- **Procedimiento Nº: E/01153/2020**

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: Con fecha de 4 de febrero de 2020 la directora de la Agencia Española de Protección de Datos (en adelante AEPD) ordenó iniciar actuaciones de investigación en relación con una brecha de seguridad de datos personales notificada por el Alcalde del AYUNTAMIENTO DE COLMENAR DE OREJA, relativa un posible acceso no autorizado a su centro de procesamiento de datos (en adelante CPD) por parte de un concejal de la Entidad Local y posterior tratamiento de contraseñas de acceso de los usuarios al sistema de información del Ayuntamiento.

Adjunto a dicha notificación de brecha de seguridad se aportó:

- Documento de información alcalde del Ayuntamiento de Colmenar de Oreja respecto a la necesidad de que los usuarios del Ayuntamiento procediesen al cambio de sus contraseñas de acceso a los servicios municipales.

SEGUNDO: 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 notificación, teniendo conocimiento de los siguientes:

ANTECEDENTES

Fecha de notificación de la brecha de seguridad de datos personales: 30/01/2020

ENTIDADES INVESTIGADAS

- AYUNTAMIENTO DE COLMENAR DE OREJA (en adelante el Ayuntamiento), con NIF P2804300H y domicilio en PLAZA MAYOR, 1 - 28380 COLMENAR DE OREJA (MADRID).
- D. ***A.A.A.*** (en adelante el concejal), con NIF ******NIF.1*** y domicilio, como concejal del Ayuntamiento por el partido político VOX ESPAÑA (con NIF G86867108), en ******DIRECCIÓN.1***

RESULTADO DE LAS ACTUACIONES DE INVESTIGACIÓN

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 las personas investigadas conforme a la siguiente secuencia:

1. Solicitud de información al Ayuntamiento, en fecha 11 de febrero de 2020 y número de registro de salida de la AEPD 012247/2020, reiterada en fecha 26 de febrero de 2020 y número de registro de salida de la AEPD 018734/2020.
2. Respuesta del Ayuntamiento, en fecha 2 de marzo de 2020 y número de registro de entrada de la AEPD 010181/2020.

3. Solicitud de información al concejal, en fecha 9 de marzo de 2020 y número de registro de salida de la AEPD 022886/2020.
4. Respuesta del concejal, en fecha 30 de junio de 2020 y número de registro de entrada de la AEPD 022438/2020.

Analizando los términos de las citadas respuestas y de la notificación de la brecha de seguridad, se desprende que:

1. Respecto a los hechos:

- El Ayuntamiento manifiesta que el 2 de diciembre de 2019 el concejal pidió al conserje municipal (D. ***B.B.B.*** con NIF ******NIF.2***) que le abriese la puerta del CPD, yendo el concejal en compañía de terceras personas que, según expone el Ayuntamiento, pertenecían a una empresa no contratada y externa al Ayuntamiento.
- El Ayuntamiento informa de que, una vez dentro del CPD, el concejal y sus acompañantes no identificados realizaron fotografías a los servidores, a las instalaciones y a documentación confidencial.
- El Ayuntamiento expone que entre dicha documentación confidencial fotografiada se encontraban las contraseñas de acceso electrónicas de los concejales de la Entidad Local al sistema del Ayuntamiento.
- El Ayuntamiento defiende que, llegado ese momento, el conserje municipal abandonó el CPD, dejando en el interior al concejal y a sus invitados ajenos al organismo, añadiendo que desconoce otras posibles acciones que pudieran haber realizado.
- El Ayuntamiento cita como testigo presencial de su versión de los hechos al conserje municipal y dice no disponer de los datos de la entidad a la que pertenecían los acompañantes del concejal en su acceso al CPD.
- El Ayuntamiento denota que, tras dicho acceso al CPD, el concejal del PARTIDO DEMOCRÁTICO DE COLMENAR DE OREJA (con NIF desconocido) y los concejales del PARTIDO POPULAR (con NIF G28570927) reportan diferentes incidencias en sus correos electrónicos, en especial falta de éstos. El Ayuntamiento añade no disponer de evidencias respecto de la persona que pudiera haber causado la desaparición de correos electrónicos.
- El Ayuntamiento manifiesta haber detectado la brecha de seguridad el 28 de enero de 2020 mediante comunicación de la secretaria del municipio y confirmación por el conserje municipal.
- El Ayuntamiento señala que los datos que se habrían visto afectados por la brecha de seguridad en cuestión corresponden a:
    - Datos económicos: Ayuntamiento y recaudación de la población.
    - Otros tipos de datos: servicios sociales (almacenados en el servidor).
    - Contraseñas de correos electrónicos de los concejales.
- El concejal alega que su acceso al CPD no se produjo el 2 de diciembre de 2019, sino el día 19 de noviembre de 2019. Según su versión, este acceso aconteció tras reunión en el despacho del Alcalde que contó con la presencia

de ambos, la de la teniente de alcalde y la de una empresa informática especializada en protección de datos (presumiblemente RCMJIT, S.L.).

- El concejal expone que en dicha reunión se trató la presentación de oferta de la empresa en cuestión para adaptar el Ayuntamiento y su CPD al *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)* (en adelante RGPD). El concejal manifiesta que el departamento de informática del Ayuntamiento no había realizado dicha adaptación normativa en el organismo.
- El concejal informa de que en la reunión la empresa externa especializada solicitó ver presencialmente el CPD, a lo que, según declara el concejal, el Alcalde otorgó su permiso y ordenó al conserje municipal abrir la puerta del CPD para acudir en ese momento todos los integrantes de la reunión a visitarlo. El concejal añade que el consentimiento del Alcalde a esta visita al CPD está reconocido en el pleno ordinario municipal del 28 de mayo de 2020.
- El concejal manifiesta que acudieron al CPD y resultó que la puerta se encontraba abierta, aunque no había persona alguna en su interior. Este acceso al CPD se produjo, según su versión, por parte de él, de la teniente de alcalde y de tres representantes de la empresa externa citada. El concejal amplía que el Alcalde fue requerido para otro asunto en el trayecto entre su despacho y el CPD.
- El concejal señala que, una vez dentro del CPD, se visualizó la situación de las dependencias y de los equipos existentes, especialmente centrados en que los representantes de la empresa externa pudieran ofrecer una oferta rápida y precisa de los trabajos a desarrollar para la adaptación al RGPD. El concejal precisa que existía temor por parte del Ayuntamiento a ser sancionados por no cumplir con la reseñada disposición legal.
- El concejal manifiesta que, al día siguiente, 20 de noviembre de 2019, con carácter urgente, la empresa externa remitió al Ayuntamiento la oferta sobre los trabajos a desempeñar en la institución para su adecuación al RGPD.
- El concejal dice no disponer de alguna otra información ni haber realizado fotografía alguna en el CPD y niega haber extraído datos confidenciales ni personales del CPD.
- El concejal alega sólo conocer los datos que le corresponden como concejal del Ayuntamiento, obtenidos por cauces legales, y guardar reserva de todos aquellos documentos que no son de dominio público.

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

- El Ayuntamiento presenta un RAT (registro de actividades de tratamiento) referido a la actividad de tratamiento de datos personales “Gestión económica”, sobre la que señala:
    - Responsable del tratamiento: Ayuntamiento de Colmenar de Oreja.

- Finalidad del tratamiento: Gestión de la contabilidad municipal, seguimiento de la gestión de proveedores y acreedores.
- Base legitimadora: El cumplimiento de obligaciones legales.
- Descripción de las categorías de afectados y de las categorías de datos personales: Personas cuyos datos constan en los libros de contabilidad del Ayuntamiento.
- Categorías de datos personales: Los necesarios para la llevanza de la gestión contable del Ayuntamiento (datos de proveedores, empleados, contribuyentes y sujetos obligados al pago).
- Tipología de datos personales:
  - *Datos de carácter identificativo:* DNI/NIF, nombre y apellidos, dirección postal, email y teléfono.
  - *Datos económicos-financieros:* datos bancarios.
  - *Categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales:* Bancos, cajas de ahorro y cajas rurales; Administración tributaria y Ministerio de Hacienda.
  - *Transferencias Internacionales de datos:* No se prevén cesiones de datos fuera del Espacio Económico Europeo.
  - *Plazos previstos para la supresión de las diferentes categorías de datos:* El plazo general más amplio de conservación de la documentación se establece con carácter general en la normativa mercantil y es de seis años desde el último asiento en los libros
- Tipo de archivos de que dispone el centro:
  - Archivos en soporte papel bajo llaves.
  - Archivos informatizados.

- El Ayuntamiento aporta un AR (análisis de riesgos), y el criterio para la valoración de los riesgos, en donde se incluye valoración de los:
  - Riesgos inherentes a la finalidad de los tratamientos de datos.
  - Riesgos inherentes al tratamiento de datos a gran escala.
  - Riesgos derivados del sistema de tratamiento de datos utilizados.
  - Riesgos imputables en derecho de información.
  - Riesgos relativos a la base jurídica del tratamiento de datos.
  - Riesgos por el acceso y ejercicio a los derechos de los interesados.
  - Riesgos derivados del tratamiento de datos llevado a cabo por el personal.
  - Riesgos derivados del acceso de datos por parte de encargado de tratamiento.

- Riesgos derivados de la cesión de datos a otras entidades.
- Riesgos derivados de la utilización de equipos informáticos.
- Riesgos derivados de la utilización de *software* en el tratamiento de datos.
- Riesgos relativos a la conservación y recuperación de la información.
- Riesgos derivados de la utilización de dispositivos de almacenamiento masivo (USB).
- Riesgos relativos al almacenamiento de la información en soporte papel.
- Riesgos correspondientes al uso de la página web.

Tras la ponderación realizada, el riesgo resultante es calificado como BAJO (en una escala valorativa definida en términos de BAJO, MODERADO, ALTO, MUY ALTO y MÁXIMO).

- El Ayuntamiento manifiesta que el acceso al CPD se realiza únicamente por medio de autorización del señor alcalde y del personal destinado en el Ayuntamiento, acceso para el cual, según informa, existe doble puerta con llave, la cual requiere de intervención del conserje municipal.
- El Ayuntamiento expone que las contraseñas de acceso de los concejales al sistema municipal son de tipo alfanuméricas.

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

3.1. De carácter correctivo (reactivas para subsanar la brecha de seguridad):

- El Ayuntamiento obligó al cambio de contraseñas seguras de todos los concejales y servidores tras detectar la brecha de seguridad.

En este sentido, el Ayuntamiento adjunta un oficio informativo, firmado por el Alcalde en fecha 28 de enero de 2020, el cual expresa la existencia de una brecha de seguridad física de datos confidenciales, su imposible cuantificación en daños y solicitud de presencia de los concejales ante el departamento de informática municipal para proceder al cambio de sus contraseñas de acceso a los servicios municipales.

- El Ayuntamiento sostiene haber procedido a una revisión de los sistemas y a un refuerzo de la seguridad.

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

- El Ayuntamiento demuestra haber realizado un recordatorio al conserje municipal sobre la no apertura de las dependencias municipales a terceras personas.

Concretamente, el Ayuntamiento presenta una notificación del Alcalde, firmada por éste el 28 de febrero de 2020 y dirigida y recibida con firma por parte del conserje municipal, en la que se evoca un modelo de obligaciones y funciones supuestamente entregado al personal del Ayuntamiento referente a la normativa legal de protección de datos.

Además de citar la necesidad de disponer de medidas de seguridad organizativas y técnicas por parte de cualquier entidad que recopile y gestione datos de carácter personal, en dicha notificación se hace conocedor explícitamente al conserje municipal de que no podrá abrir los despachos ni el CPD a terceras personas donde se realice la gestión de datos de carácter personal del Ayuntamiento, salvo cuando ocurra alguna de las siguientes circunstancias:

- Autorización expresa del responsable del Ayuntamiento (el Alcalde).
- Bajo consentimiento de la persona responsable de dicho despacho, habitáculo y CPD del Ayuntamiento, que haya sido nombrado con anterioridad por el Alcalde.

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

En el presente caso, consta que con anterioridad a la brecha de seguridad de datos personales, la investigada no tenía implantadas medidas de seguridad razonables en función de los posibles riesgos estimados. En concreto afirma que disponía de las contraseñas de acceso al sistema de información municipal de los miembros de la entidad local escritos "*en claro"* y que ahora manifiestan que ese documento fue fotografiado. No obstante, consta que esta irregularidad fue subsanada y se dictaron instrucciones a todo el personal para modificar las claves de acceso.

Al margen de la discrepancia de fechas en el acaecimiento de la posible brecha de seguridad (29/11/2019 o 2/12/2020), se debe señalar que fue detectada el 28/01/2020, dos meses después, por lo que no es posible aseverar que las irregularidades detectadas por los concejales de diversos partidos respecto a problemas con sus correos electrónicos tuvieran su origen en los hechos ahora analizados, sino que pudieron deberse a otros incidentes de diversa índole posteriores.

Por otro lado, se significa que el acceso al CPD se realizaba siempre bajo autorización del Alcalde o responsable directo del despacho. Así lo reitera el propio Alcalde al recordar a todo el personal sus obligaciones en materia de protección de datos, por lo que salvo prueba en contrario, este requisito de acceso consta cumplido.

Por último, se debe señalar que de la definición de "violación de seguridad de datos personales" (art 4.12 del RGPD), no se infiere en el presente caso que se cumplan las condiciones que permitan calificar los hechos ahora analizados como una "brecha se seguridad", toda vez que no se ha podido acreditar de forma inequívoca que se hayan

destruido, perdido o alterados accidental o ilícitamente datos personales transmitidos, conservados o tratados de otra forma, o la comunicaciones o accesos no autorizados a dichos datos, si bien podría considerarse, en su caso, como un incidente de seguridad informática o disciplinario interno.

La documentación generada de todo el proceso de detección, contención, respuesta y recolección y custodia de evidencias ante una posible brecha de seguridad de los datos personales es importante de cara a comunicaciones a las posibles partes interesadas tanto de carácter interno o externo, y para la elaboración de un informe final que tras su análisis permita extraer conclusiones. Este informe final, elaborado tras el seguimiento y cierre de este tipo de incidentes y su impacto, es una valiosa fuente de información con la que debe alimentarse el análisis y la gestión de riesgos futuros. El uso de esta información servirá para prevenir la reiteración de hechos similares.

III

En el presente caso, no han quedado acreditadas circunstancias que permitan considerar los hechos notificados como una “violación de la seguridad de los datos personales” conforme al definición del art 4.12 del RGPD, por lo que procede l archivo de las actuaciones.

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 a:

- AYUNTAMIENTO DE COLMENAR DE OREJA, con NIF P2804300H y domicilio en PLAZA MAYOR, 1 - 28380 COLMENAR DE OREJA (MADRID).
- D. ***A.A.A.***, con NIF ******NIF.1*** y domicilio, como concejal del Ayuntamiento por el partido político VOX ESPAÑA (con NIF G86867108), en ******DIRECCIÓN.1***

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.

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