- **Expediente N.º: PS/00332/2021**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: En fecha 23 de octubre de 2019, D. ***A.A.A.*** y Dª ***B.B.B.***, en adelante los reclamantes, interpusieron una reclamación ante la Agencia Española de Protección de Datos, contra la EMPRESA MUNICIPAL DE TRANSPORTES DE ******LOCALIDAD.1*** S.A.U., con CIF A46318416 (en adelante, el reclamado), en relación con una presunta vulneración del artículo 32 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (en adelante, RGPD).

En su escrito de reclamación, los reclamantes (miembros del Consejo de Administración de la Empresa Municipal de Transportes de ******LOCALIDAD.1***), manifestaban que en fecha 27 de septiembre de 2019, en una sesión extraordinaria, se les informó de un presunto fraude de más de 4 millones de euros, por una presunta suplantación de identidad del personal directivo de la empresa, con órdenes de pago, lo que suponía una grave brecha de seguridad.

Desconociendo si se había puesto en conocimiento de esta Agencia, según lo dispuesto en el RGPD, en fecha 15 noviembre de 2019, los reclamantes remitieron escrito ante la negativa de la Empresa Municipal de Transportes de ******LOCALIDAD.1*** a informar a esta Agencia y al Centro Criptológico Nacional sobre la brecha de seguridad ocurrida en septiembre de 2019, solicitando que se inicie el pertinente expediente sancionador.

SEGUNDO: En fecha 29 de noviembre de 2019, los reclamantes remiten nuevo escrito en el que amplían el objeto de la denuncia al constatarse en las auditorías realizadas a la Empresa Municipal de Transportes de ******LOCALIDAD.1***, el incumplimiento del RGPD, solicitando se investigue el mismo. Entre la documentación aportada se encuentra el Plan de Acción de Ciberseguridad, el documento del Plan de seguridad de la reclamada, documentos del servicio de auditoría y consultoría para la implantación del RGPD elaborado por una firma auditora para la reclamada y el dictamen pericial elaborado por Telefónica que ya fue aportado por la reclamada.

TERCERO: De conformidad con el artículo 65.4 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (en adelante LOPDGDD), se dio traslado de dicha reclamación al reclamado, para que procediese a su análisis e informase a esta Agencia en el plazo de un mes, de las acciones llevadas a cabo para adecuarse a los requisitos previstos en la normativa de protección de datos.

Consta en esta Agencia contestación al traslado de la reclamación, mediante escritos de fecha de 21 y 24 de febrero de 2020.

CUARTO: En fecha 1 de junio de 2020, tras analizarse la documentación que obraba en el expediente, se dictó resolución por la Directora de la AEPD, acordando el archivo de la reclamación. La resolución fue notificada a los reclamantes, en fecha 3 de junio de 2020, según confirmación de la recepción que figura en el expediente.

QUINTO: En fecha 2 de julio de 2020, los reclamantes interponen un recurso potestativo de reposición a través del Registro Electrónico de la AEPD, contra la resolución recaída en el expediente E/11294/2019, en el que muestran su disconformidad con la resolución impugnada, exponiendo que la resolución no se corresponde con los hechos denunciados y que han sido resueltas a la vez tres reclamaciones distintas. Desconocen además si la brecha de seguridad fue comunicada a esta Agencia y que no se ha resuelto sobre la falta de adaptación al RGPD. Asimismo, constatan que no se adjuntó la totalidad del expediente en el traslado de la reclamación a la reclamada faltando la documentación remitida el 15 y 29 de noviembre de 2019 y solicitan se declare la nulidad de la resolución y se acuerde investigar los hechos denunciados.

SEXTO: En fecha 12 de febrero de 2021, los reclamantes presentan nuevo escrito de ampliación del recurso al que adjuntan dos documentos:

- Memoria de actividades del ejercicio 2019 de la agencia de prevención y lucha contra el fraude y la corrupción de la Comunidad ******LOCALIDAD.1*** de 30 de marzo de 2020.

- Informe de auditoría de seguridad de la Empresa Municipal de Transportes de ******LOCALIDAD.1*** SAU, del ejercicio 2020, en los que manifiesta el reclamante que queda patente el no cumplimiento por parte del reclamado de lo establecido por la normativa de protección de datos personales y de su adaptación al RGPD.

SÉPTIMO: En fecha 26 de febrero de 2021, la Directora de la Agencia Española de Protección de Datos resuelve estimar el recurso de reposición interpuesto y acuerda la admisión a trámite de la reclamación presentada contra EMPRESA MUNICIPAL DE TRANSPORTES DE ******LOCALIDAD.1*** S.A.U.

OCTAVO: A la vista de los hechos notificados y de los documentos aportados, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos descritos en los apartados anteriores, 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), teniendo conocimiento de los siguientes extremos:

Respecto a la brecha de seguridad de datos personales

En el escrito de respuesta del denunciado en el marco de las actuaciones de referencia E/11294/2019, manifiestan lo siguiente:

(…).

Respecto de las causas que hicieron posible la brecha:

(…).

Datos afectados:

(…).

Comunicación a los afectados:

(…).

Respecto de la notificación con posterioridad a las 72 horas.

(…).

Respecto de las medidas de seguridad implantadas

(…).

El representante de la EMT aporta copia del documento denominado "*Reunión de seguimiento grado cumplimiento ciberseguridad*" elaborado por ***XX*** en ******FECHA.1***.

En el documento consta que se han completado las siguientes tareas:

(…).

En el documento consta que se han realizado los siguientes trabajos:

- ***(…).***

- El representante de la EMT aporta copia del documento *"Reunión de seguimiento grado cumplimiento en Protección de Datos y Ciberseguridad. Servicio de asesoría y consultoría para la implantación del Reglamento General de Protección de Datos (RGPD) y esquema Nacional de Seguridad (ENS) para EMT* ******LOCALIDAD.1*** *Exp. –* ******EXP.1*****.** ******FECHA.2***", en el que se especifica la situación actual de adecuación al RGPD de la EMT:

- ***(…).***

- Aportan copia del documento *"*******DOCUMENTO.1, ***LOCALIDAD.1****, SAU"*, elaborado por la Oficina de Auditoria de la Comunidad ******LOCALIDAD.1***, en el que se recoge el informe de la auditoria de ciberseguridad de la Empresa Municipal de Transportes de ******LOCALIDAD.1***, S.A.U., centrada en las áreas de ingresos por transporte de viajeros, contabilidad y tesorería, referida a la situación de los controles *durante 2020*, cuyas conclusiones son:

- ***(…).***

- Aportan evaluación de impacto de los tratamientos "Gestión de títulos personales", "Gestión de títulos no personales", "*Captación de personal*" y "*videovigilancia",* sin fecha, en los que se definen las amenazas y los controles de seguridad basados en los requerimientos del RGPD y el standard ISO 27002.

Aportan copia del documento *"Procedimiento de gestión de incidencias de privacidad y brechas de seguridad de datos personales"*, cuyo objetivo es definir un proceso de

gestión de incidentes de privacidad y brechas de seguridad de datos personales, de conformidad con el RGPD, y en concreto en sus artículos 33 y 34.

(…).

NOVENO: En fecha 1 de septiembre de 2021, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador a la entidad investigada, por la presunta infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

Notificado el acuerdo de inicio, la entidad investigada presentó escrito de alegaciones en el que, en síntesis, manifestaba lo siguiente:

1. Que se encuentra en completa indefensión respecto de los hechos y razones que han fundamentado el acuerdo de inicio del procedimiento sancionador toda vez que no tuvieron conocimiento de la impugnación de archivo de actuaciones, del recurso de reposición presentado, así como del escrito de fecha 12 de febrero de 2021, ni de la Resolución de fecha 26 de febrero de 2021.

2. Los hechos no se producen como consecuencia de un error humano sino por la falta de diligencia e incumplimiento de las medidas existentes en la EMT por parte de la que fuera Directora de Administración de EMT.

3. No se ha producido ningún acceso directo a la información ni a los sistemas de EMT, no tratándose por tanto de ninguna brecha de seguridad.

4. Los datos comunicados fueron exclusivamente los D.N.I. de dos personas, que incluyen sus firmas.

5. Hubo una reacción rápida por parte de EMT y la situación se puso en conocimiento de los interesados de forma inmediata al momento en el que se conocieron los hechos, sin que haya existido ningún perjuicio económico para los interesados.

6. Si bien los datos comunicados hacen a los interesados identificables, fueron usados exclusivamente en su condición de personal de alta dirección de EMT al objeto de eludir las políticas de seguridad en cuanto a disposiciones patrimoniales.

7. EMT en su condición de responsable del tratamiento tiene implementadas las medidas técnicas y organizativas que garantizan el cumplimiento de la normativa en materia de protección de datos, habiendo sido ya aportadas a este procedimiento. Como consta, incluso dichas medidas fueron reforzadas a raíz del conocimiento de los hechos

8. De haberse dado alguna conducta sancionable, dicha sanción, de conformidad con el artículo 77.1 c) de la LO 3/2018 de 5 de diciembre de Protección de Datos y Garantía de los Derechos Digitales, en relación con el apartado segundo del mismo artículo debería consistir en un apercibimiento.

9. Se aporta documentación relativa al Registro de Actividades del Tratamiento y Análisis de Riesgos sobre los mismos.

DÉCIMO: En fecha 11 de octubre de 2021 se formuló propuesta de resolución, proponiendo:

<< Que por la Directora de la Agencia Española de Protección de Datos se dirija un apercibimiento a EMPRESA MUNICIPAL DE TRANSPORTES DE ******LOCALIDAD.1*** S.A.U., con NIF A46318416, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.>>

UNDÉCIMO: En fecha 27 de octubre de 2021, la entidad investigada presenta escrito de alegaciones a la Propuesta de Resolución, en el que, en síntesis, manifiesta que se ha vulnerado su derecho de defensa, toda vez que no tuvieron conocimiento del recurso potestativo de reposición, ni de la ampliación del citado recurso ni de su resolución, muestra su disconformidad con la supuesta vulneración del artículo 32 del RGPD, expone que los hechos no se produjeron como consecuencia de un error humano sino por la falta de diligencia e incumplimiento de las medidas existentes por parte de la que fue Directora de administración, que hubo una rápida reacción y la situación se puso en conocimiento de los interesados de forma inmediata, que no existió culpa suficiente en los hechos previstos en el presente procedimiento y solicita la anulación del procedimiento.

A la vista de todo lo actuado, por parte de la Agencia Española de Protección de Datos en el presente procedimiento se consideran hechos probados los siguientes,

HECHOS

PRIMERO: En fecha 23 de octubre de 2019, los reclamantes, interpusieron una reclamación ante la Agencia Española de Protección de Datos, contra la EMPRESA MUNICIPAL DE TRANSPORTES DE ******LOCALIDAD.1*** S.A.U., con CIF A46318416, en relación con una presunta vulneración del artículo 32 del Reglamento (UE) 2016/679, de 27 de abril de 2016 (en adelante, RGPD).

SEGUNDO: A la vista de los hechos notificados y de los documentos aportados, la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos, 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), teniendo conocimiento de las deficiencias previas en las medidas de seguridad, técnicas y organizativas, existentes antes del ataque tipo *phishing.* (hechos investigados por el Juzgado de Instrucción número 18 de València, en las Diligencias Previas 1764/2019).

TERCERO: En la actualidad la entidad investigada ha aportado documentación que acredita la implantación progresiva de las medidas de seguridad, técnicas y organizativas, necesarias para evitar hechos similares en el futuro. La documentación aportada se encuentra incorporada al expediente.

FUNDAMENTOS DE DERECHO

PRIMERO: En virtud de los poderes que el artículo 58.2 del RGPD reconoce a cada autoridad de control, y según lo establecido en los arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

SEGUNDO: Antes de entrar en el fondo del asunto, se ha de solventar la cuestión formal planteada por la entidad investigada en su escrito de alegaciones.

Alega la entidad investigada que se encuentra en completa indefensión respecto de los hechos y razones que han fundamentado la apertura del presente procedimiento sancionador, toda vez que no tuvieron conocimiento de la impugnación del archivo de actuaciones, esto es, del recurso de reposición presentado, del escrito de ampliación del citado recurso de fecha 12 de febrero de 2021 y de su correspondiente resolución de fecha 26 de febrero de 2021, a fin de alegar lo que hubiera tenido por conveniente.

En primer lugar, como señala la reiterada jurisprudencia del Tribunal Supremo (por todas, Sentencias del Tribunal Supremo de 17 de octubre de 1991 y 21 de octubre de 1980) y la doctrina del Consejo de Estado (Dictámenes 6.175/1997, de 19 de febrero de 1998; 1/1998, de 21 de mayo; 3.170/1998, de 30 de julio, y 2.301/1998, de 10 de septiembre, entre otros muchos), la mera omisión de un trámite, aunque fuera preceptivo, no constituye necesariamente por sí solo un vicio de nulidad de pleno derecho.

Ni siquiera la simple omisión del trámite de audiencia da lugar, "siempre y de forma automática", a la nulidad por esta causa; a este respecto el Tribunal Supremo, en Sentencia de 17 de octubre de 1991, exigió *"ponderar, en cada caso, las consecuencias producidas por tal omisión a la parte interesada, la falta de defensa que realmente haya originado y, sobre todo, lo que hubiera podido variar el acto administrativo originario en caso de haberse observado el trámite omitido*".

Así se ha pronunciado el Consejo de Estado en sus Dictámenes 6.175/1997, de 19 de febrero de 1998, 1/1998, de 21 de mayo, 1.949/2000, de 22 de junio, 2.132/2000, de 20 de julio, 612/2001, de 5 de abril, y 1.224/2001, de 7 de junio, entre otros. En determinadas circunstancias, cuando un examen detenido del expediente permita excluir que la omisión del trámite de audiencia haya causado indefensión a los interesados, tal omisión puede no dar lugar a un vicio de nulidad de pleno derecho.

En este sentido, el Tribunal Constitucional, en la Sentencia 144/1996, de 16 de septiembre, afirma que "*en un procedimiento administrativo lo verdaderamente decisivo es si el sujeto ha podido alegar y probar lo que estimase por conveniente en los aspectos esenciales del conflicto en el que se encuentra inmerso".*

Como advierte la Sentencia del Tribunal Supremo de 27 de febrero de 1993, "*No cabe alegar la nulidad del acto porque la falta de notificación, aun cuando hubiera existido no afecta a la validez de la decisión no comunicada, sino exclusivamente a su eficacia respecto del concreto destinatario de la diligencia de notificación y ello a condición, por cierto, de que de la omisión o defectos formales al practicarla se hubiera seguido una efectiva indefensión para el mismo; como tampoco sería nulo el acto, conforme a aquel otro artículo invocado, cuando se prescinde en absoluto totalmente, del procedimiento establecido para adoptar la decisión; no para notificarla"'.*

Así, la notificación constituye un requisito de eficacia de los actos administrativos y no de validez, por lo que carece de fundamento propugnar la invalidez de los actos administrativos por defectos de notificación de aquellos (Por todos, los Dictámenes de este Consejo Consultivo 429/2014, de 18 de septiembre, o 251/2018, de 11 de julio).

En el caso concreto que se examina, consta que se ha producido la apertura de un procedimiento sancionador, sin que se haya dado trámite de audiencia a la entidad investigada, al no haberle dado traslado del recurso de reposición interpuesto, a fin de alegar lo que hubiera tenido por conveniente, conforme determina el artículo 118 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en lo sucesivo LPACAP), que señala lo siguiente:

"Artículo 118. Audiencia de los interesados.

1. Cuando hayan de tenerse en cuenta nuevos hechos o documentos no recogidos en el expediente originario, se pondrán de manifiesto a los interesados para que, en un plazo no inferior a diez días ni superior a quince, formulen las alegaciones y presenten los documentos y justificantes que estimen procedentes.

No se tendrán en cuenta en la resolución de los recursos, hechos, documentos o alegaciones del recurrente, cuando habiendo podido aportarlos en el trámite de alegaciones no lo haya hecho. Tampoco podrá solicitarse la práctica de pruebas cuando su falta de realización en el procedimiento en el que se dictó la resolución recurrida fuera imputable al interesado.

2. Si hubiera otros interesados se les dará, en todo caso, traslado del recurso para que, en el plazo antes citado, aleguen cuanto estimen procedente.

3. El recurso, los informes y las propuestas no tienen el carácter de documentos nuevos a los efectos de este artículo. Tampoco lo tendrán los que los interesados hayan aportado al expediente antes de recaer la resolución impugnada."

A la vista de las actuaciones obrantes en el expediente, se llega a la conclusión de que en el caso que se examina, la entidad investigada no recibió el traslado del recurso de reposición interpuesto, privándosele de la posibilidad de formular alegaciones, y habida cuenta que tal dato es esencial en orden a la defensa del interesado, procede, de conformidad con lo dispuesto en el artículo 119 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, anular las actuaciones practicadas y reponerlas al momento en que se produjo el defecto procedimental; no obstante, teniendo en cuenta que la presunta infracción estaría prescrita desde los dos años de su presunta comisión, dado que el procedimiento sancionador en este caso no ha interrumpido el plazo de prescripción, procede archivar el presente procedimiento, ello en aras del cumplimiento de los principios de eficacia, racionalización y agilidad de los procedimientos administrativos, de acuerdo con el artículo 3 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público.

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: ARCHIVAR el procedimiento sancionador PS/00332/2021 instruido a la EMPRESA MUNICIPAL DE TRANSPORTES DE ******LOCALIDAD.1*** S.A.U., con CIF A46318416, por una infracción del artículo 32 del RGPD, tipificada en el artículo 83.4 del RGPD.

SEGUNDO: NOTIFICAR la presente resolución a EMPRESA MUNICIPAL DE TRANSPORTES DE ******LOCALIDAD.1*** S.A.U.

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.

938-171221

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