- **Procedimiento Nº: PS/00389/2019**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: El 23/04/2019 la POLICIA LOCAL del AYUNTAMIENTO DE BADAJOZ remitió Acta de denuncia contra el SERVICIO AJENO DE PREVENCION LABORAL EXTREMEÑA, S.L. (en lo sucesivo el reclamado), por presunta infracción a la normativa sobre protección de datos personales, al encontrar esparcidos por el suelo, junto a un vehículo de la empresa *Servicio ajeno de prevención Laboral Extremeña, S.L.* informes de reconocimientos médicos de fecha 02/12/2010 relativos a trabajadores de la empresa Aguas del Suroeste, S.L.

SEGUNDO: Tras la recepción de la reclamación, la Subdirección General de Inspección de Datos procedió a realizar las siguientes actuaciones:

El 18/05/2019, reiterada el 30/05/2019, fue trasladada al reclamante la reclamación presentada para su análisis y comunicación al reclamante de la decisión adoptada al respecto. Igualmente, se le requería para que en el plazo de un mes remitiera a la Agencia determinada información:

- Copia de las comunicaciones, de la decisión adoptada que haya remitido al reclamante a propósito del traslado de esta reclamación, y acreditación de que el reclamante ha recibido la comunicación de esa decisión.
- Informe sobre las causas que han motivado la incidencia que ha originado la reclamación.
- Informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares.
- Cualquier otra que considere relevante.

En la misma fecha se le comunicaba a la reclamante la recepción de la reclamación y su traslado a la entidad reclamada.

El 22/10/2019, de conformidad con el artículo 65 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos acordó admitir a trámite la reclamación presentada por el reclamante contra el reclamado.

TERCERO: Con fecha 24/02/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción por la presunta infracción de los artículos 32.1, 33 y 34 del RGPD, sancionada conforme a lo dispuesto en el artículo 83.4.a) del citado RGPD, considerando que la sanción que pudiera corresponder sería de APERCIBIMIENTO.

CUARTO: Notificado el acuerdo de inicio, el reclamado al tiempo de la presente resolución no ha presentado escrito de alegaciones, por lo que es de aplicación lo señalado en el artículo 64 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, que en su apartado f) establece que en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada, por lo que se procede a dictar Resolución.

QUINTO: De las actuaciones practicadas en el presente procedimiento, han quedado acreditados los siguientes:

HECHOS PROBADOS

PRIMERO: El 23/04/2019 tiene entrada en la AEPD oficio de la POLICIA LOCAL del AYUNTAMIENTO DE BADAJOZ por el que da traslado de Acta de denuncia contra el SERVICIO AJENO DE PREVENCION LABORAL EXTREMEÑA, S.L. (en lo sucesivo el reclamado), por presunta infracción a la normativa sobre protección de datos personales, al encontrar esparcidos por el suelo, junto a un vehículo de la empresa Servicio Ajeno de Prevención Laboral Extremeña, S.L. informes de reconocimientos médicos relativos a trabajadores de la empresa Aguas del Suroeste, S.L..

SEGUNDO: Consta aportada copia del Acta de la denuncia formulada por la Policía Local del Ayuntamiento de Badajoz nº 10735 señalando: *"Se hallan esparcidos por el suelo, junto a un vehículo de la empresa Servicio ajeno de Prevención Laboral Extremeña, S.L., informes de reconocimiento médicos de fecha 02/12/10",* continuando: *"Los referidos informes médicos son relativos a trabajadores de la empresa Aguas del Suroeste, S.L. Se adjuntan fotocopias de los mismos".*

Como medida cautelar se indica por la Policía: *"Se retiran dichos informes de la vía".*

TERCERO: Constan aportadas copias de *"Informes del reconocimiento médico Periódico Ordinario practicado en el Área de Medicina Laboral del Servicio de Prevención el día 2 de diciembre de 2010 a",* relativos a dos trabajadores de la empresa Aguas del Suroeste, S.L.

CUARTO: El reclamado no ha dado respuesta a ninguno de los requerimientos formulados por la AEPD; tampoco ha realizado alegaciones al acuerdo de inicio del procedimiento sancionador.

FUNDAMENTOS DE DERECHO

I

En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en el art. 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), la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, en su artículo 64 *"Acuerdo de iniciación en los procedimientos de naturaleza sancionadora",* dispone:

"1. El acuerdo de iniciación se comunicará al instructor del procedimiento, con traslado de cuantas actuaciones existan al respecto, y se notificará a los interesados, entendiendo en todo caso por tal al inculpado.

Asimismo, la incoación se comunicará al denunciante cuando las normas reguladoras del procedimiento así lo prevean.

2. El acuerdo de iniciación deberá contener al menos:

a) Identificación de la persona o personas presuntamente responsables.

b) Los hechos que motivan la incoación del procedimiento, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.

c) Identificación del instructor y, en su caso, Secretario del procedimiento, con expresa indicación del régimen de recusación de los mismos.

d) Órgano competente para la resolución del procedimiento y norma que le atribuya tal competencia, indicando la posibilidad de que el presunto responsable pueda reconocer voluntariamente su responsabilidad, con los efectos previstos en el artículo 85.

e) Medidas de carácter provisional que se hayan acordado por el órgano competente para iniciar el procedimiento sancionador, sin perjuicio de las que se puedan adoptar durante el mismo de conformidad con el artículo 56.

f) Indicación del derecho a formular alegaciones y a la audiencia en el procedimiento y de los plazos para su ejercicio, así como indicación de que, en caso de no efectuar alegaciones en el plazo previsto sobre el contenido del acuerdo de iniciación, éste podrá ser considerado propuesta de resolución cuando contenga un pronunciamiento preciso acerca de la responsabilidad imputada.

3. Excepcionalmente, cuando en el momento de dictar el acuerdo de iniciación no existan elementos suficientes para la calificación inicial de los hechos que motivan la incoación del procedimiento, la citada calificación podrá realizarse en una fase posterior mediante la elaboración de un Pliego de cargos, que deberá ser notificado a los interesados".

En aplicación del anterior precepto y teniendo en cuenta que no se han formulado alegaciones al acuerdo de inicio, procede resolver el procedimiento iniciado.

III

El artículo 58 del RGPD, *Poderes,* señala:

"2. Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:

(…)

i) imponer una multa administrativa con arreglo al artículo 83, además o en lugar de las medidas mencionadas en el presente apartado, según las circunstancias de cada caso particular;

(…)"

El RGPD establece en el artículo 5 de los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *"integridad y confidencialidad".*

El artículo señala que:

"1. Los datos personales serán:

(…)

f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»)".

A su vez, la seguridad de los datos personales viene regulado en los artículos 32, 33 y 34 del RGPD.

El artículo 32 del RGPD *"Seguridad del tratamiento",* establece que:

"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;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;
c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) 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 33 del RGPD, *Notificación de una violación de la seguridad de los datos personales a la autoridad de control,* establece que:

"1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.

2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

3. La notificación contemplada en el apartado 1 deberá, como mínimo:

a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.

5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo".

Y el artículo 34, *Comunicación de una violación de la seguridad de los datos personales al interesado*, establece que:

"1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;
b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;
c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3".

IV

En el presente caso, consta acreditado que el 23/04/2019 la POLICIA LOCAL del AYUNTAMIENTO DE BADAJOZ aportaba copia del Acta de denuncia contra el reclamado, en el que se evidencia la infracción a la normativa sobre protección de datos personales, al hallarse esparcidos en la vía pública y junto a un vehículo de su propiedad informes de reconocimientos médicos relativos a trabajadores de la empresa *Aguas del Suroeste, S.L.* conteniendo datos sensibles y especialmente protegidos y procediendo las citadas fuerzas del orden a su retirada de la vía pública como medida cautelar.

Por otra parte, llama la atención la ausencia de sensibilidad del reclamado ante los citados hechos puesto que ni contestó a los requerimientos de información efectuados por la AEPD, ni respondió presentado escrito de alegaciones al inicio de acuerdo de procedimiento sancionador y que, además, tiene por objeto promover la

seguridad y la salud de los trabajadores mediante el desarrollo de actividades necesarias y convenientes para la prevención de riesgos derivados del trabajo.

Hay que señalar que el RGPD define las violaciones de seguridad de los datos personales como *"todas aquellas violaciones de la seguridad que ocasionen la destrucción, perdida o alteración accidental o ilícita de datos personales trasmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".*

De la documentación obrante en el expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse una brecha de seguridad en sus sistemas permitiendo y proporcionando el acceso a los datos relacionados con informes de reconocimientos médicos de fecha 02/12/2010 de trabajadores de la empresa Aguas del Suroeste que se encontraban esparcidos por el suelo.

El RGPD en el citado precepto no establece un listado de las medidas de seguridad que sean de aplicación de acuerdo con los datos que son objeto de tratamiento, sino que establece que el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas que sean adecuadas al riesgo que conlleve el tratamiento, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, alcance, contexto y finalidades del tratamiento, los riesgos de probabilidad y gravedad para los derechos y libertades de las personas interesadas.

Asimismo, las medidas de seguridad deben resultar adecuadas y proporcionadas al riesgo detectado, señalando que la determinación de las medidas técnicas y organizativas deberá realizarse teniendo en cuenta: la seudonimización y el cifrado, la capacidad para garantizar la confidencialidad, integridad, disponibilidad y resiliencia, la capacidad para restaurar la disponibilidad y acceso a datos tras un incidente, proceso de verificación (que no auditoría), evaluación y valoración de la eficacia de las medidas.

En todo caso, al evaluar la adecuación del nivel de seguridad se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, 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 y que pudieran ocasionar daños y perjuicios físicos, materiales o inmateriales.

En este mismo sentido el considerando 83 del RGPD señala que:

"(83) 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".

Tal y como se señalaba con anterioridad y en el marco del expediente de investigación ******EXPEDIENTE.1*** la AEPD traslado al reclamado el 18/05/2019 y el 30/05/2019 la reclamación presentada para su análisis solicitando la aportación de información relacionada con la incidencia reclamada, sin que se haya recibido en este organismo respuesta alguna.

La responsabilidad del reclamado viene determinada por la quiebra de seguridad puesta de manifiesto por la Policía Local del Ayuntamiento de Badajoz, ya que es responsable de tomar decisiones destinadas a implementar de manera efectiva las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo para asegurar la confidencialidad de los datos, restaurando su disponibilidad e impedir el acceso a los mismos en caso de incidente físico o técnico. Sin embargo, de la documentación aportada se desprende que la entidad no solo ha incumplido esta obligación, sino que además se desconoce la adopción de medidas al respecto, pesar de haberle dado traslado de la reclamación presentada.

El RGPD también regula en su artículo 33 la notificación de las violaciones de seguridad que pueden suponer un riesgo para los derechos y libertades de las personas físicas a la autoridad de control competente, que en el caso español se trata de la AEPD.

Por tanto, siempre que en una brecha se vean afectados datos de carácter personal de personas físicas deberemos comunicarlo a la AEPD y, además, deberemos notificarla en un plazo máximo de 72 horas a contar desde que tengamos conocimiento de la brecha.

Por último, hay que añadir que habiéndole sido comunicado el incidente de seguridad tampoco se tiene noticia de que hubiera adoptado medidas tendentes a poner remedio al mismo, una vez tuvo conocimiento del mismo.

Como tampoco se tiene constancia que, de conformidad con lo señalado en el artículo 34 hubiera comunicado a los interesados la violación de la seguridad de los datos personales sin dilaciones indebidas una vez tuvo conocimiento de ellos.

De conformidad con lo que antecede, el reclamado sería responsable de las infracciones del RGPD: la vulneración de los artículos 32, 33 y 34, infracciones tipificadas todas ellas en su artículo 83.4.a).

V

La vulneración de los artículos 32, 33 y 34 del RGPD se encuentran tipificadas en el artículo 83.4.a) del citado RGPD en los siguientes términos:

"4. 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.
(…)"

La LOPDGDD en su artículo 71, *Infracciones*, señala que: *"Constituyen infracciones los actos y conductas a las que se refieren los apartados 4, 5 y 6 del artículo 83 del Reglamento (UE) 2016/679, así como las que resulten contrarias a la presente ley orgánica".*

Y en su artículo 73, a efectos de prescripción, califica de *"Infracciones consideradas graves":*

"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:

(…)

g) El quebrantamiento, como consecuencia de la falta de la debida diligencia, de las medidas técnicas y organizativas que se hubiesen implantado conforme a lo exigido por el artículo 32.1 del Reglamento (UE) 2016/679".

r) El incumplimiento del deber de notificación a la autoridad de protección de datos de una violación de seguridad de los datos personales de conformidad con lo previsto en el artículo 33 del Reglamento (UE) 2016/679.

s) El incumplimiento del deber de comunicación al afectado de una violación de la seguridad de los datos de conformidad con lo previsto en el artículo 34 del Reglamento (UE) 2016/679 si el responsable del tratamiento hubiera sido requerido por la autoridad de protección de datos para llevar a cabo dicha notificación.

Los hechos puestos de manifiesto en la reclamación se concretan en la existencia de una brecha de seguridad en los sistemas de la reclamada permitiendo la vulnerabilidad del mismo al permitir que informes de fecha 02/12/2010 relativos a reconocimientos médicos y pertenecientes a trabajadores de la empresa Aguas del Suroeste, estuvieran esparcidos en la vía pública y permitiendo el acceso a los datos contenidos en los mismos.

Todo ello constituye una vulneración de la seguridad de los datos personales lo que constituye una infracción de los artículos 32.1, 33 y 34 del RGPD.

VI

No obstante, el artículo 58.2 del REPD dispone lo siguiente: *"Cada autoridad de control dispondrá de todos los siguientes poderes correctivos indicados a continuación:*

(…)

b) sancionar a todo responsable o encargado del tratamiento con apercibimiento cuando las operaciones de tratamiento hayan infringido lo dispuesto en el presente Reglamento;

(…)"

El RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 58.2 b) la posibilidad de acudir al apercibimiento para corregir los tratamientos de datos personales que no se adecúen a sus previsiones.

En el supuesto que nos ocupa ha quedado acreditado que el reclamado no tiene aplicadas medidas técnicas y organizativas para garantizar un nivel de seguridad adecuado capaz de garantizar la confidencialidad, integridad, disponibilidad de los datos evitando su acceso; medidas adecuadas para proceder a la notificación en caso de una violación de la seguridad de los datos personales y el procedimiento implantado para el caso de que la violación de la seguridad de los datos personales entrañe un alto riesgo ara los derechos y libertades de las personas físicas.

VII

El reclamado no ha dado respuesta al requerimiento de información formulado por el Servicio de Inspección.

En este punto, se hace necesario informar que no atender los requerimientos de la Agencia puede ser constitutivo de infracción muy grave de conformidad con lo señalado en el artículo 72 de la LOPDGDD, que establece: *"1. En función de lo que establece el artículo 83.5 del Reglamento (UE) 2016/679 se consideran muy graves y prescribirán a los tres años las infracciones que supongan una vulneración sustancial de los artículos mencionados en aquel y, en particular, las siguientes:*

(…)

ñ) No facilitar el acceso del personal de la autoridad de protección de datos competente a los datos personales, información, locales, equipos y medios de tratamiento que sean requeridos por la autoridad de protección de datos para el ejercicio de sus poderes de investigación.

o) La resistencia u obstrucción del ejercicio de la función inspectora por la autoridad de protección de datos competente".

(…)"

Paralelamente, notificado el acuerdo de inicio y transcurrido el plazo otorgado para formular alegaciones, no presento escrito alguno.

Como se señalaba con anterioridad ha quedado acreditado que el reclamado no tiene adoptadas medidas técnicas y organizativas que garanticen un nivel de seguridad adecuado capaz de asegurar la confidencialidad, integridad y disponibilidad de los datos evitando su acceso, perdida, etc.; medidas adecuadas para proceder a la notificación en caso de una violación de la seguridad de los datos personales y el procedimiento implantado para el caso de que la violación de la seguridad de los datos personales entrañe un alto riesgo ara los derechos y libertades de las personas físicas..

Se hace necesario señalar que de no corregir dichas incidencias adoptando las medidas técnicas y organizativas adecuadas adaptándolas a lo señalado en los artículos 32.1, 33 y 34 del RGPD o bien reiterar la conducta puesta de manifiesto en la reclamación y que es causa del presente procedimiento, así como no informar seguidamente a esta AEPD de las medidas adoptadas podría dar lugar al ejercicio de posibles actuaciones ante el responsable del tratamiento a fin de que se apliquen de manera efectiva las medidas apropiadas para garantizar y no comprometer la confidencialidad de los datos de carácter personal y el derecho a la intimidad de las personas.

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 SERVICIO AJENO DE PREVENCION LABORAL EXTREMEÑA, S.L., con NIF ***B06307748***, por infracción de los artículos 32.1, 33 y 34 del RGPD, tipificada conforme a lo dispuesto en el artículo 83.4.a) del citado RGPD, una sanción de apercibimiento.

SEGUNDO: REQUERIR a SERVICIO AJENO DE PREVENCION LABORAL EXTREMEÑA, S.L. con NIF ***B06307748,*** para que en el plazo de un mes desde la notificación de esta resolución, acredite: la adopción de las medidas de seguridad necesarias y pertinentes de conformidad con la normativa en materia de protección de datos de carácter personal a fin de evitar que en el futuro vuelvan a producirse incidencias como las que han dado lugar a la reclamación corrigiendo los efectos de la infracción el acceso a los datos, adecuando las citadas medidas a las exigencias contempladas en el artículo 32.1 del RGPD; las medidas adoptadas para proceder a la notificación en caso de una violación de la seguridad de los datos personales de acuerdo a lo señalado en el artículo 33 del RGPD y el procedimiento implantado para el caso de que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, de conformidad con lo señalado en el artículo 34 del RGPD.

TERCERO: NOTIFICAR la presente resolución a SERVICIO AJENO DE PREVENCION LABORAL EXTREMEÑA, S.L. con NIF ***B06307748.***

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.

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