- **Expediente N.º: EXP202400687**

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: Con fecha el 11 de diciembre de 2023 se presenta una denuncia ante la Agencia Española de Protección de Datos contra **AUDITORES DE TRATAMIENTOS DE DATOS, S.L.** con NIF ***B97325526*** (en adelante, PRODAT). Los motivos en que basa la denuncia son los siguientes:

El denunciante declara que trabajó durante el año 2022 en la empresa reclamada, siendo testigo de la creación o invención de un documento de Evaluación de Impacto de Protección de Datos (en adelante, EIPD) con datos inventados, enviándose hasta el 1 de junio de 2022, al menos a 30 entidades (entidades diversas que lista en su reclamación), que tenían control horario con huella dactilar, y con intención de enviar la EIPD a más entidades.

El denunciante indica haber puesto en conocimiento de las 30 entidades afectadas la situación relacionada con el documento de EIPD. Indica que el documento EIPD contiene un campo "ACCOUNTS.ACCOUNTNAME" en el que se introducía el nombre de la entidad a la que se enviaba el documento.

Además, afirma contar con una grabación sonora de uno de los responsables de la empresa denunciada, en la que reconoce lo fraudulento de la EIPD, así como que, si una entidad tuviera problemas, se simulase un análisis de riesgos previo.

Aporta junto al escrito de reclamación ante la AEPD, el documento de la EIPD, en el que en el punto "ACCOUNTS.ACCOUNTNAME" se introducían los nombres de las entidades a las que se enviaba el documento.

SEGUNDO: 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:

El documento de EIPD aportado por el denunciante se titula "*ANÁLISIS DE RIESGOS EVALUACIÓN DE IMPACTO DE PRIVACIDAD"* y subtitula *"TRATAMIENTO DE DATOS DE REGISTRO DE JORNADA MEDIANTE HUELLA DACTILAR".*

En esta portada se muestra un campo "{ACCOUNTS.ACCOUNTNAME}" y otro "{image Accounts}". En todas sus páginas consta, en el encabezado, el campo "{Accounts.accountname}" y el literal "Tratamiento de huella dactilar de trabajadores para registro de jornada".

En el texto del documento también se encuentra este campo {Accounts.accountname} en diversas ocasiones, donde debe aparecer el nombre de la entidad a la que se refiere. Así, en la página 4 aparece *"Por ello, {Accounts.accountname} ha encomendado a PRODAT la elaboración de un informe de Evaluación de Impacto Previa de Protección de Datos Personales*". Los campos Accounts son campos a rellenar que sirven para personalizar e individualizar un documento genérico, introduciendo, según el caso, los datos identificativos del cliente, fecha, etc.

Este documento consiste en una EIPD genérica, o un modelo de EIPD, para el tratamiento de huellas digitales de los empleados con la finalidad del control de la jornada laboral. El documento recoge algunos puntos que pueden ser comunes a diferentes entidades al tratarse del mismo tratamiento, si bien puede requerir particularización. El documento concluye lo siguiente:

"Por todo ello, teniendo en cuenta las recomendaciones de la Agencia Española de Protección de Datos sobre los riesgos a la privacidad y derechos fundamentales en caso de utilización de datos biométricos, como lo es la huella dactilar, hemos de recomendar la adopción de las siguientes actuaciones:

Primera.- Informar a los interesados si se van a utilizar los datos con otras finalidades distintas a las previamente informadas y en caso de ser así, realizar una nueva EIPD.
Segunda.- Cumplir el principio de minimización de datos, por lo que únicamente debe recogerse el dato de la huella dactilar y no otros.
Tercera. Se cumplirá con el principio de limitación del plazo de conservación, por lo que los registros se conservarán un máximo de 4 años, para dar cumplimiento a la legislación laboral.
Cuarta.- Establecer medios para facilitar información a los interesados.
Quinta.- Verificación del contrato con el prestador del servicio, verificación de confidencialidad y secreto.
Sexta. Implementación de medidas de seguridad en relación al acceso y recuperación de datos.
Una vez implantadas las medidas, será necesaria la revisión y comprobación de su implantación real y de su eficacia."

La AEPD ha efectuado requerimientos de información a cinco de las empresas listadas por el reclamante, elegidas aleatoriamente, solicitando entre otra información sobre los siguientes aspectos:

- Número de empleados (usuarios del sistema de control horario).

- Descripción detallada del sistema de control horario utilizado con información sobre si utiliza tecnología de huella dactilar u otros datos biométricos para la identificación del empleado a la hora de fichar.
- Copia de la EIPD realizada por PRODAC para el sistema de control horario, así como de toda la documentación adicional relacionada que en su caso facilitara PRODAC.

Las cinco entidades requeridas han manifestado que no disponen de sistemas de control horario que utilicen tecnologías de huella digital u otros datos biométricos para la identificación del empleado, por lo que no han realizado ninguna EIPD.

Por su parte, el 19/02/2024 PRODAT, a iniciativa propia, informó a la AEPD de que había tenido conocimiento de la denuncia a través de sus clientes, porque un antiguo empleado suyo remitió un correo electrónico a todos los clientes informándoles de la denuncia presentada a la AEPD, sin ser ya empleado de PRODAT.

Considera PRODAT que la única motivación para la denuncia es causar un perjuicio reputacional a PRODAT y no el cumplimiento de la normativa de protección de datos. Por esta razón, PRODAT ha iniciado acciones judiciales contra el antiguo empleado (el denunciante).

FUNDAMENTOS DE DERECHO

I
Competencia

De acuerdo con las funciones que el artículo 57.1 a), f) y h) del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) confiere a cada autoridad de control y según lo dispuesto en los artículos 47 y 48.1 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 Presidencia 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
Conceptos previos

Del artículo 4 *"Definiciones"* del RGPD se extraen los conceptos de aplicación al caso:

7) «responsable del tratamiento» o «responsable»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros;

8) «encargado del tratamiento» o «encargado»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento;

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

Los responsables del tratamiento serían es este caso las personas físicas y jurídicas que planean o han decidido utilizar la huella digital como medio de control de la jornada laboral, por tratarse de los sujetos que determinan los fines y medios del tratamiento.

De conformidad con la información aportada por las empresas, PRODAT es una persona jurídica (S.L.) cuya función se limita en principio al asesoramiento para la EIPD sobre la utilización la huella digital como medio de control de la jornada laboral, por lo que no parece, en este caso, que tenga la condición de encargado del tratamiento, dado que no realiza tratamiento de datos personales por cuenta del responsable.

El tratamiento de datos dactiloscópicos necesario para el control horario de los trabajadores, implica el tratamiento técnico de los datos biométricos para la identificación única de la persona.

III

Tratamiento de categorías especiales de datos personales

El artículo 9 del RGPD, que regula el tratamiento de categorías especiales de datos personales, establece lo siguiente (se subraya lo relevante al caso):

"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 la orientación sexual de una persona física.

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

a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;

b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión o de los Estados miembros o un convenio colectivo

con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;

c) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento;

d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;

e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;

f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;

g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;

h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;

i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, sobre la base del Derecho de la Unión o de los Estados miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional;

j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.

3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un

profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.

4. Los Estados miembros podrán mantener o introducir condiciones adicionales, inclusive limitaciones, con respecto al tratamiento de datos genéticos, datos biométricos o datos relativos a la salud."

IV
Evaluación de impacto relativa a la protección de datos

La evaluación de impacto relativa a la protección de datos se regula en el artículo 35 del RGPD en los siguientes términos (se subraya lo relevante al caso):

"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."

Para que esta Agencia pueda declarar la existencia de una infracción en materia de protección de datos, resulta imprescindible constatar que el tratamiento de datos personales se ha realizado sin base jurídica válida o en vulneración de los principios y derechos establecidos en el RGPD. Asimismo, dicho tratamiento debe ser imputable a una persona física o jurídica identificada, en su condición de responsable o encargado del tratamiento.

El denunciante aportó como prueba un documento titulado “Análisis de Riesgos – Evaluación de Impacto de Privacidad. Tratamiento de datos de registro de jornada mediante huella dactilar”, que contiene múltiples campos sin completar (como “{Accounts.accountname}”), típicos de plantillas personalizables, lo que pone de manifiesto que se trata de un modelo genérico. Este tipo de documento está diseñado para ser adaptado a diferentes entidades, mediante la incorporación de sus datos identificativos, fechas u otras variables específicas, pero no constituye por sí mismo prueba de que el tratamiento descrito haya sido efectivamente implantado por las empresas mencionadas en la reclamación.
Durante el transcurso de las actuaciones de investigación, las empresas responsables del tratamiento a las que hizo referencia el denunciante han descartado el uso de la huella digital o de otros datos biométricos para el control horario de los trabajadores, optando en su lugar por bien una tarjeta o un código, o una combinación de ambos.

Por otro lado, la entidad denunciada, que figura como autora del documento modelo aportado por el denunciante, ha informado a esta Agencia que tuvo conocimiento de la reclamación presentada ante la AEPD por un antiguo empleado que, sin autorización y tras haber cesado su relación laboral, remitió el documento a clientes de la entidad, informando de la denuncia presentada. Esta conducta ha motivado el inicio de acciones judiciales contra dicha persona por los perjuicios reputacionales causados, considerando que la denuncia responde a un interés particular ajeno al cumplimiento de la normativa de protección de datos.

Por otra parte, en contestación a los requerimientos realizados por esta Agencia a empresas a las que PRODAT remitió el citado documento modelo, indican que su intervención se limita al asesoramiento jurídico y técnico en el ámbito de la protección de datos, sin que se pueda constatarse que PRODAT realice tratamiento de datos personales por encargo de dichas empresas.

Consecuentemente, no se han podido acreditar los hechos denunciados, ni que, en su caso, el tratamiento de datos personales se realizara en vulneración de los principios y derechos establecidos en el RGPD. Por tanto, no concurren indicios de infracción de la normativa aplicable ni elementos suficientes que permitan imputar responsabilidad alguna a la denunciada en materia de protección de datos.

V
Conclusión

Por lo tanto, en base a lo indicado en los párrafos anteriores, no se han encontrado evidencias que acrediten la existencia de infracción en el ámbito competencial de la Agencia Española de Protección de Datos.

Todo ello sin perjuicio de las posibles actuaciones posteriores que esta Agencia pudiera llevar a cabo, aplicando los poderes de investigación y correctivos que ostenta.

Así pues, al no haber sido posible atribuir la responsabilidad por el tratamiento de acuerdo con lo señalado, por la Presidencia de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución a **AUDITORES DE TRATAMIENTOS DE DATOS, S.L.**.

De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez sea firme en vía administrativa.

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 Presidencia 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.

940-120525

Lorenzo Cotino Hueso
Presidente de la Agencia Española de Protección de Datos