

## Identificación del expediente

Resolución de procedimiento sancionador núm. PS 1/2022, referente al Ayuntamiento de Reus.

## Antecedentes

1. En fecha 28/10/2020 el Ayuntamiento de Reus (en adelante, el Ayuntamiento) notificó a la Autoridad Catalana de Protección de Datos una violación de seguridad de los datos (NVS 67/2020). En esta notificación se exponía que en fecha 26/10/2020 se tuvo conocimiento, mediante el aviso de un ciudadano, del hallazgo en el vertedero de escombros "(...)" del municipio de Tarragona (depósito de escombros y de construcción), de unas bolsas de plástico que contenían expedientes del área de servicios sociales del Ayuntamiento (que incluían datos de menores) y documentación del área de servicios económicos (listados de productividad de trabajadores y de proveedores), para su destrucción.

Asimismo, el Ayuntamiento informaba que la misma mañana en la que tuvo conocimiento del incidente, envió una unidad autorizada al depósito de escombros para recoger la información y devolverla a las dependencias municipales, y que se desconocía la causa que habría propiciado su aparición en el vertedero de escombros, en vez de ser destruida de acuerdo con el circuito seguro del Ayuntamiento, por lo que se había iniciado una investigación interna, para determinar las circunstancias y también si "terceras empresas" habrían intervenido en la violación de seguridad sufrida.

2 . A raíz de esta notificación de violación de seguridad, la Autoridad abrió una fase de información previa (núm. IP 362/2020), de acuerdo con lo que prevé el artículo 7 del Decreto 278/1993, de 9 de noviembre, sobre el procedimiento sancionador de aplicación a los ámbitos de competencia de la Generalidad, y el artículo 55.2 de la Ley 39/2015, de 1 de octubre, del procedimiento administrativo común de las administraciones públicas (en adelante, LPAC), para determinar si los hechos eran susceptibles de motivar la incoación de un procedimiento sancionador, concretamente, en lo referente a las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (art. 32 del RGPD) en la gestión de la documentación destinada a su destrucción, la identificación de la persona o personas que pudieran ser responsables y las circunstancias relevantes que concurrían.

Se incorporó a esta información previa una copia de las actuaciones llevadas a cabo en el marco de la notificación de dicha violación de seguridad (NVS 67/2020). También se incorporó las capturas de pantalla de las noticias sobre el incidente publicadas en diferentes medios de comunicación digitales, y el vídeo grabado por la persona ciudadana que encontró los expedientes municipales en el vertedero de escombros, y que publicó el Diari de Tarragona, en su versión digital, en fecha 02/11/2020.

3 . En el seno de esta fase de información, en fecha 15/01/2021 se requirió al Ayuntamiento de Reus para que informara de lo siguiente:

- del resultado de la indagación interna sobre el suceso incidente.
- del protocolo implantado por el Ayuntamiento para la gestión de la documentación en formato papel destinada a su destrucción y su circuito, incluida la documentación encontrada en el vertedero, y si a raíz del incidente de seguridad sufrido se había revisado y actualizado dicho protocolo/circuito.

4. En fecha 28/01/2021, el Ayuntamiento respondió al anterior requerimiento, a través de escrito en el que exponía, entre otros, lo siguiente:

- Que en cuanto a los resultados de la investigación interna y reservada efectuada por el consistorio de forma inmediata, una vez tuvo conocimiento de la aparición de expedientes municipales en el depósito de escombros, se aporta copia del informe de la misma fecha 28/01/2021 elaborado por el responsable de seguridad del Ayuntamiento (“Informe ejecutivo sobre la investigación interna derivada de la violación de seguridad detectada a raíz del hallazgo de expedientes y documentación municipal en el depósito de escombros y residuo controlado de la (. ..)”).
- En el apartado de conclusiones de dicho informe se hace constar lo siguiente:

*En atención a los hechos comprobados, la investigación abierta concluye lo siguiente:*

*PRIMERA.- Pérdida de control y rotura de los procedimientos en la organización.*

*a. En relación a los expedientes de servicios sociales, la causa que origina la pérdida del control sobre la información se concreta en el momento en que se da la orden, por vía telefónica, de que la documentación debe destruirse, encargándose de esta tarea la unidad de brigadas y sin que se ponga en marcha el procedimiento de «transferencias documentales» para trasladar la documentación al Archivo Municipal para, posteriormente, ser destruida mediante entidad certificadora habilitada que acredite que la destrucción es conforme a la normativa en materia de protección de datos.*

*b. En relación a los expedientes de servicios económicos, la causa que origina la pérdida del control sobre la información se concreta en el momento en que se decide transportar esta documentación a la unidad de brigadas, mediante los servicios de logística, para que sea destruida, y sin que se ponga en marcha el procedimiento de «transferencias documentales» para trasladar la documentación al Archivo Municipal para, posteriormente, ser destruida mediante entidad certificadora habilitada que acredite que la destrucción es conforme a la normativa en materia de protección de datos.*

*c. En ambos casos, y después de entrevistarse con las personas intervinientes, se aprecia desconocimiento de los protocolos y procedimientos a seguir por parte de las personas pertenecientes a las unidades y departamentos, cuya documentación es objeto de traslado, ya que no se activa el procedimiento de “transferencias documentales” a través del Archivo Municipal aplicable dentro de la organización y que asegura el correcto traslado y eliminación.*

*d. Que en las conclusiones a) y b) se detecta el origen de la causa de todo el incidente, que lleva parte de la documentación que está en las brigadas municipales en el depósito de (...), aunque no se pueda determinar con certeza el motivo que explique su aparición en este sitio.*

*e. Que la destrucción de la documentación en dependencias de las brigadas municipales y el personal encargado de hacerlo, evidencien que esta unidad no dispone de las condiciones de seguridad óptimas ni de un control adecuado que garantice que la destrucción se realiza de forma segura, además de que no es la unidad encargada de realizar este tipo de*

*eliminaciones, las cuales se realizan mediante el Archivo Municipal, por el procedimiento mencionado en las letras anteriores.*

*SEGUNDA.- Aparición de los documentos en el depósito controlado de (...).*

*a. La única conexión entre los expedientes encontrados (ubicados en las brigadas municipales) y el vertedero de (...) es la empresa subcontratada que recoge los escombros y los vierte en diferentes vertederos, entre ellos el de (...). Por tanto, se constata que la pérdida del control de la documentación se produce desde que la documentación está ubicada en la unidad de brigadas municipales ya través de un procedimiento carente de las garantías suficientes y adecuadas.*

*b. El lugar donde se encuentra la documentación (vertedero) no es un espacio fácilmente accesible, separado del centro urbano de la ciudad de Tarragona, tratándose de una zona habilitada por empresas transportistas de escombros, por lo que el escape de datos se considera muy remota, salvo la persona denunciante, y no queda constancia de que haya ido más allá, habiéndose contrastado con los departamentos afectados de que la documentación recuperada es la que se encuentra en el vertedero.*

*c. No se ha podido acreditar ni se aprecia intencionalidad de ningún trabajador que implique una mala fe, o dolo con el fin de producir un perjuicio de reputación o económico en el Ayuntamiento. Tampoco se ha podido identificar concretamente a un sujeto o grupo de personas como responsables directos e inmediatos de los hechos ocurridos, sino que son consecuencia de una cadena de desconocimientos y errores a lo largo de todo el procedimiento de traslado y eliminación de la misma. documentación.*

*TERCERA.- Recomendaciones.*

*a. Las brigadas no deben hacer destrucción de documentación administrativa puesto que las instalaciones no son las adecuadas para estas tareas ni su personal está formado para hacerla con las condiciones de seguridad adecuadas.*

*b. Deben revisarse los protocolos de actuación y, especialmente, el referente a los procesos de traslado y destrucción de la documentación en soporte papel y dotarse de nuevos que definan claramente las directrices y procedimientos a seguir y los responsables traslados y eliminación.*

*c. Debe garantizarse que la eliminación de la documentación se realiza a través de una empresa y un servicio de contenedores que garanticen un servicio de destrucción certificada y confidencial de los datos administrativos.*

*d. Se debe hacer difusión y formación a los empleados de los nuevos protocolos y garantizar su cumplimiento.”*

*-Se aporta copia del nuevo protocolo elaborado por la Alcaldía, y aprobado por Decreto de fecha 28/01/2021 “Protocolo de actuación en el tratamiento y destrucción de soportes no automatizados que contengan datos de carácter personal de los que el Ayuntamiento de Reus es responsable” y “ que engloba el procedimiento y circuito a seguir en cuanto al tratamiento, conservación y posterior destrucción de soportes no automatizados que*

*dispongan de datos de carácter personal. Este circuito incluye desde que el Ayuntamiento comienza a tratar documentación con datos personales hasta su posterior destrucción y eliminación.” (...) “ Habiéndose aprobado por el órgano pertinente de la Entidad el Protocolo éste será puesto a disposición de los empleados para su conocimiento y aplicación práctica.”*

5. En fecha 10/01/2022, la directora de la Autoridad Catalana de Protección de Datos acordó iniciar un procedimiento sancionador contra el Ayuntamiento de Reus por una presunta infracción prevista en el artículo 83.4.a), en relación con el artículo 32; ambos del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril, relativo a la protección de las personas físicas en lo que se refiere al tratamiento de datos personales ya la libre circulación de éstas (en adelante, RGPD ). Este acuerdo de iniciación se notificó a la entidad imputada en fecha 11/01/2022.

6. En el acuerdo de iniciación se concedía a la entidad imputada un plazo de 10 días hábiles para formular alegaciones y proponer la práctica de pruebas que considerase convenientes para defender sus intereses.

7. En fecha 25/01/2022, el Ayuntamiento formuló alegaciones al acuerdo de iniciación . Junto con su escrito de alegaciones aportó documentación diversa para justificar sus pretensiones, y pidió también que se tuvieran por reproducidos los documentos aportados en la NVS 67/2020 y en la fase de información previa al presente procedimiento, los cuales, de acuerdo con lo que se informó, ya constaban incorporados al presente procedimiento.

8. En fecha 28/03/2022, la persona instructora de este procedimiento formuló una propuesta de resolución, por la que proponía que la directora de la Autoridad Catalana de Protección de Datos amonestara al Ayuntamiento de Reus como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32, ambos del RGPD.

Esta propuesta de resolución se notificó el mismo día 28/03/2022 al Ayuntamiento de Reus y se concedía un plazo de 10 días para formular alegaciones.

9. La entidad imputada presentó escrito de alegaciones a la propuesta de resolución.

### **Hechos probados**

En fecha 25/10/2020 una persona ciudadana encontró en el depósito de escombros “(...)”, del municipio de Tarragona, varias bolsas de plástico que contenían documentación con datos personales relativos a expedientes del Área de Servicios Sociales del Ayuntamiento (que incluían datos de menores), de los ciudadanos atendidos por el Área de Bienestar en el distrito V entre los años 2012 y 2015, y del Área de Servicios Económicos (listados de productividad de trabajadores y proveedores), que estaban destinados a ser destruidos.

Toda esta documentación con datos personales fue trasladada, a petición de personal del consistorio, a las instalaciones de la Unidad de Brigadas del Ayuntamiento, para su destrucción, y depositada en el espacio en el que se encuentra ubicada la máquina industrial de destrucción de papel, zona sin ningún cierre perimetral, a unos metros de los contenedores de escombros, lo que propició que empresas externas las trasladaran al vertedero de “(...)”, de modo que terceras personas no autorizadas habrían tenido acceso a la información allí contenida.

## Fundamentos de derecho

1. Son de aplicación a este procedimiento lo que prevén la LPAC, y el artículo 15 del Decreto 278/1993, según lo que prevé la DT 2a de la Ley 32/2010, de 1 de octubre, de Autoridad Catalana de Protección de Datos. De conformidad con los artículos 5 y 8 de la Ley 32/2010, la resolución del procedimiento sancionador corresponde a la directora de la Autoridad Catalana de Protección de Datos.

2. El Ayuntamiento de Reus ha formulado alegaciones tanto en el acuerdo de iniciación como en la propuesta de resolución. En el escrito de alegaciones a la propuesta, la entidad se reiteró en las que ya formuló ante el acuerdo de iniciación. Por eso, aunque dichas alegaciones ya se analizaron en la propuesta de resolución, se reproducen aquí.

### 2.1. Sobre las medidas previamente adoptadas.

La entidad imputada esgrime que el Ayuntamiento disponía, en el momento de producirse los hechos, de medidas técnicas y organizativas adecuadas en los términos del artículo 32 del RGPD, conocidas por todo el personal, para su traslado y destrucción segura de la documentación con datos personales, si bien éstos, por error humano interno de las unidades intervinientes, no fueron aplicados correctamente.

Añade que, a tal efecto, el Ayuntamiento disponía de dos documentos internos, que se encontraban a disposición del personal en la Intranet, y que regulaban los procesos de traslado y de destrucción de la documentación, en concreto, el *documento interno de trámite de transferencia* y el *documento interno de archivo de gestión de oficina*, los cuales fueron aportados durante la fase de información previa, y evidenciaban la existencia de medidas de seguridad para la destrucción de la documentación.

Y que, *“ adicionalmente a los procedimientos indicados en dichos documentos, el Ayuntamiento aplicaba determinados procesos estandarizados relativos al tratamiento de datos en formato no automatizado, si bien éstos no constaban documentados ”*.

Respecto a estas alegaciones, tal y como indicaba la instructora, lo primero que hay que hacer notar es que ninguno de los dos documentos internos a los que hace referencia la entidad imputada, establecen un procedimiento o circuito a seguir para la destrucción segura de la documentación en papel con datos personales (es decir, desde el momento en que se decide que la documentación debe ser destruida, hasta su destrucción definitiva) sino que lo que establecen es, en el caso del *“ documento interno del trámite de transferencia ”*, las pautas que las diferentes unidades administrativas deben seguir para transferir la documentación administrativa de más de cinco años al Archivo Municipal (cómo se debe ordenar y preparar dicha documentación), a fin de que dicho órgano no asuma su custodia y decida su destino después de un proceso de valoración documental, sin hacer ninguna referencia al proceso de destrucción, y en el caso del *“ documento interno de archivo de gestión de oficina ”*, se explica cuáles son los documentos que forman parte de un expediente administrativo que pueden eliminarse en la propia unidad administrativa, si bien tampoco incluye ninguna indicación sobre cuál es el proceso a seguir para la destrucción de dicha información.

Dicho esto, el artículo 5.1.f) del RGPD establece que los datos personales serán *“ tratados de tal modo que se garantice una seguridad adecuada de las datos personales , incluida la*

*protección contra el tratamiento no autorizado o ilícito y contra su pérdida , destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (« integridad y confidencialidad »).*”

A su vez, el artículo 32.1 RGPD dispone que *“el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo (...)”*.

Lo que exige el artículo 32.1 RGPD es que las medidas de seguridad, que deben determinarse teniendo en cuenta los riesgos derivados de la pérdida o el acceso no autorizado a los datos (entre otros), sean las adecuadas.

Pues bien, en el caso concreto que nos ocupa, se ha puesto de manifiesto que el Ayuntamiento no tenía implementadas las medidas técnicas y organizativas adecuadas para garantizar un nivel de seguridad adecuado al riesgo en la gestión de la documentación en papel destinada a su destrucción, y esto lo ha evidenciado la realidad de los hechos probados, no contradichos por el Ayuntamiento, los cuales llevan a concluir que no se garantizó la seguridad de los datos de forma efectiva en el procedimiento de destrucción de la documentación en papel , y en particular su correcta custodia para evitar el acceso por terceros no autorizados.

En efecto, la seguridad de los datos se vio comprometida, tal y como reconoce el propio Ayuntamiento en sus conclusiones reproducidas en esta resolución (antecedente 4º), desde el momento en que el personal desconocía cuál era el procedimiento a seguir para la destrucción segura de la documentación con datos personales, y que la destrucción se llevó a cabo mediante un *“ procedimiento carente de las garantías suficientes y adecuadas ”*, que comportó que la documentación quedara depositada en una zona que *“ no disponía de las condiciones de seguridad adecuadas ni de un control adecuado que garanticen que la destrucción se realiza de forma segura ”*.

Así las cosas, no puede lograr la afirmación de la entidad imputada en el sentido de que el Ayuntamiento, en el momento de producirse los hechos, tenía implementadas las medidas técnicas y organizativas adecuadas o adecuadas para garantizar la seguridad de los datos en la fase de destrucción.

Por último, cabe señalar que, según el sistema de responsabilidad previsto en el RGPD y particularmente en el artículo 70 del LOPDDDD la responsabilidad por las infracciones a la normativa de protección de datos recae, en todo caso, sobre los responsables de los tratamientos, y no sobre su personal. En concreto, el citado artículo 70 de la LOPDDDD establece que:

*“Sujetos responsables.*

*1. Están sujetas al régimen sancionador que establecen el Reglamento (UE) 2016/679 y esta Ley orgánica:*

*a) Los responsables de los tratamientos.*

2.2 Sobre las medidas adoptadas después de los hechos probados.

El Ayuntamiento ha alegado que una vez ocurridos los hechos que motivaron la incoación del presente procedimiento, se adoptaron, de forma inmediata, determinadas medidas para corregir los efectos de la infracción imputada, como *“ la recogida y custodia de todos los*

*expedientes en un espacio cerrado y de acceso restringido” y el posterior traslado al Archivo Municipal, y que, asimismo, y con el fin de evitar que, en la medida de lo posible, se volvieran a producir incidentes de la misma naturaleza se “ procedió de forma inmediata a actualizar el circuito existente, (...) y se va elaborar un nuevo protocolo, en sustitución de los procedimientos documentados existentes en ese momento, denominado “protocolo de actuación en el tratamiento y destrucción de soportes no automatizados que contengan datos de carácter personal de los que el Ayuntamiento de Reus es responsable” (en adelante , el Protocolo), que engloba el procedimiento y circuito a seguir en cuanto al tratamiento, conservación y posterior destrucción de soportes no automatizados que dispongan de datos de carácter personal. Este circuito incluye desde que el Ayuntamiento comienza a tratar documentación con datos personales hasta su posterior destrucción y eliminación”.*

En este mismo sentido, el Ayuntamiento detalla, cuáles son las medidas que ha implementado, a raíz de la aprobación del Protocolo, a fin de garantizar la destrucción segura de la documentación con datos personales, y pide que, a tal efecto, se tenga por reproducida la documentación acreditativa de éstas que se aportó ante el acuerdo de incoación. Las medidas se pueden resumir en las siguientes:

- La instalación de contenedores herméticos, en diversas estancias y puestos de trabajo del Ayuntamiento, “ *para la recogida y traslado seguro de la documentación con datos personales objeto de destrucción en el Archivo Municipal, y la posterior destrucción a través de la empresa externa (...)* ”.
- Si bien la Unidad de Brigadas Municipales, continúa participando en el proceso de traslado de documentación, en plena coordinación con las unidades administrativas, dicha Unidad “ *ya no es competente para llevar a cabo “ninguna función -ni de colaboración- relacionada con la destrucción y eliminación de documentación del Ayuntamiento que contenga datos personales”.*
- El Archivo Municipal, “ *en la línea ya adoptada con anterioridad a la aprobación del Protocolo (...)*” es el único órgano que *coordina el servicio de destrucción segura de la documentación*, mediante los servicios que presta la empresa ( ...), de acuerdo con lo que se acredita con los certificados de destrucción segura aportados (documentos 11 a 57).
- El Protocolo se ha puesto a disposición de todos los empleados del Ayuntamiento , a través de la Intranet, ( documento 59 aportado delante el acuerdo de incoación ) y se les ha informado de su contenido .

Al respecto, cabe poner de manifiesto, como ya se adelantaba en la propuesta de resolución, que si bien todas estas medidas, llevadas a cabo una vez ocurrido el incidente, no desvirtúan los hechos aquí imputados ni tampoco su calificación jurídica , si que despliegan efectos en el sentido de que hacen innecesario que la Autoridad requiera adoptar medidas correctoras para corregir los efectos de la infracción.

### 2.3 Sobre la carencia de denuncias de las personas afectadas.

Por último, para justificar su solicitud de sobreseimiento del procedimiento, el Ayuntamiento esgrime que, una vez se efectuó la comunicación pública del incidente, de conformidad con lo previsto en el artículo 34 del 'RGPD, ninguna de las personas afectadas (titulares de los

datos personales contenidos en los expedientes hallados en el vertedero de escombros), ha formulado queja alguna al respecto, ni se tiene constancia tampoco de que la Autoridad haya recibido denuncia alguna.

Al respecto, cabe decir que, entre los elementos objetivos que conforman el tipo infractor previsto en el artículo 83.4.a) del RGPD no se incluye la necesidad de que la persona titular de los datos, en relación a los cuales se ha producido la infracción, considere vulnerada su privacidad o intimidad. El tipo sólo requiere la falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos exigidos en el artículo 32.1 del RGPD. Es decir, el elemento objetivo del tipo infractor se dará siempre y cuando se produzca una efectiva carencia de medidas de seguridad adecuadas al riesgo.

Por eso, esta alegación tampoco puede lograr.

**3.** En relación con los hechos descritos en el apartado de hechos probados, es necesario acudir al artículo 5.1.f) del RGPD, que regula el principio de integridad y de confidencialidad, determinando que los datos personales serán *“tratados de tal modo que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad)”*.

Por su parte, el artículo 32.1 del RGPD, en lo referente a la seguridad de los datos, dispone lo siguiente:

*“1. Teniendo en cuenta el estado de la técnica, las costas de aplicación, y la naturaleza, el alcance, el contexto y las 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.”*

En el presente caso, ha quedado acreditado que el Ayuntamiento de Reus, en tanto que responsable de tratamiento de los datos afectados, no adoptó o implementó medidas técnicas y organizativas apropiadas para garantizar su seguridad (tendientes a evitar que a estos datos se encuentre pudieran acceder personas no autorizadas), lo que se considera constitutivo de la infracción prevista en el artículo 83.4.a) del RGPD, que tipifica la vulneración de *las obligaciones del responsable y del encargado a tenor de los artículos 8, 11, 25 a 39, 42 y 43*”, entre las que se encuentra la prevista en el artículo 32 RGPD.

Dicho esto, la conducta que aquí se aborda se ha recogido como infracción grave en el artículo 73.f) de la LOPDDDD, en la siguiente forma:

*"f) La falta de adopción de las medidas técnicas y organizativas que sean apropiadas para garantizar un nivel de seguridad adecuado al riesgo del tratamiento, en los términos que exige el artículo 32.1 del Reglamento (UE) 2016/679."*

4. El artículo 77.2 LOPDGDD dispone que, en el caso de infracciones cometidas por los responsables o encargados enumerados en el art. 77.1 LOPDGDD, la autoridad de protección de datos competente :

*"(...) debe dictar una resolución que las sancione con una amonestación. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se haya cometido.*

*La resolución se notificará al responsable o encargado del tratamiento, a cuyo órgano dependa jerárquicamente, en su caso, ya los afectados que tengan la condición de interesado, en su caso."*

En términos similares a la LOPDDDD, el artículo 21.2 de la Ley 32/2010 , determina lo siguiente:

*"2. En el caso de infracciones cometidas con relación a ficheros de titularidad pública, el director o directora de la Autoritat Catalana de Protecció de Dades debe dictar una resolución que declare la infracción y establezca las medidas a adoptar para corregir sus efectos . Además, puede proponer, en su caso, la iniciación de actuaciones disciplinarias de acuerdo con lo que establece la legislación vigente sobre el régimen disciplinario del personal al servicio de las administraciones públicas. Esta resolución debe notificarse a la persona responsable del fichero o del tratamiento, a la encargada del tratamiento, si procede, al órgano del que dependen ya las personas afectadas, si las hubiere".*

Como se ha avanzado en los antecedentes y en el fundamento de derecho 2º, el Ayuntamiento de Reus ha informado a esta Autoridad haber llevado a cabo determinadas medidas para corregir los efectos de la infracción imputada, y también de aquellas tendentes a evitar que volvieron a producirse hechos como los que habían dado lugar a la incoación del presente procedimiento sancionador. Así las cosas, en este caso, y tal y como se ha avanzado, no es necesario requerir medidas correctoras.

Por todo esto, resuelvo:

**1.** Amonestar al Ayuntamiento de Reus como responsable de una infracción prevista en el artículo 83.4.a) en relación con el artículo 32, ambos del RGPD.

No es necesario requerir medidas correctoras para corregir los efectos de la infracción, de conformidad con lo expuesto en el fundamento de derecho 4º.

**2.** Notificar esta resolución al Ayuntamiento de Reus.

**3.** Comunicar la resolución al Síndic de Greuges, de conformidad con lo que prevé el artículo 77.5 del LOPDDDD

**4 .** Ordenar que se publique la resolución en la web de la Autoridad (apdcat.gencat.cat), de conformidad con el artículo 17 de la Ley 32/2010, de 1 de octubre

Contra esta resolución, que pone fin a la vía administrativa de acuerdo con los artículos 26.2 de la Ley 32/2010, de 1 de octubre, de la Autoridad Catalana de Protección de Datos, y 14.3 del Decreto 48/2003 , de 20 de febrero, por el que se aprueba el Estatuto de la Agencia Catalana de Protección de Datos, la entidad imputada puede interponer, con carácter potestativo, un recurso de reposición ante la directora de la Autoridad Catalana de Protección de Datos, en el plazo de un mes a contar desde el día siguiente de su notificación, de acuerdo con lo que prevén el artículo 123 y siguientes de la LPAC. También puede interponer directamente un recurso contencioso administrativo ante los Juzgados de lo Contencioso-Administrativo, en el plazo de dos meses a contar desde el día siguiente de su notificación, de acuerdo con los artículos 8, 14 y 46 de la Ley 29/1998, de 13 de julio, reguladora de la jurisdicción contencioso-administrativa.

Si la entidad imputada manifiesta a la Autoridad su intención de interponer recurso contencioso administrativo contra la resolución firme en vía administrativa, la resolución se suspenderá cautelarmente en los términos previstos en el artículo 90.3 de la LPAC.

Igualmente, la entidad imputada podrá interponer cualquier otro recurso que estime conveniente para defender sus intereses.

La directora,

Traducción Autoritat Catalana de Protecció de Dades