- Procedimiento Nº: E/10900/2019

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: Las reclamaciones interpuestas por el reclamante 1 y el reclamante 2 tienen entrada con fecha 08/05/2019 en la Agencia Española de Protección de Datos. Las reclamaciones se dirigen contra el Ayuntamiento de TEULADA, con NIF ***P0312800F*** (en adelante, el reclamado).

Los motivos en que basa el reclamante 1 su escrito de reclamación es, en síntesis, los siguientes:

- Que desde hace tiempo, el sistema de control de presencia y la forma de recabar los datos personales y biométricos no garantizan los derechos de los trabajadores y posiblemente vulnera la Ley de Protección de Datos.

Que tras diferentes requerimientos de subsanación el Ayuntamiento no contesta.

Que es delegado sindical del Ayuntamiento de Teulada por el sindicato FeSP-UGT-PV.

Que el 08/04/2018 los trabajadores del Ayuntamiento de Teulada recibieron un correo electrónico enviado desde la cuenta de un empleado del Departamento de Informática del consistorio en el que se informaba que ya estaba disponible el fichado del conservatorio. El lector de presencia se había roto y se había habilitado uno en el conservatorio en su sustitución.

Que el día 18 y 19/04/2018, los trabajadores recibieron un correo electrónico enviado desde la cuenta del Departamento de Recursos Humanos por una empleada informando de que el Departamento de Informática tenía que recoger la huella de todos los funcionarios. Que se adjuntaba a tal correo una relación de funcionarios que debían de presentarse en el citado departamento según horario establecido. Que no se adjuntaba documentación alguna a rellenar para expresar la autorización por escrito de toma de dato de huella dactilar.

Que el 20/04/2018 se presentó escrito en el Ayuntamiento denunciando una serie de irregularidades en el sistema de control de presencias sin que se haya obtenido respuesta.

Que el 07/05/2018 se recibió correo electrónico desde el Departamento de Informática que informaba de que debido a la rotura de relojes de fichajes se había procedido al cambio de estos por un sistema nuevo, estando desde la semana pasada en marcha en pruebas, estando ya instalados y con las huellas de los que hasta el momento las habían colocado y que en breve el sistema será definitivo.

Que a día de hoy son numerosos los funcionarios del Ayuntamiento de Teulada que, con la reciente renovación de los sistemas de fichaje por huella, han otorgado su huella a solicitud de los departamentos de recursos humanos y de nuevas tecnologías, sin previamente haber firmado ningún documento donde se exprese su consentimiento explícito.

Que no consta certificado de RRHH donde señale que los datos están siendo encriptados y almacenados en el sistema de control de presencia de forma que solo pueden ser utilizados a través del sistema que gestiona dicho departamento.

Que no se ha informado a los trabajadores si los datos de carácter personal, recogidos a través del sistema de terminales de marcaje de control de presencia biométrico, se incluyen en algún tipo de fichero que sea responsabilidad del Ayuntamiento de Teulada.

Que se inicia la recogida de datos biométricos sin autorización de disposición publicada en BOE, puesto que estos datos concretos no se encuentran recogidos en el fichero que supuestamente debería estar creado, ni se ha producido la modificación del mismo.

Y, entre otra, anexa la siguiente documentación:

 Escrito fechado a 20/04/2018 y dirigido al Alcalde-Presidente del Ayuntamiento de Teulada, reproduciendo las manifestaciones anteriores.

Los motivos en que basa el reclamante 2 su escrito de reclamación es, en síntesis, los siguientes:

Que es funcionario del Ayuntamiento de Teulada.

Que desde abril de 2018, tras la implantación del nuevo sistema de fichaje por medio de huella digital, ya que el anterior se rompió y al parecer perdieron los datos que en él se contenían, se ha solicitado que se cumpla con el correspondiente derecho de información por parte del Ayuntamiento llegando a presentar hasta 5 escritos.

Que dichos escritos no fueron contestados.

Que se le llegó a incoar un expediente por no realizar el fichaje. Que finalmente y ante el miedo de que dicho expediente prosperase, decidió facilitar nuevamente su huella digital de manera voluntaria pese a que ya la facilitó en marzo de 2007 y a que no se le facilitó información.

Que no se cumple con la necesaria identificación previa por aproximación de la tarjeta ya que no existe tal, únicamente se realiza la comprobación a través de la huella digital.

Y, entre otra, anexa la siguiente documentación:

 Escrito fechado a 09/05/2018 y dirigido al Alcalde-Presidente del Ayuntamiento de Teulada, reproduciendo las manifestaciones anteriores.

SEGUNDO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

El 19/06/2019 el reclamado remite a esta Agencia la siguiente información:

1. Que desde el año 2007 se venía desarrollando pacíficamente y sin problemas por todos los trabajadores el sistema de fichaje mediante un sistema biométrico.

2. Que los marcados eran parciales y confusos motivo por el cual se insistió en la obligatoriedad de fichar.

3. Que no consta al Ayuntamiento que el reclamante 2 sea representante del sindicato UGT-PV.

Se aporta denuncia firmada electrónicamente por el Alcalde-Presidente del Ayuntamiento de Teulada en fecha 01/06/2018 y presentada, según se manifiesta, ante la Guardia Civil el mismo día, que:

a. Entre las 22:30h del día 06/04/2018 y las 00:30h del 07/04/2018 machacaron el soporte para identificar las huellas digitales. Que el control de presencias ubicado en el parking corrió la misma suerte que el situado en el Hall.

b. Que por interés general, que es asegurar la presencia de los funcionarios durante la jornada laboral ya que ello se traduce en un mejor servicio al ciudadano, no puede menos que considerarse necesario el sistema de control de presencia instaurado por el Ayuntamiento y por ende exceptuado de la obligación de obtener el previo consentimiento de los funcionarios.

Se aporta informe del Delegado de Protección de Datos del Ayuntamiento de Teulada firmado electrónicamente con, entre otras, las siguientes manifestaciones:

a) La Jurisprudencia del Tribunal Supremo (STS 5200/2007 de dos de julio) se ha pronunciado sobre el uso de la biometría en el ámbito laboral, concretamente al resolver un recurso de casación en el que se dilucidaba la adecuación al derecho fundamental a la protección de datos, de la resolución del Consejero de Presidencia de la Comunidad Autónoma de Cantabria, por la que se implantaba un sistema de control horario del personal al servicio de la Administración del Gobierno de dicha Comunidad Autónoma, sistema basado en la captación digital de datos biométricos de la mano.

b) Que en cuanto al Reglamento General de Protección de Datos en su artículo 9 apartado 2.b) recoge la excepción a tratar datos biométricos.

c) Que el departamento técnico de los equipos biométricos y desarrolladores de software de los equipos instalados en el Ayuntamiento de Teulada, el 23 de abril por correo electrónico manifiestan:

i. Que un sistema biométrico dactilar libra al usuario del uso de tarjetas y llaves que son susceptibles de extravío o sustracción.

ii. Que evita que un usuario fiche por otro empleado.

(…)

d) Que desde el departamento de RRHH se ha comunicado por medios telemáticos y presenciales sobre la finalidad de los datos biométricos recabados que es el control del cumplimiento del horario de trabajo al que vienen obligados los empleados públicos.

e) Que recomienda que nuevamente sean debidamente informados los empleados públicos especialmente de la finalidad de los datos biométricos recabados.

Con fecha 04/03/2020 el reclamado remite a esta Agencia la siguiente información:

1. Que han dado formación e información regularmente siendo la última en octubre de 2019.

2. Que a fecha del primer requerimiento de la AEPD, el Ayuntamiento estaba en el proceso de integrar un nuevo proyecto de cumplimiento integral de RGPD, LOPDGDD y ENS. Que en este proyecto se solucionan algunas carencias en materia de

documentación. Que en el transcurso del nuevo proyecto se ha desarrollado el nuevo documento informativo hacia el personal, material de formación, registro de actividades y EIPD.

Se aporta EIPD con exclusivamente la documentación de salida de la herramienta GESTIONA EIPD. Se aporta Registro de Actividades, material de formación y modelo de documento informativo hacia el personal.

3. Que la información a los trabajadores se facilitó durante el proceso de registro de las huellas en el año 2010 y en el nuevo registro realizado antes los cambios de los lectores, si bien en este momento no se les facilitó un documento escrito dado que en esa fecha estaba en proceso el cambio hacia el documento adjuntado.

4. Que en relación a la captura, almacenado y tratamiento de la huella manifiesta que:

"Los lectores no graban imagen alguna de la huella, limitándose a capturar unas coordenadas (denominadas "minucias") de la huella y aplicarles un algoritmo matemático por el que se obtienen los denominados "templates", por lo que el "dato biométrico" queda reducido a dicho hash.

5. Que las bases jurídicas consideradas con la obligación legal y el interés público. Que por esos motivos se implantó el control de presencia y control horario desde el año 2010 y se mantiene en la actualidad al considerar, tras una nueva ponderación, que con los niveles de seguridad aplicados, es un método idóneo, justificado y proporcional para la finalidad del tratamiento.

6. Que en relación a las medidas de seguridad aplicadas:

a. El sistema de información utilizado para la gestión del tratamiento de la huella dactilar se llama SAVIA, de la empresa SOLUCIONES AVANZADAS EN INFORMÁTICA APLICADA S.L. sistema certificado en categoría MEDIA bajo el Esquema Nacional de Seguridad. Que el sistema que se utiliza es en modalidad SaaS, por lo que las infraestructuras técnicas no residen en el Ayuntamiento.

Aporta certificado de conformidad con el Esquema Nacional de Seguridad expedido el 10/01/2020.

(…)

Con fecha 16/06/2020, el denunciado remite a esta Agencia la siguiente información y manifestaciones:

1. Que SOLUCIONES AVANZADAS EN INFORMÁTICA APLICADA, S.L. ha suscrito contratos con otros proveedores para la provisión del servicio al AYUNTAMIENTO DE TEULADA siendo estos proveedores VODAFONE e INFORMÁTICA DEL ESTE como proveedor de infraestructura y el fabricante del software.

2. Que los datos se encuentran almacenados en dos direcciones correspondientes al municipio de Madrid.

3. Se aporta Informe de Auditoría de ENS de fecha 16/12/2019 realizado a SOLUCIONES AVANZADAS EN INFORMÁTICA APLICADA, S.L. en el que consta que:

a) Para los servicios *https://saviacloud.net, http://www.mysaas.es, https://hroptics.savia.net, https://[subdominiocliente].savia.net* han sido categorizadas en el nivel BAJO para todas las dimensiones de seguridad (Disponibilidad, Integridad, Confidencialidad, Autenticidad, Trazabilidad) excepto para el servicio *https://*

[subdominiocliente].savia.net el cual, para la dimensión de Disponibilidad, ha sido categorizado en el nivel MEDIO.

b) Para la "Información", y en concreto, para "Huellas" se ha categorizado en el nivel BAJO para todas las dimensiones de seguridad.

c) Consta que:

"Se ha revisado:

…

4. El análisis de riesgos realizado con una metodología basada en MAGERIT..."

4. Se aporta Contrato con la empresa SOLUCIONES AVANZADAS EN INFORMÁTICA APLICADA, S.L. siendo su objeto *"la prestación del servicio de mantenimiento de los servicios Saas del programa de recursos humanos (Ginpix7) de la empresa SOLUCIONES AVANZADAS EN INFORMÁTICA APLICADA, S.L. (SAVIA) que el Ayuntamiento de Teulada viene utilizando desde su adquisición."*

Que en su *"Cláusula décimonovena. Ejecución del contrato y protección de datos"* se estipula que:

"…

La ejecución se realizará a riesgo y ventura del contratista.

(…)

…"

5. Como ANEXO III al contrato anterior se adjunta *"CONTRATO TRATAMIENTO DE DATOS PERSONALES"* siendo el AYUNTAMIENTO DE TEULADA el responsable del tratamiento y SOLUCIONES AVANZADAS EN INFORMÁTICA APLICADA, S.L. el encargado del tratamiento.

Con fecha 06/06/2020, se comprueba que VODAFONE ESPAÑA, S.A.U. posee certificado en el Esquema Nacional de Seguridad nivel BASICO.

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 47 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

En el presente caso, de conformidad con lo señalado en el hecho primero los reclamantes interpusieron sendos escritos ante la AEPD, dirigidas contra el reclamado y relacionados con la implantación de un sistema de control de ausencia del personal del Ayuntamiento de Teulada mediante huella digital, con el que estaban disconformes

y sobre cuya implantación no se les había proporcionado toda la información necesaria y adecuada.

En relación con la cuestión planteada en el caso presente, habría que señalar que la implantación de un sistema de control de presencia basado en la huella dactilar por parte del Ayuntamiento de Teulada, ha de ser informado a todos los afectados de completa, clara, concisa y, además, la citada información debe ser adicionada con referencia tanto a las bases legales que den cobertura a dicho tipo de control de acceso como a la información básica a la que hace referencia el artículo 13 del RGPD.

El propio DPD de la Corporación en su informe señala la necesidad de sean debidamente informados los empleados públicos especialmente de la finalidad de los datos biométricos recabados.

La instalación de un sistema de control basado en la recogida y tratamiento de la huella dactilar de los empleados públicos implica el tratamiento de sus datos personales puesto que dato personal es toda aquella información sobre una persona física identificada o identificable de conformidad con el artículo 4.1 del RGPD.

Hay que señalar que los datos biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación.

Según el Dictamen 3/2012 sobre la evolución de las tecnologías biométricas*, "Los datos biométricos cambian irrevocablemente la relación entre el cuerpo y la identidad, ya que hacen que las características del cuerpo humano sean legibles mediante máquinas y estén sujetas a un uso posterior."*

En relación con ellos, el Dictamen precisa que cabe distinguir diversos tipos de tratamientos al señalar que *"Los datos biométricos pueden tratarse y almacenarse de diferentes formas. A veces, la información biométrica capturada de una persona se almacena y se trata en bruto, lo que permite reconocer la fuente de la que procede sin conocimientos especiales; por ejemplo, la fotografía de una cara, la fotografía de una huella dactilar o una grabación de voz. Otras veces, la información biométrica bruta capturada es tratada de manera que solo se extraen ciertas características o rasgos y se salvan como una plantilla biométrica."*

Los datos biométricos los define el artículo 4.14 del RGPD:

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

Hay que señalar que el RGPD no parece considerar a todo tratamiento de datos biométricos como tratamiento de categorías especiales de datos, ya que el artículo 9.1. se refiere a los "datos biométricos dirigidos a identificar de manera unívoca a una persona física", por lo que, de una interpretación conjunta de ambos preceptos parece dar a entender que los datos biométricos solo constituirían una

categoría especial de datos en el caso de que se sometan a un tratamiento técnico específico dirigido a identificar de manera unívoca a una persona física.

En este sentido, parece que igualmente se pronuncia el Considerando 51 al señalar que *"El tratamiento de fotografías no debe considerarse sistemáticamente tratamiento de categorías especiales de datos personales, pues únicamente se encuentran comprendidas en la definición de datos biométricos cuando el hecho de ser tratadas con medios técnicos específicos permita la identificación o la autenticación unívocas de una persona física".*

Con igual criterio, el Protocolo de enmienda al Convenio para la Protección de Individuos con respecto al procesamiento de datos personales, aprobada por el Comité de Ministros en su 128º período de sesiones en Elsinore el 18 de mayo de 2018 (Convenio 108+) incluye únicamente como categorías especiales de datos, en su artículo 6.1 a los datos biométricos dirigidos a la identificación unívoca de una persona ("biometric data uniquely identifying a person"), sin incluir la referencia a la autenticación.

Al objeto de aclarar las dudas interpretativas que surgen respecto a la consideración de los datos biométricos como categorías especiales de datos puede acudirse a la distinción entre identificación biométrica y verificación/autenticación biométrica que establecía el Grupo del Artículo 29 en su Dictamen 3/2012 sobre la evolución de las tecnologías biométricas:

Identificación biométrica: la identificación de un individuo por un sistema biométrico es normalmente el proceso de comparar sus datos biométricos (adquiridos en el momento de la identificación) con una serie de plantillas biométricas almacenadas en una base de datos (es decir, un proceso de búsqueda de correspondencias uno-a-varios).

Verificación/autenticación biométrica: la verificación de un individuo por un sistema biométrico es normalmente el proceso de comparación entre sus datos biométricos (adquiridos en el momento de la verificación) con una única plantilla biométrica almacenada en un dispositivo (es decir, un proceso de búsqueda de correspondencias uno-a-uno).

Esta misma diferenciación se recoge en el Libro blanco sobre la inteligencia artificial de la Comisión Europea:

"En lo que se refiere al reconocimiento facial, por «identificación» se entiende que la plantilla de la imagen facial de una persona se compara con otras muchas plantillas almacenadas en una base de datos para averiguar si su imagen está almacenada en ella. La «autenticación» (o «verificación»), por su parte, se refiere habitualmente a la búsqueda de correspondencias entre dos plantillas concretas. Permite la comparación de dos plantillas biométricas que, en principio, se supone que pertenecen a la misma persona; así, las dos plantillas se comparan para determinar si la persona de las dos imágenes es la misma. Este procedimiento se emplea, por ejemplo, en las puertas de control automatizado de fronteras empleadas en los controles fronterizos de los aeropuertos".

Atendiendo a la citada distinción, puede interpretarse que, de acuerdo con el artículo 4 del RGPD, el concepto de dato biométrico incluiría ambos supuestos, tanto la identificación como la verificación/autenticación. Sin embargo, y con carácter general, los datos biométricos únicamente tendrán la consideración de categoría especial de datos en los supuestos en que se sometan a tratamiento técnico dirigido a la identificación biométrica (uno-a-varios) y no en el caso de verificación/autenticación biométrica (uno-a-uno).

El tratamiento de datos biométricos requerirá, además de la concurrencia de una de las bases jurídicas establecidas en el artículo 6 del RGPD, alguna de las excepciones previstas en el artículo 9.2 del RGPD.

El análisis de la base legal de legitimación para realizar este tratamiento viene del artículo 6 del RGPD, relativo a la licitud del tratamiento, que en su apartado 1, letra b) señala: *"El tratamiento será lícito si se cumple al menos una de las siguientes condiciones: (…) b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de éste de medidas precontractuales (…)".*

En virtud de este precepto, el tratamiento sería lícito y no requeriría el consentimiento, cuando el tratamiento de datos se realice para el cumplimiento de relaciones contractuales de carácter laboral.

Este precepto daría cobertura también al tratamiento de datos de los empleados públicos, aunque su relación no sea contractual en sentido estricto. Hay que señalar que en ocasiones, para el cumplimiento de sus obligaciones en relación con los empleados públicos, la Administración ha de realizar tratamientos de determinados datos a los que se refiere el RGPD, en su artículo 9, como "categorías especiales de datos".

En este punto hay que hacer especial mención de la letra b) del artículo 9.2 del RGPD, según la cual la prohibición general de tratamiento de datos biométricos no será de aplicación cuando *"el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado".*

En el ordenamiento español, el artículo 20 del Texto refundido del Estatuto de los trabajadores (TE), aprobado por el Real decreto legislativo 2/2015, de 23 de octubre, prevé la posibilidad de que el empresario adopte medidas de vigilancia y control para verificar el cumplimiento de las obligaciones laborales de sus trabajadores:

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

Y en el Estatuto Básico del Empleado Público, aprobado por Real Decreto Legislativo 5/2015, de 30 de octubre, en su artículo 54 en relación con los principios de conducta de los empleados públicos señala: *"El desempleo de las tareas correspondientes a su puesto de trabajo se realzará de forma diligente y cumpliendo la jornada y el horario establecidos"*

También conviene señalar que la legislación básica de régimen local atribuye al Alcalde Presidente de la Corporación la dirección del gobierno y administración municipal así como ejercer la superior dirección del personal al servicio de la administración municipal.
Es innegable la posibilidad de utilización de sistemas basados en datos biométricos para llevar a cabo el control de acceso y horario, aunque tampoco parece que sea o deba ser el único sistema que puede ser usado: el uso de tarjetas personales, la utilización de códigos personales, la visualización directa del punto de marcaje, etc., que pueden constituir, por sí mismos o en combinación con alguno de los otros sistemas disponibles, medidas igualmente eficaces para llevar a cabo el control.

En cualquier caso, con carácter previo a la decisión sobre la puesta en marcha de un sistema de control de este tipo, teniendo en cuenta sus implicaciones, el tratamiento de datos de una categoría especial (biométricos), etc., sería preceptivo establecer el Registro de Actividades de Tratamiento y llevar a cabo una Evaluación de Impacto relativa a la protección de datos de carácter personal para evaluar tanto la legitimidad del tratamiento y su proporcionalidad como la determinación de los riesgos existentes y las medidas para mitigarlos de conformidad con lo señalado en el artículo 35 RGPD.

En el presente caso, el Ayuntamiento ha acreditado tener implantado tanto el Registro de Actividades de Tratamiento regulado en el artículo 30 del RGPD y haber llevado a cabo la preceptiva Evaluación de Impacto relativa a la protección de datos regulada en el artículo 35 del RGPD.

IV

También en relación la necesidad de información a los interesados hay que señalar que los datos biométricos están estrechamente vinculados a una persona, dado que pueden utilizar una determinada propiedad única de un individuo para su identificación o autenticación.

El tratamiento de estos datos está expresamente permitido por el RGPD cuando el empresario cuenta con una base jurídica, que de ordinario es el propio contrato de trabajo. A este respecto, la STS de 2 de julio de 2007 (Rec. 5017/2003), que ha entendido legitimo el tratamiento de los datos biométricos que realiza la Administración para el control horario de sus empleados públicos, sin que sea preciso el consentimiento previo de los trabajadores.

Sin embargo, debe tenerse en cuenta lo siguiente:

1. El empleado debe ser informado sobre estos tratamientos en los términos del artículo 13 del RGPD.

2. Deben respetarse los principios de limitación de la finalidad, necesidad, proporcionalidad y minimización de datos.

En todo caso, el tratamiento también deberá ser adecuado, pertinente y no excesivo en relación con dicha finalidad. Por tanto, los datos biométricos que no sean necesarios para esa finalidad deben suprimirse y no siempre se justificará la creación de una base de datos biométricos (Dictamen 3/2012 del Grupo de Trabajo del art. 29).

3. Uso de plantillas biométricas: Los datos biométricos deberán almacenarse como plantillas biométricas siempre que sea posible. La plantilla deberá extraerse de una manera que sea específica para el sistema biométrico en cuestión y no utilizada por otros responsables del tratamiento de sistemas similares a fin de garantizar que una persona solo pueda ser identificada en los sistemas biométricos que cuenten con una base jurídica para esta operación.

4. El sistema biométrico utilizado y las medidas de seguridad elegidas deberán asegurarse de que no es posible la reutilización de los datos biométricos en cuestión para otra finalidad.

5. Deberán utilizarse mecanismos basados en tecnologías de cifrado, a fin de evitar la lectura, copia, modificación o supresión no autorizadas de datos biométricos.

6. Los sistemas biométricos deberán diseñarse de modo que se pueda revocar el vínculo de identidad.

7. Deberá optarse por utilizar formatos de datos o tecnologías específicas que imposibiliten la interconexión de bases de datos biométricos y la divulgación de datos no comprobada.

8. Los datos biométricos deben ser suprimidos cuando no se vinculen a la finalidad que motivó su tratamiento y, si fuera posible, deben implementarse mecanismos automatizados de supresión de datos.

Por lo tanto, de acuerdo con lo señalado,

La Directora de la Agencia Española de Protección de Datos,

SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al Ayuntamiento de TEULADA, con NIF P0312800F junto con el ANEXO 1 y a cada uno de los reclamantes con el ANEXO que le corresponda en el que se incluye su identificación.

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

Contra esta resolución, que pone fin a la vía administrativa según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, 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.

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

ANEXO I

- Reclamante 1: A.A.A.
- Reclamante 2: B.B.B.
-

ANEXO II

- Reclamante 1: A.A.A.

ANEXO III

- Reclamante 2: B.B.B.