- **Procedimiento Nº: PS/00425/2020**

RESOLUCIÓN DE PROCEDIMIENTO SANCIONADOR

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

ANTECEDENTES

PRIMERO: Con fecha de 17 de febrero de 2020 la directora de la Agencia Española de Protección de Datos (en adelante AEPD) acuerda iniciar actuaciones de investigación en relación con una brecha de seguridad de datos personales notificada por el AYUNTAMIENTO DE MADRID en fecha 12 de febrero de 2020 y número de registro de entrada de la AEPD 006633/2020 (en adelante referenciado como E/01657/2020), relativa al acceso no autorizado a justificantes de autorizaciones como personas residentes del servicio de estacionamiento regulado de vehículos de Madrid.

Junto a dicha notificación de brecha de seguridad se aportó:

- Documento complementario de resumen de la brecha de seguridad acontecida.

- Notificación interna del Ayuntamiento de Madrid de vulnerabilidad de seguridad, firmada por el señor Director General de Sostenibilidad y Control Ambiental del ayuntamiento en fecha 10 de febrero de 2020, dirigida a la Dirección General de Transparencia (Subdirección General de Protección de Datos) del organismo y referida en detalles al incidente en cuestión.

- Captura de pantalla sobre la indisponibilidad de la Sede Electrónica de la AEPD a las 18:23 horas del 11 de febrero de 2020 para la notificación de la presente brecha de seguridad.

SEGUNDO: Con fecha de 4 de marzo de 2020 la directora de la Agencia Española de Protección de Datos (en adelante AEPD) acuerda iniciar actuaciones de investigación en relación con una brecha de seguridad de datos personales notificada por el AYUNTAMIENTO DE MADRID en fecha 27 de febrero de 2020 y número de registro de entrada de la AEPD 009711/2020 (en adelante referenciado como E/01997/2020), relativa a la comunicación por un ciudadano a través de correo electrónico sobre una reclamación que había interpuesto en el Ayuntamiento en el año 2015 y que aparece publicada en Internet haciendo una búsqueda a través de Google.

El Ayuntamiento manifiesta que se había producido modificaciones en el Sistema de Información de Sugerencias y Reclamaciones (SyR) para el envío de las contestaciones a las SyR presentadas en el Ayuntamiento. Entre estas modificaciones estaba que en el enlace que reciben los ciudadanos para acceder a su contestación se requeriría una identificación con dos campos de validación. Este nuevo sistema se puso en marcha en agosto de 2019.

El Ayuntamiento conocedor de que algunos usuarios habían publicado en redes sociales el enlace facilitado y a raíz de la comunicación del ciudadano se procedió desde el Organismo Autónomo Informática Ayuntamiento de Madrid (IAM) a la eliminación de

toda indexación de páginas en cualquier buscador de internet, actuando prioritariamente sobre Google. Esta solución funciona correctamente para todas la SyR respondidas desde agosto de 2019.

Respecto de las búsquedas realizadas a través de otros buscadores diferentes a Google, IAM ha actuado para que no se muestre ningún enlace de respuesta que el usuario haya decidido publicar en cualquier página de internet, como foros, blogs, etc. Esta actuación a través del fichero robot.txt afecta a todos los buscadores.

TERCERO: A la vista de los hechos notificados y de los documentos aportados por el Ayuntamiento, 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:

ENTIDADES INVESTIGADAS

AYUNTAMIENTO DE MADRID (en adelante la investigada), Dirección General de Transparencia, con NIF P2807900B y domicilio en C/ Alcalá 45, 28014 Madrid.

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN. E/01657/2020

Fecha de notificación de la brecha de seguridad en la AEPD: 12/02/2020

ANTECEDENTES

Las actuaciones de investigación han sido llevadas a cabo mediante el envío de requerimiento de información desde la AEPD y contestación al mismo por parte de la investigada conforme a la siguiente secuencia temporal:

1. Solicitud de información a la investigada, en fecha 24 de febrero de 2020 y número de registro de salida de la AEPD 017919/2020.

2. Respuesta de la investigada, en fecha 22 de julio de 2020 y número de registro de entrada de la AEPD 025844/2020.

(Se hace notar que el Expediente de Investigación asociado (E/01657/2020) se ha visto afectado, en términos de plazos administrativos, por lo dispuesto en el Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma)

Analizando los términos que componen la citada respuesta de la investigada, se desprende:

i. Respecto a los hechos:

- La investigada informa de que su Subdirección General de Arquitectura y Seguridad de Informática comunicó el 7 de febrero de 2020 por correo electrónico a la Dirección General de Sostenibilidad y Control Ambiental, responsable del servicio de estacionamiento regulado de vehículos de Madrid (en adelante SER), la información recibida el 6 de febrero de 2020 desde el Instituto Nacional de Ciberseguridad (en adelante INCIBE) referida a un posible incidente de seguridad con afectación al sitio web:

  https://movilidad.madmovilidad.es

  El incidente, que a su vez había sido reportado por un usuario al INCIBE, consistía en la posibilidad de acceder a justificantes de autorizaciones de terceros residentes del SER, en los que constaba el nombre, apellidos y DNI de la persona autorizada, así como matrícula del vehículo, a través de la URL:

  https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imprimirJustificantePeriodo.pdf?idPeriodo=2046824&tipoAutorizacion=1

- La investigada expone que la vulnerabilidad detectada fue confirmada el mismo 7 de febrero de 2020 y estaba referida a la impresión de justificantes que se emiten para que los usuarios tengan una evidencia de su autorización de residente en el SER. El incidente radicaba en que la numeración de la URL era consecutiva, por lo que el cambio secuencial de un dígito permitía el acceso a datos personales de terceros.

- La investigada identifica la implicación de cuatro encargados del tratamiento en la actividad de tratamiento que sufrió la brecha de seguridad que se corresponden con las empresas concesionarias que prestan el servicio de gestión del SER en régimen de concesión indirecta:

  Empresa 1: ******EMPRESA.1***

  Empresa 2: ******EMPRESA.2***

  Empresa 3: ******EMPRESA.3***

  Empresa 4: ******EMPRESA.4***

- Los citados encargados de tratamiento de la investigada sostienen que:

  o El 7 de febrero de 2020 la investigada les trasladó el incidente, como responsable del tratamiento, y que, tras comprobar su existencia, automáticamente y como medida preventiva deshabilitaron la página de trámites del SER, impidiendo el acceso a la página, así como a cualquier información contenida en la misma hasta determinar el origen y alcance del acceso no autorizado.

- Los días 8 y 9 de febrero de 2020 realizaron una auditoría de la aplicación de trámites del SER para determinar y verificar la existencia de otros posibles accesos fraudulentos no reportados.

- El 12 de febrero de 2020 procedieron al despliegue en entornos no productivos de la solución adoptada para la resolución de la incidencia y se la trasladaron a la investigada para que la validase como responsable del tratamiento.

- El 13 de febrero de 2020, tras comprobar la validez de la solución adoptada, desplegaron ésta en el entorno de producción, se validó por parte de la investigada y se habilitó en la página web de trámites del SER.

- La investigada afirma que se revisaron todos los *logs* disponibles de accesos a justificantes desde internet, sin haberse detectado accesos sistemáticos a la información expuesta. La investigada asevera que los accesos no autorizados de los que existe constancia son los realizados por la persona que comunicó la vulnerabilidad al INCIBE, iterando sobre el parámetro "idPeriodo" en la URL indicada:

  https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imprimirJustificantePeriodo.pdf?idPeriodo=2046824&tipoAutorizacion=1

  https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imprimirJustificantePeriodo.pdf?idPeriodo=2046823&tipoAutorizacion=1

  https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imprimirJustificantePeriodo.pdf?idPeriodo=2046822&tipoAutorizacion=1

  https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imprimirJustificantePeriodo.pdf?idPeriodo=2046821&tipoAutorizacion=1

- La investigada reseña que este método que permitía el acceso a la información no habilitaba modificación alguna ni borrado de los datos involucrados en la brecha de seguridad.

- Los encargados del tratamiento de la investigada anteriormente citados manifiestan que:

  - La aplicación web de trámites del SER está basada en una arquitectura MVC (modelo-vista-controlador) en la cual se utiliza *Spring WebFlow* con JSP (páginas de servidor *Java*), en la que todas las peticiones se realizaban mediante el método HTTP POST (procedimiento por el que el navegador envía información al servidor de forma no visible en la URL), excepto la descarga del PDF del justificante de autorización del SER involucrada en la brecha de seguridad, que se realizaba

mediante el método HTTP GET (procedimiento por el que el navegador envía información al servidor de forma visible en la URL).

o El acceso a dicha funcionalidad se producía pulsando un botón del formulario de autorización del SER denominado “Imprimir justificante”, tras lo cual se lanzaba una petición con método HTTP GET al servidor con los siguientes parámetros:

a) “idPeriodo”: identificador con número único de un periodo asociado a una autorización. Este identificador se genera internamente y nunca es mostrado en los formularios al usuario. Dicho identificador debe pertenecer a un periodo activo, ya que si no el justificante no puede ser descargado.

b) “tipoAutorizacion”: dependiendo del tipo de autorización este toma un valor u otro, siendo el valor “1” tipo de autorización de residente.

o Al llegar la petición al servidor, generaba el correspondiente PDF asociado al “idPeriodo”, es decir, contenido como parámetro en la propia petición, y una vez generado el fichero, el servidor devolvía lo oportuno al navegador para que se realizara la descarga en el equipo cliente.

Tratándose de una petición realizada mediante el método HTTP GET, la petición se mostraba visible en la barra de direcciones del navegador web con el siguiente formato:

*https://movilidad.madmovilidad.es/TramitesPortalWeb/app/imprimirJustificantePeriodo.pdf?***idPeriodo***=nnnnn&***tipoAutorizacion***=n*

o Por tanto, en caso de alterarse los señalados parámetros en el enlace de descarga mencionado, accediendo al mismo mediante un navegador, era posible la descarga del PDF de justificantes de autorización del SER para determinado periodo. En todo caso, el nuevo identificador introducido debía existir, esto es, pertenecer a un periodo en estado activo y ser para una autorización del mismo tipo que el indicado en el segundo parámetro “tipoAutorizacion”.

o Aunque se varíe manualmente el identificador existente, esto no implica que el nuevo identificador exista debido a que:

- los periodos, entre otras funcionalidades, pueden darse de baja por los propios usuarios.

- el estado del periodo (que puede ser: en trámite, pendiente de pago, pendiente de notificación, activo, caducado, pendiente de pin,

cancelado, rechazado, enviado a domicilio o modificado), para poder realizar la descarga del PDF de justificantes de autorización del SER, debe ser el de activo en el momento en el que se realizaba la petición de la descarga en cuestión.

- La investigada expresa que el número de registros de datos afectados son cuatro, es decir, exactamente el número de personas afectadas por el incidente, de los que confirma que se produjo acceso por el tercero que lo notificó al INCIBE:
    - Nombre y apellidos.
    - DNI.
    - Matrícula de vehículo.
    - Denominación de la zona del SER a la que corresponde la autorización.
- La investigada sostiene no tener conocimiento de la utilización por terceros de los datos personales obtenidos mediante el acceso no autorizado a datos personales acontecido.
- La investigada alega que la notificación de brecha de seguridad a la AEPD se produjo de manera tardía, el 12 de febrero de 2020, debido a un error en el servidor de la sede electrónica de la AEPD el día 11 de febrero de 2020. La investigada aporta captura de pantalla de dicho error en la fecha señalada a las 18:23 horas.

ii. Respecto a las medidas previas al acontecimiento de la brecha de seguridad:

- Respecto al alojamiento de la aplicación de trámites del SER, los encargados del tratamiento de la investigada manifiestan que se encuentra alojada en un proveedor de servicios externo de tecnologías de la información y de la comunicación (corporación estadounidense: ***(…),*** con sus servicios: *Managed Services*), cuya infraestructura digital consiste en un entorno de nube privada segura, y que dispone de un centro de respaldo en modalidad activo - pasivo. Asimismo, según informan, dicho proveedor tiene implementados y certificados los siguientes estándares:
    - Para los servicios de centro de datos:
        - ISO 27001 - Gestión de la seguridad de la información.

- ISO 22301 - Continuidad del negocio.
- PCI DSS (estándar de seguridad de datos para la industria de tarjeta de pago).
- Informes SOC 1 / SOC2 (control de creación de informes financieros / cumplimiento de seguridad, confidencialidad, integridad, disponibilidad y privacidad).

o Para los servicios gestionados:

- ISO 27001 - Gestión de la seguridad de la información.
- ISO 22301 - Continuidad del negocio.
- ISO 20000–1 - Requisitos de los sistemas de gestión de servicios.

Según los encargados del tratamiento de la investigada, este proveedor de servicios externo de tecnologías de la información y de la comunicación contempla un proceso global de gestión de incidencias sobre actuación, escalada y comunicación a clientes para el caso necesario, incluyendo el aviso a las autoridades correspondientes en función del tipo de incidencia. Además, según su versión, dicho proveedor incluye un plan de contingencia, formación y plan de pruebas de continuidad anual, contemplándose, según determinados resultados, un análisis y un plan de actuación de mejora.

- Respecto a la arquitectura de la aplicación de trámites del SER, los encargados del tratamiento de la investigada exponen que en el acceso a los trámites:

o Alta de autorización de vehículos para residentes:

https://movilidad.madmovilidad.es/TramitesPortalWeb//app/altaResidente-flow?execution=e1s1

o Consulta y gestión de autorizaciones:

https://movilidad.madmovilidad.es/TramitesPortalWeb//app/consulta-flow?execution=e2s1

se genera una cookie en el cliente, denominada “jsessionid”, que guarda un identificador único de sesión que es recuperado en cada petición al servidor. De tal forma que para poder visualizar la información comprometida en este caso, se requiere que en los formularios se completen:

o Alta de autorización de vehículos para residentes:

- Tipo de documento de identificación del titular.
- Número del documento de identificación del titular.
- Matrícula del vehículo.
- Prueba CAPTCHA (Imagen de verificación à Código de verificación).

Según los encargados de tratamiento de la investigada, para poder continuar, la persona deberá figurar como empadronada en la base de datos del padrón de habitantes de la investigada y figurar como titular del vehículo con esa matrícula en la base de datos de la Dirección General de Tráfico del Ministerio del Interior. En ese caso, según dicha versión, el usuario podrá elegir el periodo de duración y realizar el alta de la correspondiente autorización en el SER.

o Consulta y gestión de autorizaciones

- Tipo de documento de identificación del titular.
- Número del documento de identificación del titular.
- Código de la autorización *[sólo conocido por el usuario al realizar el alta / pago de la autorización del SER según defienden]*.
- Matrícula o vado.
- Correo electrónico.
- Confirmación de correo electrónico.
- Prueba CAPTCHA (Imagen de verificación à Código de verificación).

Finalmente, según los encargados de tratamiento de la investigada, además de requerirse datos correctos, se insiste en que todas las peticiones realizadas para navegar y comunicarse entre las diferentes páginas y el servidor se realizan mediante método HTTP POST, a excepción de la funcionalidad relacionada con la impresión del justificante de autorización del SER para un periodo que ha generado la presente brecha de seguridad (realizado por el método HTTP GET).

- La investigada aporta una copia del inventario de actividades de tratamiento (IAT) parcial, en la que se enmarcan los datos personales comprometidos en la brecha de seguridad y con la siguiente información:

  - Actividad de tratamiento: Zonas de estacionamiento regulado.

  - Responsable del tratamiento: Dirección General de Sostenibilidad y Control Ambiental del Ayuntamiento de Madrid, con su dirección postal de contacto completa.

  - Finalidad: Gestión del estacionamiento en la vía pública.

  - Delegado de protección de datos: Dirección General de Transparencia del Ayuntamiento de Madrid.

  - Categoría de personas interesadas: Ciudadanos y residentes, representantes legales, contribuyentes y sujetos obligados, personas de contacto y titulares de vehículos.

  - Datos personales: Identificativos (nombre y apellidos, DNI/NIF, dirección, teléfono y correo electrónico particular), sociales (propiedades y posesiones), información comercial (actividades y negocios), económico-financieros (datos bancarios y de tarjetas de crédito) y otros tipos de datos (vehículos-matrícula).

  - Órganos destinatarios de cesiones: Dirección General de Gestión y Vigilancia de la Circulación (Ordenanza de movilidad para la ciudad de Madrid) y Administración de Justicia y sus órganos de apoyo.

  - Transferencias internacionales de datos: No.

  - Medidas técnicas y organizativas de seguridad: Política de Seguridad de la Información del Ayuntamiento de Madrid y sus Organismos Públicos, aprobada mediante acuerdo de la Junta de Gobierno ANM 2017/36, de 24 de mayo.

  - Legitimación para el tratamiento de los datos: Interés público (asignación del espacio de estacionamiento de vehículos en la vía pública. Impulsar la movilidad sostenible) y consentimiento del afectado.

  - Plazos de conservación de los datos: Los identificativos no se suprimen, se mantienen para consulta en el histórico.

No consta información sobre sus encargados del tratamiento.

- La investigada manifiesta que, en el marco de su proyecto “Verificación del grado de adecuación del Ayuntamiento de Madrid al *Reglamento General de Protección de Datos (RGPD)* y la *Ley Orgánica 3/2018, de Protección de Datos Personales y garantía de los derechos digitales (LOPDGDD)* e implantación de una metodología para la realización de análisis de riesgos y evaluación de impacto de protección de datos”, se ha realizado un análisis preliminar de riesgos de la actividad de tratamiento “Zonas de Estacionamiento Regulado”, cuyo resultado ha obtenido la calificación de la misma como de riesgo escaso.

  En todo caso, la investigada no aporta dicho análisis de riesgos (AR) referido a la citada actividad de tratamiento “Zonas de Estacionamiento Regulado” de su IAT e involucrada en el incidente en cuestión.

- La investigada no aporta, ni motiva dicha ausencia, respecto a posible necesidad y ejecución de evaluación de impacto relativa a la protección de datos (EIPD) referida a la citada actividad de tratamiento “Zonas de Estacionamiento Regulado” de su IAT e involucrada en el incidente en cuestión.

iii. Respecto a las medidas posteriores al acontecimiento de la brecha de seguridad:

*iii.a. De carácter correctivo (reactivas para subsanar la brecha de seguridad):*

- Los encargados del tratamiento de la investigada expresan que la primera medida adoptada el 7 de febrero de 2020 por los técnicos de la aplicación de trámites del SER, tras recibir la notificación de la vulnerabilidad analizada, fue deshabilitar la aplicación impidiendo cualquier acceso tanto a la página como a la información custodiada. Según su relato, todos los accesos a la aplicación desde ese momento eran resueltos con los códigos de error “*HTTP Status 404 -Not Found*” y “*HTTP Status 503 - Service unavailable*” hasta que se implementó la solución definitiva el 13 de febrero de 2020.

- Los encargados del tratamiento de la investigada defienden haber llevado a cabo un análisis del riesgo y el impacto sobre posibles accesos no autorizados a la aplicación web de trámites del SER y concretamente a la funcionalidad de la descarga de justificantes de autorización del SER por periodo.

  Estos encargados del tratamiento de la investigada relatan el citado análisis como sigue:

  - Identificación de amenazas:

    - Aplicación de trámites del SER: función de descarga del PDF del justificante de autorización del SER en un periodo realizada por método HTTP GET.

- Accesos a la aplicación: recopilación y análisis de todas las peticiones realizadas entre el 5 de enero de 2020 y el 7 de febrero de 2020 (fecha del incidente).

o Evaluación de riesgos:

- Aplicación de trámites del SER: no está permitida la modificación ni eliminación de datos personales ante eventual acceso no autorizado a una descarga del PDF de autorización del SER de un tercero. Se requiere conocer la funcionalidad y el formato de la URL a invocar y que existe corresponden entre los parámetros “idPeriodo” y “tipoAutorizacion”, lo cual no es directo en todos los casos (no estricta correlación).

- Accesos a la aplicación: se establece como criterio catalogación de riesgos otorgar puntuaciones de 0 (muy bajo) a 5 (altamente sospechosos), sobre el que se aplicará una depuración y evaluación de accesos.

o Tratamiento de los riesgos:

- Aplicación de trámites del SER: deshabilitar la aplicación web hasta la que incidencia estuviera solucionada, evitando potenciales nuevos accesos no autorizados.

  Realización de desarrollos técnicos en la aplicación en el ámbito del envío de la información (cambio del método HTTP GET) y cifrado de la información mediante un algoritmo.

  Tras verificación de la solución, se determina la inexistencia de estos riesgos y se rehabilitó la aplicación.

- Accesos a la aplicación:

  - Accesos considerados como autorizados: 13.846 accesos de riesgo 0, 37 accesos de riesgo 1 y 36 accesos de riesgo 2.

  - Accesos considerados como no autorizados: 14 accesos de riesgo 3, 0 accesos de riesgo 4 y no constan de riesgo 5. De 12 de los accesos de riesgo 3 se obtienen 4 justificantes de autorización del SER que coinciden con los identificadores notificados por el INCIBE y objeto de esta brecha de seguridad. Los otros 2 accesos de riesgo

3 se corresponden a una misma dirección IP (protocolo de internet), ******IP.1***, posiblemente enmascarada por una VPN (red privada virtual) debido a su geolocalización, y probablemente pertenezca a quien identificó la incidencia.

Se establece que los datos comprometidos corresponden a 4 personas físicas, siendo una de ellas posiblemente la que identificó la propia incidencia. Contemplando el número de accesos y las fechas y horas, se consideran accesos de forma manual, sin la utilización de ataques masivos, iterativos o automatizados.

- Los encargados del tratamiento de la investigada informan de que el método HTTP GET para la impresión de justificantes de autorización del SER fue cambiado por el método HTTP POST, siendo ésta la principal medida técnica con la que se valoró mitigado el riesgo.

  Dichos encargados del tratamiento establecen que esta variación fue implantada, probada y verificada en el entorno de preproducción el 12 de febrero de 2020, sin parámetros legibles ni identificativos posibles de manipular en la URL a nivel de la petición.

  Por último, los encargados del tratamiento de la investigada manifiestan que, no habiendo detectado vulnerabilidades, implantaron la solución al entorno de producción y, posteriormente, lo habilitaron en la aplicación web el 13 de febrero de 2020, de tal forma que, desde ese momento, se recuperó el servicio no pudiendo invocar la impresión de justificantes de autorización del SER por el método HTTP GET.

  En la notificación de brecha de seguridad a esta AEPD y en su documentación adjunta, la investigada señaló expresamente que la brecha de seguridad no entraña un alto riesgo para los derechos y libertades de las personas físicas afectadas y que se trata de un número reducido de éstas, por lo que no ha considerado necesaria la comunicación y no la ha realizado.

*iii.b. De carácter preventivo (proactivas para evitar que se repita la brecha de seguridad):*

- Los encargados del tratamiento de la investigada exponen que, además de la implantación del método HTTP POST para la impresión de justificantes de autorización del SER, el parámetro “idPeriodo” pasa a acompañarse de dos nuevos parámetros: el código de autorización y la ráfaga de pago. Con ello, exponen la existencia de una identificación única de cada justificante generado.

  Dichos encargados del tratamiento sostienen que la correlación entre los tres parámetros establecida es sólo conocida por la aplicación. Añaden que los tres parámetros se combinan en uno, el cual se codifica mediante un cifrado AES (estándar de encriptado avanzado) y una clave almacenada en el servidor y

desconocida en todo momento por los clientes, según su versión. Al llegar la petición de impresión de justificante de autorización del SER al servidor, la cadena se descifra con la misma clave para poder obtenerlo y ofrecérselo al usuario de la aplicación.

CUARTO: Con fecha 30 de noviembre de 2020, la Directora de la Agencia Española de Protección de Datos acordó iniciar procedimiento sancionador al AYUNTAMIENTO DE MADRID, por la presunta infracción de los artículos 32,33,34 y 35 del RGPD en relación con el artículo 5.1.f) del RGPD y por la presunta infracción del artículo 5.1.f) del RGPD.

QUINTO: En fecha 29/12/2020 la investigada presentó alegaciones al acuerdo de inicio manifestando, entre otras, que el acuerdo de inicio adolece de vicio de nulidad de pleno derecho al incoar en un solo expediente dos hechos distintos realizados por diferentes responsables, por lo que solicita el archivo del expediente por falta de responsabilidad del Ayuntamiento de Madrid en las infracciones imputadas.

## HECHOS PROBADOS

PRIMERO: Consta como responsable del tratamiento en el Registro de Actividades de Tratamiento (RAT) de la operación de tratamiento relativa a “Sugerencias y Reclamaciones” (SyR) la Dirección General de Transparencia y Calidad, adscrita al Área de Gobierno de Vicealcaldía, según consta en la estructura orgánica del Ayuntamiento de Madrid.

SEGUNDO: Consta como responsable del tratamiento en el Registro de Actividades de Tratamiento (RAT) de la operación de tratamiento relativa a “Zonas de Estacionamiento Regulado” (ZER) la Dirección General de Sostenibilidad y Control Ambiental, adscrita al Área de Gobierno de Medio Ambiente y Movilidad, según consta en la estructura orgánica del Ayuntamiento de Madrid.

## 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 arts. 47 y 48.1 de la LOPDGDD, la Directora de la Agencia Española de Protección de Datos es competente para resolver este procedimiento.

II

El art´. 89.1.d) de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (LPACAP) señala lo siguiente:

*<Artículo 89. Propuesta de resolución en los procedimientos de carácter sancionador.*

*1. El órgano instructor resolverá la finalización del procedimiento, con archivo de las actuaciones, sin que sea necesaria la formulación de la propuesta de resolución, cuando en la instrucción procedimiento se ponga de manifiesto que concurre alguna de las siguientes circunstancias:*

*d) Cuando no exista o no se haya podido identificar a la persona o personas responsables o bien aparezcan exentos de responsabilidad.>*

El art. 28.1 de la ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público (en lo sucesivo LRJSP) señala lo siguiente:

*< Artículo 28. Responsabilidad.*

*1. Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa>.*

El art 70 de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, señala lo siguiente:

*<Artículo 70. Sujetos responsables.*

*1. Están sujetos al régimen sancionador establecido en el Reglamento (UE) 2016/679 y en la presente ley orgánica:*

*a) Los responsables de los tratamientos.*
*b) Los encargados de los tratamientos.*
*c) Los representantes de los responsables o encargados de los tratamientos no establecidos en el territorio de la Unión Europea.*
*d) Las entidades de certificación.*
*e) Las entidades acreditadas de supervisión de los códigos de conducta.*

*2. No será de aplicación al delegado de protección de datos el régimen sancionador establecido en este Título>.*

Teniendo en cuenta los citados artículos y los hechos probados, en el presente caso, en relación con la alegación (entre otras) arriba indicada relativa a que el acuerdo de inicio adolece de vicio de nulidad de pleno derecho al incoar en un solo expediente dos hechos distintos realizados por diferentes responsables, la misma debe ser aceptada y proceder al archivo del procedimiento sancionador, toda vez que la persona jurídica imputada no se corresponde con el responsable de los tratamientos analizados.

No obstante, se significa que la notificación de las dos violaciones de seguridad (tratamientos SyR y ZER) de conformidad con lo dispuesto en el artículo 33 del RGPD, fueron notificadas a esta AEPD por el Ayuntamiento de Madrid en calidad de "Responsable" de los mismos.

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 presente procedimiento sancionador.

SEGUNDO: NOTIFICAR la presente resolución a AYUNTAMIENTO DE MADRID, con NIF: P2807900B.

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.

938-131120

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