- **Procedimiento Nº: E/03876/2021**

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos y teniendo como base los siguientes

HECHOS

PRIMERO: La reclamación interpuesta por ***A.A.A.*** con NIF ******NIF.1*** (en adelante, el reclamante) tiene entrada con fecha 03/01/2021 en la Agencia Española de Protección de Datos (en adelante, AEPD). La reclamación se dirige contra **CONSORCIO REGIONAL DE TRANSPORTES,** con CIF Q7850003J (en adelante, el reclamado). Los motivos en que basa la reclamación son:
-que ha recibido un correo electrónico publicitario del Club de Amigos del Transporte Público del Consorcio Regional de Transportes de la Comunidad de Madrid, existiendo previamente dos denegaciones explicitas del consentimiento para el envío de comunicaciones comerciales. El alta en el Club de Amigos se realizaba a través de la web en el momento de solicitar una nueva tarjeta de transporte público. No obstante, el denunciante marcó la casilla correspondiente con NO.

Junto a la reclamación aporta:
-copia del correo mencionado, impresiones de pantalla con la solicitud de tarjeta de transporte público, donde consta sin marcar la solicitud de consentimiento para la pertenencia al Club de Amigos del Transporte Público de Madrid, de fecha 28 de septiembre de 2014.
-con fecha 4 de enero de 2021, certificado de Adigital, de 1 de septiembre de 2020, donde constan datos del denunciante en la Lista Robinson, entre ellos tres direcciones de correo electrónico, una de las cuales corresponde con la dirección de mail donde se le ha remitido la comunicación publicitaria del reclamado, incluida en la mencionada lista el 07/11/2019.

SEGUNDO: 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), con número de referencia RR/00119/2021, se dio traslado de dicha reclamación al reclamado, para que procediese a su análisis e informase a esta AEPD 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.

TERCERO**:** Con fecha 11 de febrero de 2021, se remitió al interesado resolución en el que se inadmite la reclamación por considerar que los hechos habían prescrito.
Con fecha 4 de marzo de 2021, el denunciante presenta Recurso de Reposición en el que alega error por parte de la AEPD al realizar el computo de 6 meses transcurridos entre la recepción del correo electrónico por parte del reclamante, y la presentación de su reclamación ante la AEPD.
En fecha 7 de abril de 2021, se estima el recurso de reposición del reclamante y se procede a la apertura de E/03876/2021.

CUARTO: La Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el esclarecimiento de los hechos objeto de la reclamación, teniendo conocimiento de los siguientes extremos:

ENTIDAD INVESTIGADA:

Durante las presentes actuaciones se ha investigado la siguiente entidad: **CONSORCIO REGIONAL DE TRANSPORTES** con CIF Q7850003J con domicilio en PLAZA DESCUBRIDOR DIEGO DE ORDÁS, N.º 3 - 28003 MADRID (MADRID)

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN:

1.- Con fecha ******FECHA.1*** consta una notificación de brecha del Consorcio Regional de Transporte de Madrid.

2.- Con fecha 13 de abril de 2021 se solicitó información al **CONSORCIO REGIONAL DE TRANSPORTES** (en adelante Consorcio). De la respuesta recibida se desprende lo siguiente:

Respecto de la cronología de los hechos:

Acciones tomadas con objeto de minimizar los efectos adversos y medidas adoptadas para su resolución final

- El 04/08/2020 se recibió en la cuenta habilitada por el Consorcio para atender las cuestiones relacionadas con la protección de datos (******EMAIL.1***), un correo electrónico por medio del cual el reclamante informó que había recibido una comunicación en su dirección de correo electrónico, remitida por el Club de Amigos ******EMAIL.2***, en la que informaba que no había manifestado su voluntad de pertenecer a dicho Club y, en consecuencia, no había dado su consentimiento para que sus datos fuesen objeto de tratamiento en la actividad “Promoción del Transporte Público en la Comunidad de Madrid”

El Consorcio manifiesta que el 06/08/2020 el DPD de este Organismo remitió al afectado un mensaje de correo electrónico, facilitando toda la información que se detalla en el artículo 34.2 del RGPD sobre la violación de la seguridad de los datos personales que se había producido, y se comunicaba que se había atendido a su solicitud de ser dado de baja del Club de Amigos y se había procedido a suprimir sus datos personales de la actividad de tratamiento “Promoción del Transporte Público en la Comunidad de Madrid”

- El ******FECHA.1***, El Consorcio notificó a la AEPD la brecha de seguridad y se ordenó el cese inmediato del envío de mailing a todos los integrantes del Club de Amigos del Transporte Público. Esta medida fue adoptada para evitar que continuasen produciéndose recepción de comunicaciones no deseadas, por quienes no habían manifestado su voluntad de pertenecer al Club de Amigos.

- El 14 de noviembre de 2020 finalizó el contrato para la gestión del Club de Amigos y todas las operaciones de tratamiento asociadas al mismo. El Consorcio ha aportado copia del contrato suscrito para la “Gestión del club de amigos del consorcio regional de transportes públicos regulares de Madrid”

Respecto de las causas que hicieron posible la brecha:

• Con motivo de la actualización masiva de títulos de transporte (tarjetas) que tuvo lugar a finales del 2017 y principios del 2018, pasando de una duración de 7 años a 10 años, se ejecutó de forma automática en todos los puntos oficiales de carga/recarga de la red del Consorcio mediante un software que no existía previamente, encargado por el Consorcio a sus redes de venta. Este software cumplimentó, por defecto, de forma automática y en sentido afirmativo, el campo en el que se recogía la manifestación de los usuarios relativa a su deseo de pertenecer, o no, al Club de Amigos del Transporte Público. La pertenencia al Club implica el tratamiento de datos en la actividad denominada "Promoción del Transporte Público en la Comunidad de Madrid". No obstante, la causa fue debido a que el tratamiento mencionado se obtuvo de la base de datos correspondiente a la “Gestión de las Tarjetas de Transporte Público”.

Respecto de los datos afectados:

• El Consorcio manifiesta que no se puede precisar el número de afectados, ya que la única información al respecto es un flag, en el que se indica si el usuario tiene o no pertenencia al Club, pero no se mantiene un histórico de los estados anteriores. Las personas que tenían asociado la pertenencia al club (flag) también tenían que haber proporcionado una dirección de correo electrónico para el envío de mail del Club de amigos. El proceso de modificación afectó a todos los usuarios que actualizaron sus tarjetas, pero el Consorcio solo tiene datos personales de las tarjetas, y dentro de este grupo, solo podía afectar a los que tuviesen email. Por lo tanto, esta situación pudo afectar potencialmente a 372.294 (cuentas de correo de usuarios teóricas, ya que muchos correos pueden no ser correctos). Además de esto, no se sabe cuántos de ellos anteriormente eran miembros del Club y cuantos no.

• La consecuencia para los afectados es que sus datos hayan sido tratados por la empresa adjudicataria del contrato para la gestión del Club de Amigos, sin que hubieran prestado consentimiento para ello. Este tratamiento concreto, realizado por el encargado del tratamiento, se limita al envío a través de correo electrónico, de información acerca de ofertas comerciales que supongan beneficios o descuentos en productos o servicios. De manera que el efecto más apreciable ha sido la recepción de mensajes de correo no deseados.

• Para la pertenencia al Club de Amigos, es el interesado quien consigna, directamente, los datos personales requeridos en la inscripción a las promociones o concursos concretos en los que desee participar. El Consorcio manifiesta que nunca se comunican a las entidades colaboradoras del Club de Amigos, ni a otros terceros, los datos de las personas que no han manifestado interés por las ofertas. La tipología de datos que se han cedido a terceros (a los cuales ha accedido el encargado del tratamiento) son las direcciones de correo electrónico de los afectados.

• En relación con estos hechos solo se ha recibido la reclamación del denunciante.

Para la baja en el Club de amigos se disponía de enlace: ******URL.1***

• El Consorcio manifiesta que no han realizado la comunicación a los afectados, aunque ya se había elaborado el escrito de comunicación, debido a que mientras se estaban llevando a cabo actuaciones para identificar a todas aquellas personas a las que se ha incluido en el Club de Amigos del Transporte Público, sin recabar el pertinente consentimiento, se advirtió que el contrato se encontraba próxima a expirar

(14 de noviembre de 2020) y, por consiguiente, finalizaría también en esta fecha el tratamiento de datos personales, tanto de los afectados como del resto. Teniendo en cuenta que ya se había dado instrucciones al encargado del tratamiento, para que, de manera inmediata, cesase de enviar comunicaciones a los integrantes del Club de Amigos, el Consorcio consideró que se había cumplido la condición reflejada en el artículo 34.3.a) del RGPD y, en consecuencia, ya no resultaba preciso efectuar la comunicación a los afectados.

A este respecto han aportado copia del documento elaborado para comunicar a los afectados.

Respecto de las medidas de seguridad implantadas:

• El Consorcio manifiesta que este incidente no es una brecha se seguridad, a efectos informáticos, ya que la causa del tratamiento de datos sin consentimiento por parte de la empresa adjudicataria del contrato y envío de mails ha sido la inicialización de un campo

• En todo caso el Consorcio manifiesta que dispone de medidas de seguridad, entre otras, protocolos de intercambio mediante certificados digitales, que envían mediante un canal seguro, ficheros firmados por las Redes de Venta, además, cada registro de estos ficheros (transacciones), a su vez están firmadas digitalmente por un elemento de seguridad del Consorcio.

• Aparte de estas medidas técnicas, y antes de la detección de la brecha, concretamente el 29 de junio de 2020, se ordenó adoptar la medida organizativa propuesta por el Delegado de Protección de Datos del Organismo, consistente en “Eliminar la posibilidad de apuntarse al Club de Amigos, a través de la solicitud de obtención de la Tarjeta de Transporte Público”. No obstante, esta medida no se extendió a las manifestaciones de la voluntad de incorporarse al Club de Amigos, incorporadas a las solicitudes de la tarjeta de transporte público, que se habían efectuado con anterioridad.

• El ******FECHA.1*** y como medida de mitigación de los efectos negativos sobre los afectados se ordenó el cese del envío de mailing a los integrantes del Club de Amigos y el 14 de noviembre de 2020, finalizó el tratamiento de los datos personales correspondiente a la actividad “Promoción del Transporte Público en la Comunidad de Madrid” Asimismo, se ha incorporado al acervo la conciencia de que es un error grave que los datos que son objeto de tratamiento en una actividad concreta provengan de la base de datos correspondiente a otra actividad de tratamiento distinta.

Respecto de la notificación con posterioridad a las 72 horas:

• Tal y como se ha indicado en la notificación de la brecha de seguridad, con número de registro 028342/2020, efectuada el ******FECHA.1*** a las 13:34:13 horas, la detección de la brecha de seguridad se verificó el 04/08/2020, concretamente a las 17:31 horas, a través del mensaje de correo del denunciante dirigido a la cuenta habilitada, por el Consorcio, el cual informó de la incidencia. Como puede comprobarse, entre las 17:31 horas del 4 de agosto y las 13:34 horas del 7 de agosto de 2020, no ha transcurrido el plazo de 72 horas, en el que, de conformidad con lo previsto en el artículo 33.1 del RGPD, debe notificarse.

Información sobre la recurrencia de estos hechos y número de eventos análogos acontecidos en el tiempo:

- No ha habido recurrencia de estos hechos, ni se han producido eventos análogos

FUNDAMENTOS DE DERECHO

I

De acuerdo con los poderes de investigación y correctivos que el artículo 58 del Reglamento (UE) 2016/679 (Reglamento general de protección de datos, en adelante RGPD) otorga a cada autoridad de control, y según lo dispuesto en el artículo 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), es competente para resolver estas actuaciones de investigación la Directora de la Agencia Española de Protección de Datos.

II

El artículo 4 apartado 12 del RGPD define, de un modo amplio, las "violaciones de seguridad de los datos personales" (en adelante quiebra de seguridad) 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.*"

Hay que señalar, que la notificación de una quiebra de seguridad no implica la imposición de una sanción de forma directa, ya que es necesario analizar la diligencia de responsables y encargados y las medidas de seguridad aplicadas.

La seguridad de los datos personales viene regulada en los artículos 32 y 33 del RGPD:

Artículo 32

"Seguridad del tratamiento

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".

Artículo 33

"Notificación de una violación de la seguridad de los datos personales a la autoridad de control

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".

En el presente caso, consta una brecha de seguridad de datos personales en las circunstancias arriba indicadas, categorizada como una brecha de confidencialidad, al haber tenido acceso a datos personales una empresa externa, encargada del contrato para la promoción publicitaria, sin consentimiento expreso del reclamante.

Tras el requerimiento de información llevado a cabo por la Inspección de esta AEPD, el reclamado ha informado de todas las actuaciones llevadas a cabo para paliar el incidente, entre ellas, eliminar la posibilidad de apuntarse al Club de Amigos, a través de la solicitud de obtención de la Tarjeta de Transporte Público.

Hay que destacar la rapidez de respuesta del Consorcio, ya que inmediatamente, tras recibir una queja por parte del reclamante, ordenó el cese inmediato del envío de mailing a todos los integrantes del Club de Amigos del Transporte Público.

No constan ante esta AEPD reclamaciones de posibles afectados, salvo la que ha dado origen al presente expediente.

III

Se ha acreditado, pues, que la actuación del reclamado como entidad responsable del tratamiento, ha sido acorde con la normativa sobre protección de datos personales analizada en los párrafos anteriores.

Por lo tanto, de acuerdo con lo señalado, por la Directora de la Agencia Española de Protección de Datos, SE ACUERDA:

PRIMERO: PROCEDER AL ARCHIVO de las presentes actuaciones.

SEGUNDO: NOTIFICAR la presente resolución al reclamante, ***A.A.A.,*** con NIF ******NIF.1*** y al reclamado, **CONSORCIO REGIONAL DE TRANSPORTES,** con CIF Q7850003J.

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 según lo preceptuado por el art. 114.1.c) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y de conformidad con lo establecido en los arts. 112 y 123 de la citada Ley 39/2015, de 1 de octubre, los interesados podrán interponer, potestativamente, recurso de reposición ante la 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.

940-0419

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