

- Procedimiento N°: PS/00054/2021

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: La **D. G. DE LA GUARDIA CIVIL - PUESTO PRINCIPAL DE ***LOCALIDAD.1** (en adelante, el reclamante) con fecha 07/08/2019 remitió oficio ante la Agencia Española de Protección de Datos, en el que se adjunta escrito por posible vulneración de la normativa sobre protección de datos. La reclamación se dirige contra ELECTROTECNIA BASTIDA, S.L. con CIF B96466461 (en adelante, el reclamado). Los motivos en que basa la reclamación son, que en un descampado del polígono industrial de la localidad se encuentra en estado de abandono sobres conteniendo información médica confidencial, conteniendo datos de carácter personal correspondientes a trabajadores del reclamado.

SEGUNDO: A la vista de los hechos denunciados y de los documentos aportados por el reclamante de los que ha tenido conocimiento esta Agencia, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones para el esclarecimiento de los hechos en cuestión.

El 15/10/2019 fue trasladada al reclamado la reclamación presentada para su análisis y comunicación a la denunciante 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.

El reclamado no ha dado respuesta al requerimiento formulado por la Agencia Española de Protección de Datos.

TERCERO: El 08/06/2020, 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.

CUARTO: Con fecha 12/02/2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, por la presunta infracción de artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del citado RGPD.

QUINTO: 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.

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

HECHOS PROBADOS

PRIMERO: En fecha 07/08/2019 la G.C. de *****LOCALIDAD.1** remitió oficio a la AEPD, en el que adjunta escrito por posible vulneración de la normativa sobre protección de datos por el reclamado, motivado por el abandono de documentación médica confidencial de sus trabajadores, en un descampado del polígono industrial de la localidad.

SEGUNDO: Consta aportado Informe de la G.C. en el que se señala que la patrulla del puesto se dirigió al polígono industrial tomando fotografías del lugar donde se encontraban los documentos, recogiendo los mismos que fueron trasladados al cuartel; que los documentos son 29 sobres, dos de ellos abiertos, de la Clínica *****CLÍNICA.1** (Gestión de medicina y prevención, SL) figurando en cada uno de ellos el nombre y apellidos de los trabajadores del reclamado que solicitan un “Examen específico de salud”; que se examina uno de los sobres que se encontraba abierto y en su interior figuran dos informes: “Examen específico de salud” y un segundo informe de dos folios de la clínica *****CLÍNICA.2** de *****LOCALIDAD.2** (Valencia); que el 25/06/2019 el agente que suscribe el informe se personó en el domicilio del reclamado e identificado el administrador de la entidad, el cual no supo dar explicación del abandono de la documentación de sus trabajadores en el descampado. Se deja igualmente constancia en el Informe del listado de las 29 personas afectadas por los hechos junto a la fecha de realización del examen específico de salud.

TERCERO: Consta reportaje fotográfico, aportando fotografía general de la documentación abandonada, 29 sobres; así como fotografía detallada de uno de los sobres donde consta el membrete de *confidencial*.

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 los artículos 47 y 48 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para iniciar y para resolver este procedimiento.

II

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

“2. 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 artículo 5 del RGPD establece los principios que han de regir el tratamiento de los datos personales y menciona entre ellos el de *“integridad y confidencialidad”*.

El citado 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»).

(...)

III

Los hechos denunciados se materializan en el abandono en un descampado del polígono industrial de la localidad de *****LOCALIDAD.1**, documentación conteniendo datos confidenciales de carácter personal posibilitando su acceso a terceros; datos que corresponden a trabajadores del reclamado, vulnerando la normativa en materia de protección de datos.

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”.

La vulneración del artículo 32 del RGPD se encuentra tipificada 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.
(...)”

Por su parte, la LOPDGDD 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”.
(...)”

IV

El RGPD define las violaciones de seguridad de los datos personales como “todas aquellas violaciones de la seguridad que ocasionen 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”.

De la documentación aportada al expediente se ofrecen indicios evidentes de que el reclamado ha vulnerado el artículo 32 del RGPD, al producirse un incidente de seguridad, al ser abandonados documentos conteniendo datos personales sensibles de trabajadores del reclamado, permitiendo el acceso a los mismos por terceros con quebrantamiento de las medidas establecidas.

Hay que señalar que 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”.

En el presente caso, tal y como consta en los hechos y en el marco del expediente de investigación E/09606/2019 la AEPD trasladó al reclamado el 15/10/2019, 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 el reclamante, 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.

De conformidad con lo que antecede, se estima que el reclamado sería presuntamente responsable de la infracción del RGPD: la vulneración del artículo 32, infracción tipificada en su artículo 83.4.a).

V

A fin de establecer la multa administrativa que procede imponer han de observarse las previsiones contenidas en los artículos 83.1 y 83.2 del RGPD, que señalan:

“1. Cada autoridad de control garantizará que la imposición de las multas administrativas con arreglo al presente artículo por las infracciones del presente Reglamento indicadas en los apartados 4, 5 y 6 sean en cada caso individual efectivas, proporcionadas y disuasorias.

2. Las multas administrativas se impondrán, en función de las circunstancias de cada caso individual, a título adicional o sustitutivo de las medidas contempladas en el artículo 58, apartado 2, letras a) a h) y j). Al decidir la imposición de una multa administrativa y su cuantía en cada caso individual se tendrá debidamente en cuenta:

- a) la naturaleza, gravedad y duración de la infracción, teniendo en cuenta la naturaleza, alcance o propósito de la operación de tratamiento de que se trate así como el número de interesados afectados y el nivel de los daños y perjuicios que hayan sufrido;*
- b) la intencionalidad o negligencia en la infracción;*
- c) cualquier medida tomada por el responsable o encargado del tratamiento para paliar los daños y perjuicios sufridos por los interesados;*
- d) el grado de responsabilidad del responsable o del encargado del tratamiento, habida cuenta de las medidas técnicas u organizativas que hayan aplicado en virtud de los artículos 25 y 32;*
- e) toda infracción anterior cometida por el responsable o el encargado del tratamiento;*
- f) el grado de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la infracción;*
- g) las categorías de los datos de carácter personal afectados por la infracción;*
- h) la forma en que la autoridad de control tuvo conocimiento de la infracción, en particular si el responsable o el encargado notificó la infracción y, en tal caso, en qué medida;*

- i) cuando las medidas indicadas en el artículo 58, apartado 2, hayan sido ordenadas previamente contra el responsable o el encargado de que se trate en relación con el mismo asunto, el cumplimiento de dichas medidas;*
- j) la adhesión a códigos de conducta en virtud del artículo 40 o a mecanismos de certificación aprobados con arreglo al artículo 42, y*
- k) cualquier otro factor agravante o atenuante aplicable a las circunstancias del caso, como los beneficios financieros obtenidos o las pérdidas evitadas, directa o indirectamente, a través de la infracción.*

En relación con la letra k) del artículo 83.2 del RGPD, la LOPDGDD, en su artículo 76, “Sanciones y medidas correctivas”, establece que:

“2. De acuerdo con lo previsto en el artículo 83.2.k) del Reglamento (UE) 2016/679 también podrán tenerse en cuenta:

- a) El carácter continuado de la infracción.*
- b) La vinculación de la actividad del infractor con la realización de tratamientos de datos personales.*
- c) Los beneficios obtenidos como consecuencia de la comisión de la infracción.*
- d) La posibilidad de que la conducta del afectado hubiera podido inducir a la comisión de la infracción.*
- e) La existencia de un proceso de fusión por absorción posterior a la comisión de la infracción, que no puede imputarse a la entidad absorbente.*
- f) La afectación a los derechos de los menores.*
- g) Disponer, cuando no fuere obligatorio, de un delegado de protección de datos.*
- h) El sometimiento por parte del responsable o encargado, con carácter voluntario, a mecanismos de resolución alternativa de conflictos, en aquellos supuestos en los que existan controversias entre aquellos y cualquier interesado.”*

- De acuerdo con los preceptos transcritos, a efectos de fijar el importe de la sanción de multa a imponer en el presente caso por la infracción tipificada en el artículo 83.4.a) del RGPD de la que se responsabiliza al reclamado, en una valoración inicial, se estiman concurrentes los siguientes factores:

La naturaleza y gravedad de la infracción dada que se trata de datos especialmente sensibles de trabajadores del reclamado.

El alcance meramente local del tratamiento llevado a cabo por la entidad reclamada.

El elevado número de personas cuyos datos se han visto afectados por la conducta infractora (29).

La entidad reclamada no consta que haya adoptado medidas para evitar que se produzcan incidencias similares; tampoco ha respondido al requerimiento informativo de la Agencia lo que incide en la ausencia de cooperación con la autoridad de control con el fin de poner remedio a la infracción y mitigar los posibles efectos adversos de la misma.

No se tiene constancia de que la entidad hubiera obrado dolosamente, aunque la actuación revela una grave falta de diligencia.

La vinculación de la actividad del infractor con la realización de tratamientos de datos de carácter personal.

La entidad reclamada es una pequeña empresa.

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 ELECTROTECNIA BASTIDA, S.L., con CIF B96466461, por una infracción del artículo 32.1 del RGPD, tipificada en el artículo 83.4.a) del RGPD, una multa de 3.000 € (tres mil euros), de conformidad con el artículo 73.g) de la LOPDGDD.

SEGUNDO: NOTIFICAR la presente resolución a ELECTROTECNIA BASTIDA, S.L., con CIF B96466461.

TERCERO: Advertir al sancionado que deberá hacer efectiva la sanción impuesta una vez que la presente resolución sea ejecutiva, de conformidad con lo dispuesto en el art. 98.1.b) de la ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante LPACAP), en el plazo de pago voluntario establecido en el art. 68 del Reglamento General de Recaudación, aprobado por Real Decreto 939/2005, de 29 de julio, en relación con el art. 62 de la Ley 58/2003, de 17 de diciembre, mediante su ingreso, indicando el NIF del sancionado y el número de procedimiento que figura en el encabezamiento de este documento, en la cuenta restringida nº **ES00 0000 0000 0000 0000 0000**, abierta a nombre de la Agencia Española de Protección de Datos en la entidad bancaria CAIXABANK, S.A.. En caso contrario, se procederá a su recaudación en período ejecutivo.

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

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

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer, potestativamente, recurso de reposición ante la Directora de la Agencia Española de Protección de Datos en el plazo de un mes a contar desde el día siguiente a la notificación de esta resolución o directamente recurso contencioso administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de

la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

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

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