- Procedimiento Nº: E/03925/2020

940-0419

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: La reclamación interpuesta por Doña ***A.A.A.***, en nombre de la Sección Sindical Estatal CGT-ATOS IT (en adelante, la reclamante) tiene entrada con fecha 24 de octubre de 2019 en la Agencia Española de Protección de Datos. La reclamación se dirige contra **ATOS IT SOLUTIONS AND SERVICES IBERIA, S.L.,** con NIF B85908093 (en adelante, el reclamado).

Los motivos en que basa la reclamación son que la entidad reclamada recaba datos biométricos sensibles de sus trabajadores sin cumplir la normativa de protección de datos. En concreto, no recaba el consentimiento explícito de sus trabajadores, no ha efectuado la evaluación de impacto ni el Registro de Actividades de tratamiento. Fundamenta su reclamación en lo establecido en el artículo 9 del RGPD.

Junto a la reclamación aporta numerosos correos electrónicos que se han intercambiado entre el sindicato y la entidad reclamada, en los cuales se indica, entre otras cosas, que el sistema al recoger la huella, por primera vez, crea un template/hash mediante un algoritmo y eso es lo que se almacena en la base de datos de la entidad con todas las medidas de seguridad adecuadas. Señalando que a partir de ese Template/Hash no es posible reconstruir la huella dactilar ni ningún otro dato biométrico.

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), con número de referencia E/11347/2019, se dio traslado de dicha reclamación al reclamado, 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.

La reclamada informó, en relación con la reclamación, en el sentido siguiente:

*"**Evaluación de Impacto realizada**: Se aportan dos análisis de necesidad de realización de una evaluación de impacto y dos evaluaciones de impacto correspondientes al sistema de control de acceso y al sistema de registro de jornada (documentos 1, 2, 3 y 4). La evaluación de impacto se denomina DPIA (Data Privacy Impact Asessment) en Atos. Para mayor entendimiento, el documento 13 "Contexto y alegaciones" citado en el apartado "cualquier otra que considere relevante", especifica la conexión entre ambos tratamientos.*

1.- DPIA_Evaluación_necesidad DPIA_Facilities_Dorlet_controldeaccesos.V3
2.- DPIA_Evaluación_necesidad DPIA_RRLL-controljornada.V2.

3.- DPIA-DORLET_controldeacceso.V3
4.- DPIA-Registro_Jornada_V2

***Información facilitada a los trabajadores**: se adjuntan las cláusulas informativas publicadas a través de diferentes canales y medios corporativos (intranet, correo electrónico, red social corporativa…etc); adicionalmente, se aportan las "Preguntas Frecuentes" (FAQ's) e información facilitada al Comité de Empresa.*

5.- Comunicación_cláusulainformativa_Dorlet_control accesos
6.- Comunicación_cláusulainformativa_Registro_Jornada (uso virtual) (varios documentos)
7.- Actualización_cláusula_informativa_Registro_Jornada (conexión con el sistema de control de acceso) (varios documentos)
8.- Comunicación_complementaria_cláusulainformativa_controlacceso.
9.- Preguntas Frecuentes (FAQ's)
10.- Documentación_facilitada_ComitédeEmpresa

La reclamante alega: *"Recabar datos biométricos (de carácter sensible) a los trabajadores y trabajadoras de la empresa sin cumplir los requisitos ni la normativa que regula dicho tratamiento. No ha solicitado el consentimiento expreso de los interesados donde se especifique claramente con qué finalidad se van a obtener los datos biométricos de la huella a los trabajadores de dicha empresa". Al respecto de dichas alegaciones procede señalar lo siguiente:*

El tratamiento de los datos biométricos a los que se refiere la reclamación tiene como base de legitimación el artículo 9.2 b) del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante RGPD); en relación con el artículo 20 y 34 del Estatuto de los Trabajadores (Real Decreto Legislativo 2/2015, de 23 de octubre, por el que se aprueba el texto refundido de la Ley del Estatuto de los Trabajadores) y el Real Decreto-Ley 8/2019, de 8 de marzo, de medidas urgentes de protección social y de lucha contra la precariedad laboral en la jornada de trabajo.

En este sentido, al contrario de lo que la reclamante alega, no se entiende necesario recabar el consentimiento de los titulares de los datos (empleados de Atos).

En la misma línea, cabe destacar que se ha realizado la correspondiente evaluación de impacto previa (ver documentos 3 y 4).

De acuerdo con lo especificado en el documento 13 "Contexto y alegaciones" así como a través de las evidencias aportadas, se puede observar que se ha procedido con diligencia y transparencia a la hora de facilitar la información exigida por el artículo 13 del RGPD y el artículo 11 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de Derechos Digitales (LOPD y GDD).

Entre la información facilitada está la finalidad de tratamiento de los datos.

La reclamante es un miembro del Comité de Empresa. En este sentido, ha sido informada de los tratamientos que se iban a desplegar por la compañía en calidad, no sólo de empleada de Atos, sino también como miembro del Comité de Empresa. Incluso, se ha iniciado un procedimiento de análisis por parte de la Inspección de Trabajo a petición de la mencionada empleada, en base al cual se ha proporcionado toda la documentación requerida. Atos desconoce por qué habiendo recibido la citada información y habiéndose mantenido reuniones periódicas con el Comité de Empresa, se ha procedido a interponer esta reclamación.

Una vez iniciado el tratamiento, se ha realizado el correspondiente ***registro de actividades de tratamiento.*** *(Ver documento 11 Registro_actividades_tratamiento_CADP_extracto)*

En el supuesto de ejercicio de los derechos regulados en los artículos 15 a 22 del RGPD, acreditación de la respuesta facilitada al reclamante:

Solamente se ha producido oposición inicial de la empleada a facilitar sus datos, habiendo sido explicada toda la información acerca del tratamiento a través de diversos canales y en reiteradas ocasiones (ver documentos 5 a 9), así como durante las reuniones del Comité de Empresa y a través del procedimiento iniciado en la Inspección de Trabajo. Adicionalmente, el día en que la usuaria facilitó su dato de hash de huella, se mantuvo una conversación telefónica con ella, reiterando el contenido de la información facilitada con anterioridad a la captura de los datos, en su rol de empleada y de miembro del Comité de Empresa. Se le indicó que podía no facilitar los datos, pero esta circunstancia implicaba la imposibilidad de acceder a las instalaciones de la compañía."

Acompañan toda la documentación reseñada.

TERCERO**:** Con fecha 30 de marzo de 2020, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante.

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

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 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:

- El trabajador debe ser informado sobre estos tratamientos.
- Deben respetarse los principios de limitación de la finalidad, necesidad, propor-

cionalidad 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).

- 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.

- 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.

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

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

- 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.

- 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.

III

En el presente caso, el reclamado ha implantado un sistema de gestión de la asistencia laboral de sus trabajadores mediante huella dactilar.

Hay que señalar que la legitimación para el tratamiento de la huella para el acceso y control horario de los trabajadores por parte del empleador debemos buscarlo en el artículo 9 y 6 del RGPD.

El artículo 9 del RGPD establece en sus apartados 1 y 2.b) lo siguiente:

"1. Quedan prohibidos el tratamiento de datos personales que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientaciones sexuales de una persona física.

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

(…)

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

(…)"

El artículo 6.1.b) del RGPD indica:

"1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:

(…)

b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.

(…)"

El reclamado tiene legitimación, fundamentada en la normativa señalada, para efectuar el control de acceso y de horario en relación con sus trabajadores, siempre que cumpla los requisitos indicados. No es necesario que solicite el consentimiento a los trabajadores, ya que la causa que legitima el tratamiento revisado son las señaladas del artículo 9 del RGPD, que levanta la prohibición de tratamiento de los datos biométricos y el 6.1.b) que lo legitima.

IV

También indica la reclamante que no han sido informados conforme establece el artículo 13 del RGPD, con todas las garantías del tratamiento previsto.

En este artículo se determina la información que debe ser facilitada al interesado en el momento de la recogida de sus datos, estableciendo lo siguiente:

"Artículo 13. 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; 4.5.2016 L 119/40 Diario Oficial de la Unión Europea ES
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intere-

ses legítimos del responsable o de un tercero;
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 hecho de que se hayan prestado.

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 que no facilitar tales datos;
f) la existencia de decisiones automatizas, 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".

La entidad reclamada ha acompañado la cláusula informativa que ha facilitado a sus empleados informándoles del sistema de control mediante huella dactilar, actualizándose con la publicación del Real Decreto 8/2018, de 8 de marzo.

V

El artículo 30 del RGPD establece lo siguiente en relación con el Registro de

las actividades de tratamiento:

<<1. Cada responsable y, en su caso, su representante, llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:

a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;

b) los fines del tratamiento;

c) una descripción de las categorías de interesados y de las categorías de datos personales;

d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;

e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.

2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:

a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;

b) las categorías de tratamientos efectuados por cuenta de cada responsable;

c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;

d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.

3. Los registros a que se refieren los apartados 1 y 2 constarán por escrito, inclusive en formato electrónico.

4. El responsable o el encargado del tratamiento y, en su caso, el representante del responsable o del encargado pondrán el registro a disposición de la autoridad de control que lo solicite.

5. Las obligaciones indicadas en los apartados 1 y 2 no se aplicarán a ninguna empresa ni organización que emplee a menos de 250 personas, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales indicadas en el artículo 9, apartado 1, o datos personales relativos a condenas e infraccio-

nes penales a que se refiere el artículo 10.>>

La empresa reclamada ha aportado como Documento 11, el registro de actividades de tratamiento realizado, que se adecua a lo establecido en el artículo referido.

VI

Por último, la reclamante indica que no se ha realizado la Evaluación de Impacto. El artículo 35 del RGPD establece lo siguiente:

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

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

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

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

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

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

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

7. La evaluación deberá incluir como mínimo:

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

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

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

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

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

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

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

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

En el supuesto objeto de reclamación, nos encontraríamos en el supuesto de necesidad de realizar una evaluación de impacto al efectuar un tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1; en este caso, datos biométricos. 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.

Por lo tanto, de acuerdo con lo señalado, por 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 reclamante y reclamado.

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