Expediente Nº: E/02824/2018

RESOLUCIÓN DE ARCHIVO DE ACTUACIONES

De las actuaciones practicadas por la Agencia Española de Protección de Datos ante el Ayuntamiento de Valdepeñas, en virtud de la notificación presentada por el mencionado Ayuntamiento, y teniendo como base los siguientes

HECHOS

PRIMERO: Con fecha 4 de mayo de 2018, tuvo entrada en esta Agencia un escrito remitido por el Ayuntamiento de Valdepeñas en el que notifica una quiebra de seguridad con el que aporta un informe de la incidencia en el que se pone de manifiesto que:

> Con fecha 18 de abril detectan, por medio de un empleado del servicio de informática, que el servicio de Tesorería firmó un documento, con fecha 28 de febrero de 2018, que contenía los certificados de retenciones de los trabajadores del Ayuntamiento, con objeto de agilizar el trámite de los certificados y no tramitar uno a uno cuando el trabajador lo solicitará.
>
> El documento se archivó en un expediente del citado servicio al que solo tiene acceso el personal adscrito al mismo y los administradores del sistema. No obstante, había una posibilidad de acceso al documento que desde el servicio no se contempló.
>
> Al firmarse el documento electrónicamente, al pie de página del mismo se incluye información sobre la firma que incluye un código de verificación con objeto de que se pueda consultar en la sede electrónica del Ayuntamiento. Al realizar esta consulta se obtiene la firma y el documento original, por lo que era posible acceder a los certificados de todos los trabajadores.
>
> El servicio de Tesorería ha verificado que se han emitido 15 o 10 copias del documento (de la parte correspondiente a cada trabajador que lo solicitó).
>
> Aunque verificar la firma del documento no es una práctica habitual (hay que introducir todo el código CSV en un navegador), no tienen la certeza de que el documento original con los datos de los trabajadores no haya sido accedido.
>
> Tras detectar la anomalía se han tomado las siguientes medidas:
>
> - Informar al servicio de Tesorería de la situación para que dejase de emitir copias parciales de ese documento.
> - Adoptar medidas técnicas consistentes en bloquear el acceso al documento a través del verificador de la sede electrónica.
> - Notificar la quiebra de seguridad a la Agencia.

SEGUNDO: Tras la recepción de la denuncia la Subdirección General de Inspección de Datos procedió a la realización de actuaciones previas de investigación para el

esclarecimiento de los hechos denunciados, teniendo conocimiento de los siguientes extremos:

Con fecha 6 de junio de 2018 se solicita al Ayuntamiento de Valdepeñas información y documentación en relación con la quiebra de seguridad notificada y, con fecha 22 de junio de 2018, remiten la siguiente:

1. Informe de la incidencia de seguridad que coincide con el aportado en la notificación de la brecha de seguridad a la Agencia.
2. Respecto a la cronología de los hechos:
    a. Con fecha 28 de febrero de 2018, se firma el documento que contiene en cada página, el certificado de retenciones de cada empleado del Ayuntamiento, a cada empleado se entrega la página correspondiente a su certificado a medida que lo solicitan.
    b. 18 de abril de 2018, un empleado del Ayuntamiento, perteneciente a los servicios informáticas, detecta la incidencia.
    c. 18 de abril de 2018, se bloquea el acceso al documento a través del código validador en la sede electrónica.
    d. 27 de abril de 2018, se efectúa la notificación de la incidencia a la Agencia.
3. Respecto a las causas de la incidencia:
    a. Se produce por un error humano, al desconocer las consecuencias de firmar electrónicamente un único documento con los datos de varias personas y la distribución del mismo a todas ellas, aunque solo se les hiciera entrega de la parte del documento que les correspondía.
4. Respecto al número de personas afectadas:
    a. El documento se entregó aproximadamente a 15 personas, aunque a cada una solo se le hizo entrega de su certificado de retenciones.
5. El Ayuntamiento no ha tenido constancia de la utilización por parte de terceros de los datos que constaban en el documento.
6. Teniendo en cuenta el número de afectados y que se trata de un documento interno que, a priori, no sería susceptible de que por parte de los destinatarios se comprobara la firma, se tomó la decisión de no notificar a los afectados sobre la quiebra de seguridad.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver la Directora de la Agencia Española de Protección de Datos, conforme a lo establecido en el artículo 37.d) en relación con el artículo 36, ambos de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD).

II

El 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 lo sucesivo RGPD) indica que las violaciones de la seguridad de los datos personales pueden entrañar daños y perjuicios físicos, materiales o inmateriales para las personas físicas. Por consiguiente, tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una violación de la seguridad de los datos personales debe, sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, notificar la violación de la seguridad de los datos personales a la autoridad de control competente, a menos que el responsable pueda demostrar, atendiendo al principio de responsabilidad proactiva, la improbabilidad de que la violación de la seguridad de los datos personales entrañe un riesgo para los derechos y las libertades de las personas físicas.

El responsable del tratamiento debe comunicar al interesado sin dilación indebida la violación de la seguridad de los datos personales en caso de que puede entrañar un alto riesgo para sus derechos y libertades, y permitirle tomar las precauciones necesarias. La comunicación debe describir la naturaleza de la violación de la seguridad de los datos personales y las recomendaciones para que la persona física afectada mitigue los potenciales efectos adversos resultantes de la violación. Dichas comunicaciones a los interesados deben realizarse tan pronto como sea razonablemente posible y en estrecha cooperación con la autoridad de control, siguiendo sus orientaciones o las de otras autoridades competentes, como las autoridades policiales. Así, por ejemplo, la necesidad de mitigar un riesgo de daños y perjuicios inmediatos justificaría una rápida comunicación con los interesados, mientras que cabe justificar que la comunicación lleve más tiempo por la necesidad de aplicar medidas adecuadas para impedir violaciones de la seguridad de los datos personales continúas o similares.

En el artículo 33 del RGPD establece la forma en que ha de notificarse una violación de la seguridad de los datos personales a la autoridad de control, determinando lo siguiente:

“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."

Por otro lado, el artículo 34 del Reglamento mencionado indica cuando es necesario informar de una violación de la seguridad de los datos personales al interesado, señalando lo siguiente:

1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3."

El Ayuntamiento de Valdepeñas notificó a esta autoridad de control la quiebra de seguridad que se había detectado en la Tesorería de ese Consistorio, en fecha 4 de mayo de 2018. La quiebra fue detectada por un empleado de informática el día 18 de abril de 2018, es decir, con anterioridad a la plena aplicación del RGPD, que se produjo el día 25 de mayo de 2018.

El Ayuntamiento de Valdepeñas ha expuesto, detalladamente, todas las actuaciones realizadas tras la detección de la quiebra de seguridad indicando que no han tenido constancia de la utilización por terceros de los datos personales obtenidos a través de la quiebra. Por último señala el Ayuntamiento que teniendo en cuenta el número de posibles afectados y que se trata de un documento interno y no es susceptible, a priori, de que los propios trabajadores comprueben la veracidad de las firmas, al estar familiarizados con ese tipo de documentos y haberlos solicitado personalmente a los responsables del servicio, tomaron la decisión de no notificar a los afectados la quiebra de seguridad.

El Ayuntamiento de Valdepeñas ha cumplido lo establecido en el RGPD al notificar la brecha de seguridad detectada en la Tesorería del mismo; aún con anterioridad a ser plenamente aplicable el mencionado Reglamento. El plazo establecido de las 72 horas para notificar no se ha cumplido ya que, como indican, era improbable que dicha violación de la seguridad constituyese un riesgo para los derechos y las libertades de las personas físicas.

III

El artículo 126.1, apartado segundo, del Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD) establece:

"Si de las actuaciones no se derivasen hechos susceptibles de motivar la imputación de infracción alguna, el Director de la Agencia Española de Protección de Datos dictará resolución de archivo que se notificará al investigado y al denunciante, en su caso."

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

SE ACUERDA:

PROCEDER AL ARCHIVO de las presentes actuaciones.

NOTIFICAR la presente Resolución al **AYUNTAMIENTO DE VALDEPEÑAS.**

De conformidad con lo establecido en el apartado 2 del artículo 37 de la LOPD,

en la redacción dada por el artículo 82 de la Ley 62/2003, de 30 de diciembre, de medidas fiscales, administrativas y del orden social, la presente Resolución se hará pública, una vez haya sido notificada a los interesados. La publicación se realizará conforme a lo previsto en la Instrucción 1/2004, de 22 de diciembre, de la Agencia Española de Protección de Datos sobre publicación de sus Resoluciones y con arreglo a lo dispuesto en el artículo 116 del Reglamento de desarrollo de la LOPD aprobado por el Real Decreto 1720/2007, de 21 diciembre.

Contra esta resolución, que pone fin a la vía administrativa (artículo 48.2 de la LOPD), y de conformidad con lo establecido en los artículos 112 y 123 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, 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 del referido texto legal.

Sin embargo, el responsable del fichero de titularidad pública, de acuerdo con el artículo 44.1 de la citada LJCA, sólo podrá interponer 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 LJCA, 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 del referido texto legal.

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