

Recibida la notificación y una vez ejecutiva, si la fecha de ejecutividad se encuentra entre los días 1 y 15 de cada mes, ambos inclusive, el plazo para efectuar el pago voluntario será hasta el día 20 del mes siguiente o inmediato hábil posterior, y si se encuentra entre los días 16 y último de cada mes, ambos inclusive, el plazo del pago será hasta el 5 del segundo mes siguiente o inmediato hábil posterior.

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 conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente

recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) de la LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada Ley 39/2015, de 1 de octubre. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

938-21112023

Mar España Martí
Directora de la Agencia Española de Protección de Datos