- Procedimiento Nº: PS/00463/2019

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: D. ***A.A.A.*** (en adelante, el reclamante) con fecha 17/10/2018 interpuso reclamación ante la Agencia Española de Protección de Datos. La reclamación se dirige contra AYUNTAMIENTO DE BAENA, con NIF ***P1400700I*** (en adelante, el reclamado o AYUNTAMIENTO). Los motivos en que basa la reclamación son según manifestaciones del denunciante, en síntesis: que al comprobar en la sede electrónica del reclamado, mediante el código seguro de verificación (CSV), el certificado colectivo de empadronamiento que había solicitado su padre, el sistema de la sede electrónica devuelve 23 certificados de diversa índole relacionados con el padrón donde aparecen datos personales de los componentes de la familia del reclamante y de los interesados de los otros 22 certificados firmados el mismo día. Todos los certificados firmados el mismo día tienen el mismo CSV. El reclamante solicita que ya que no se puede cambiar el CSV una vez generado, se introduzca en el sistema un campo adicional o segundo paso donde se solicite el DNI para poder discriminar el documento correcto antes de visualizarlo.

SEGUNDO: A la vista de los hechos denunciados en la reclamación y de los documentos aportados por el reclamante, 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 los poderes de investigación otorgados a las autoridades de control en el artículo 57.1 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 Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en lo sucesivo LOPDGDD).

Con fecha 23/07/2019 se solicita al reclamante que especifique el CSV y los documentos a los que hace referencia en su reclamación.

Con fecha 29/07/2019 se recibe en esta Agencia escrito remitido por el reclamante aportando la información solicitada.

Y anexa la siguiente documentación:

• Certificado Colectivo de Inscripción Padronal correspondiente a la familia del reclamante

• Los 23 documentos mostrados en la sede electrónica del AYUNTAMIENTO al introducir como código de verificación el correspondiente al certificado del reclamante.

Los antecedentes que constan son los siguientes:

Con fecha de notificación de 13/12/2018 se da traslado de la reclamación al AYUNTAMIENTO solicitando la siguiente información: (i) 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, (ii) informe sobre las causas que han motivado la incidencia que ha originado la reclamación, (iii) informe sobre las medidas adoptadas para evitar que se produzcan incidencias similares y (iv) cualquier otra que considere relevante.

Con fecha de 13/02/2019, sin haberse recibido en esta Agencia la información solicitada en el traslado de la reclamación, se acuerda admitir a trámite la reclamación presentada por el reclamante contra el AYUNTAMIENTO.

Pese a que ha sido informado el AYUNTAMIENTO mediante el traslado de la reclamación de la incidencia detectada, aún sigue exponiendo los datos personales de los interesados que constan en los 23 documentos del padrón que se obtienen al introducir el CSV del certificado colectivo de inscripción padronal.

TERCERO: Con fecha 07/02/2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al reclamado, 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.

CUARTO: Notificado el citado acuerdo de inicio, en escrito de 06/03/2020 el reclamado manifestaba ser cierto que en la emisión del certificado señalado por el reclamante se incluyeron por error otros certificados confeccionados aquel día y que fueron digitalizados en conjunto; que en relación con dicho incidencia por el Técnico informático se emitió informe sobre las causas que motivaron la misma y que originaron la reclamación y las medidas adoptadas para evitar que se produzcan hechos similares; que por la Jefa de Negociado del Servicio de Atención Ciudadana donde se expiden dichos certificados emitió informe del que se desprende que en la actualidad dichos certificados sean de la clase que sean se emiten de manera individualizada y de forma automatizadas a través de GEX.

SEXTO: En fecha 02/06/2020 fue dictada Propuesta de Resolución en el sentido de que se sancionara con apercibimiento al reclamado por vulneración de los artículos 32.1, 33 y 34 del RGPD, tipificadas en el artículo 83.4.a) del citado RGPD y sancionada conforme a lo dispuesto en el artículo 77.2 de la LOPDGDD.

Transcurrido el plazo establecido para ello el reclamado no ha presentado escrito de alegaciones al tiempo de dictar la presente resolución.

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

HECHOS PROBADOS

PRIMERO. El 17/10/2018 tiene entrada en la AEPD escrito del reclamante manifestando que al comprobar en la sede electrónica del reclamado, mediante el código seguro de verificación (CSV), el certificado colectivo de empadronamiento que había solicitado su padre, el sistema de la sede electrónica devuelve 23 certificados de diversa índole relacionados con el padrón donde aparecen datos personales de los componentes de la familia del reclamante y de los interesados de los otros 22

certificados firmados el mismo día. Todos los certificados firmados el mismo día tienen el mismo CSV.

SEGUNDO. Consta aportado Certificado Colectivo de Empadronamiento solicitado por el padre, en el que figuran las personas inscritas en el domicilio.

TERCERO. Constan aportados por el reclamante 23 documentos solicitados por personas distintas y relativos a diferentes tipos de certificaciones expedidos por el Padrón Municipal de Habitantes del Ayuntamiento de Baena que comparten CSV y fecha de expedición: Certificados Colectivos, Individuales, Históricos de Movimientos y cambios de datos o padrón, Nuevas Altas, etc,.). En los citados documentos figuran datos de carácter personal relativos a las personas inscritas: nombre y apellidos, lugar y fecha de nacimiento, DNI, domicilio y fecha de alta en el Padrón, etc.

CUARTO. El reclamado ha aportado informe técnico elaborado por el Responsable Informático municipal en el que se analizan las causas que motivaron la incidencia así como las medidas técnicas y correctoras adoptadas para evitar que se produzcan hechos similares en el futuro.

También consta que se solicitó al Departamento de Atención Ciudadana que se emitiera informe sobre la forma de emitir los certificados colectivos de empadronamiento señalándose que tanto los certificados individuales como los colectivos y los históricos, individuales y colectivos, que se expidieran desde el Padrón de Habitantes se hicieran de manera individualizada y automatizada a través de GEX.

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:

(…)

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".

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.

(…)"

Por su parte, 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 presente reclamación evidencian la existencia de un incidente de seguridad en los sistemas del reclamado permitiendo la vulnerabilidad del mismo al posibilitar que el sistema de su sede electrónica permitiera el acceso a los datos relacionados con el padrón donde figuraban además de los datos personales de los componentes de la familia del reclamante los de otros interesados.

III

En el presente caso, el reclamante al comprobar en la sede electrónica del reclamado, mediante el código seguro de verificación (CSV), el certificado colectivo de empadronamiento que había solicitado su padre, el sistema de la sede electrónica devuelve 23 certificados de diversa índole relacionados con el padrón donde aparecen datos personales de los componentes de la familia del reclamante y de los interesados de los otros 22 certificados firmados el mismo día. Todos los certificados firmados el mismo día tienen el mismo CSV. El reclamante solicita que ya que no se puede cambiar el CSV una vez generado, se introduzca en el sistema un campo adicional o segundo paso donde se solicite el DNI para poder discriminar el documento correcto antes de visualizarlo.

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 el acceso a los datos relacionados con el padrón.

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/01827/2019 la AEPD el 13/12/2018 dio traslado de la reclamación al reclamado solicitando la aportación de información relacionada con la incidencia reclamada, sin que se recibiera en este organismo respuesta alguna y, a pesar del requerimiento anterior, se acreditó que se seguían exponiendo los datos personales de los interesados que constaban en los 23 documentos del padrón que se obtenían al introducir el código seguro de verificación del certificado colectivo de inscripción padronal.

Hay que señalar, que 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 y, entre ellas, las dirigidas a restaurar la disponibilidad y el acceso a los datos de forma rápida en caso de incidente físico o técnico. Sin embargo, de la documentación aportada se desprende que la entidad no solo incumplió esta obligación, sino que además no había adoptado ninguna medida a pesar de haberle dado traslado de la reclamación informándole de ello.

También el RGPD 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.

Hay que señalar, que ninguna de estas obligaciones fue atendida por el reclamado; todo lo contrario, habiéndole sido comunicado el incidente de seguridad puesto de manifiesto en la reclamación, no remitió a la AEPD noticia alguna 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, que hubiera comunicado a los interesados la violación de la seguridad de los datos personales sin dilaciones indebidas una vez tuvo conocimiento de ello.

No obstante, también es cierto que aperturado el acuerdo de inicio del procedimiento sancionador, en escrito de alegaciones de fecha 06/03/2020 el reclamado confirmaba la infracción cometida y manifestaba ser cierto que en la emisión del certificado señalado por el reclamante se incluyeron por error otros certificados confeccionados aquel día y que fueron digitalizados en conjunto.

Asimismo ha señalado que en relación con la incidencia producida el Técnico Informático había emitido un informe sobre las causas que motivaron la misma y que originaron la reclamación así como las medidas adoptadas para evitar que se produzcan hechos similares en el futuro. Además, la Jefa del Negociado del Servicio de Atención Ciudadana donde se expiden dichos certificados emitió igualmente informe del que se desprende que en la actualidad dichos certificados sean de la clase que sean se emiten de manera individualizada y de forma automatizada.

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

IV

No obstante, también la LOPDGDD en su artículo 77, *Régimen aplicable a determinadas categorías de responsables o encargados del tratamiento*, establece lo siguiente:

"1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

a) Los órganos constitucionales o con relevancia constitucional y las instituciones de las comunidades autónomas análogas a los mismos.

b) Los órganos jurisdiccionales.

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local.

d) Los organismos públicos y entidades de Derecho público vinculadas o dependientes de las Administraciones Públicas.

e) Las autoridades administrativas independientes.

f) El Banco de España.

g) Las corporaciones de Derecho público cuando las finalidades del tratamiento se relacionen con el ejercicio de potestades de derecho público.

h) Las fundaciones del sector público.

i) Las Universidades Públicas.

j) Los consorcios.

k) Los grupos parlamentarios de las Cortes Generales y las Asambleas Legislativas autonómicas, así como los grupos políticos de las Corporaciones Locales.

2. Cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de

esta ley orgánica, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

3. Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

4. Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

5. Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

6. Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 de este artículo, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda a una autoridad autonómica de protección de datos se estará, en cuanto a la publicidad de estas resoluciones, a lo que disponga su normativa específica".

De conformidad con las evidencias de las que se dispone, dicha conducta constituye por parte del reclamado la infracción a lo dispuesto en los artículos 32.1, 33 y 34 del RGPD.

Hay que señalar que el RGPD, sin perjuicio de lo establecido en su artículo 83, contempla en su artículo 77 la posibilidad de acudir a la sanción de *apercibimiento* para corregir los tratamientos de datos personales que no se adecúen a sus previsiones, cuando los responsables o encargados enumerados en el apartado 1 cometiesen alguna de las infracciones a las que se refieren los artículos 72 a 74 de esta ley orgánica.

En el presente caso, atendiendo a la naturaleza de la infracción y habida cuenta que el reclamado en escrito de fecha 06/03/2020 ha informado a esta Agencia las circunstancias en las que se produjo la incidencia que propició la reclamación así como las medidas adoptadas a fin de evitar que hechos como el reclamado vuelvan a producirse en el futuro. Asimismo, reconoce el error cometido y que en la emisión del

certificado señalado por el reclamante se incluyeron otros certificados confeccionados aquel día siendo digitalizados en conjunto y remitidos al circuito digital por lo que el contenido del fichero contuvo la misma firma y mismo CSV; ante dicha incidencia el Técnico Informático municipal ha emitido informe sobre las causas que motivaron la incidencia y las medidas técnicas adoptadas para evitar que se produzcan hechos similares en el futuro. De la misma forma, la Jefa de Negociado del Servicio de Atención Ciudadana donde se expiden dichos certificados ha emitido informe señalando que los certificados individuales, colectivos e históricos individuales y colectivos que se expidan desde el Padrón de Habitantes se hace de forma individualizada y automatizada.

Por tanto, se considera que la respuesta del reclamado ha sido razonable y diligente, reconociendo los hechos y subsanando de manera inmediata los errores cometidos, no teniéndose constancia de otras reclamaciones por parte de las personas afectadas y adoptando medidas adecuadas para evitar cualquier anomalía o incidencia futura que pueda producirse.

No obstante, advertir al reclamado que para el caso de que se produzca algún otro incidente de seguridad que pueda suponer un riesgo para los derechos y libertades de las personas físicas su obligación de notificarlo a la autoridad de control así como a los posibles afectados por el incidente sin dilaciones indebidas una vez tenido el conocimiento de ello.

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 al AYUNTAMIENTO DE BAENA, con NIF ***P1400700I***, por una infracción de los artículos 32.1, 33 y 34 del RGPD, tipificados en el artículo 83.4 del RGPD, una sanción de apercibimiento de conformidad con el artículo 77.2 de la LOPDGDD.

SEGUNDO: NOTIFICAR la presente resolución al AYUNTAMIENTO DE BAENA, con NIF ***P1400700I***.

TERCERO: COMUNICAR la presente resolución al Defensor del Pueblo, de conformidad con lo establecido en el artículo 77.5 de la LOPDGDD.

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