La consulta se plantea en los siguientes términos: la consultante es un Consorcio público que aglutina varios Ayuntamientos de la provincia de Granada. Este Consorcio es propietario del 60% de las acciones de la empresa que gestiona el agua en todos estos municipios. Dicho Consorcio ha aprobado un protocolo titulado "protocolo regulador de medidas contra la pobreza hídrica y la vulnerabilidad económica" (que se acompaña a la consulta). Dicho protocolo, entre otras cosas, -continúa la consulta- señala que la empresa de aguas dará traslado de los clientes que tengan impago de facturas “al Consorcio”, conteniendo dicha notificación sus datos personales identificativos así como la deuda pendiente. El Consorcio, a su vez, dará traslado de los expedientes de estos deudores a cada Ayuntamiento para que pueda activar alguna de las políticas sociales que crean oportuno. La concreta pregunta dice así: “nos preguntamos desde el Consorcio si esta comunicación de datos desde la empresa de aguas al Consorcio y desde este a los ayuntamientos es lícita”. A su vez, pregunta “qué medidas de seguridad se podrían aplicar ya que los datos son recibidos y enviados por el Consorcio en formato papel y nos preocupa que uso se puede hacer en el Ayuntamiento sobre todo a nivel de personal que los va a tratar”.

I

Pues bien, examinado el protocolo a que se hace referencia en la consulta, y que como ha quedado dicho ha sido aportado por el consultante, vemos que el mismo contiene unas pautas de actuación ante el caso de impago de recibos de agua. Dicho protocolo dice que cuando un usuario, titular de una póliza de suministro de agua, “se encuentra en una situación económica muy desfavorable y no puede hacer frente al pago del recibo de agua” podrá dirigirse a la compañía suministradora, a los servicios sociales del ayuntamiento, o dejar el recibo pendiente de pago. Estas tres alternativas son a continuación desarrolladas en el protocolo.

(i) Cuando el usuario se dirige a la compañía suministradora, esta le informa de las posibilidades de obtener una tarifa acorde a su situación, e intenta negociar aplazamientos o fraccionamientos de facturas en caso de que se trate de una dificultad temporal o puntual. Pero sí se trata de un problema continuado, la empresa

de aguas remite el caso a los servicios sociales (es de suponer que del Ayuntamiento correspondiente) “para encontrar una solución a su situación”.

(ii) Si el usuario se dirige a los Servicios Sociales, éstos realizan en primer lugar la misma función informativa en relación con los posibles tarifas aplicables a la situación concreta del interesado. Pero añade que el Ayuntamiento, a través de sus Servicios Sociales, comunicará la empresa de aguas con la mayor celeridad posible los casos que considere vulnerables.

(iii) Si el interesado deja de pagar las facturas, la empresa de aguas trata de encontrar una solución, pero en este caso no se establece en el protocolo una cesión de datos a un tercero.

A mayor abundamiento, el protocolo añade que la empresa de aguas enviará al Consorcio “el listado de cortes de suministro” para que ésta “dé traslado de forma ágil y a la mayor brevedad de listado por Ayuntamientos, y comunicará dicha remisión a la empresa de aguas, para que los Ayuntamientos, a través de los Servicios Sociales se puedan poner en contacto con la empresa de aguas si detectase la existencia de algún cliente vulnerable que no estuviese identificado por” la empresa de aguas “a la fecha del comunicado”.

II

El art. 3 a) LOPD define dato de carácter personal como “cualquier información concerniente a personas físicas identificadas o identificables”.

Nos encontramos por lo tanto con que el protocolo hace referencia a una serie de tratamientos de datos, en concreto a cesiones de datos, que son definidas en el art. 3 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, (LOPD) como “toda revelación de datos realizada a una persona distinta del interesado”.

El protocolo prevé que la empresa de aguas pueda transmitir los datos (a) a los servicios sociales; (b) que los servicios sociales lo puedan trasmitir a la empresa de aguas; (c) que la empresa de aguas remita al Consorcio el listado

de los cortes de suministro, de forma individual, por lo tanto identificando a las personas concretas que resultan deudoras o, más allá, a quienes se ha cortado el suministro, o (d) que el Consorcio lo remita a los Ayuntamientos. Toda ello supone una cesión de datos personales ya que consisten en informaciones concernientes a personas físicas identificadas o identificables.

El art. 11.1 LOPD establece que los datos de carácter personal sólo podrán ser comunicados a un tercero (…) con el previo consentimiento del interesado. El art. 11.2 prevé que dicho consentimiento no será preciso en una serie de situaciones, ninguna de las cuales serán el presente caso (la cesión no parece estar autorizada por la ley, no se trata de datos recogidos de fuentes accesibles al público, no se deriva la cesión directamente de la relación jurídica de suministro de aguas, etc.)

En ningún lugar del protocolo se hace referencia alguna a la necesidad de obtener el consentimiento del interesado para comunicar los datos a un tercero.

Es más, la normativa de protección de datos está basada en el principio de finalidad del tratamiento (principio de calidad de los datos), de suerte que la utilización de los datos personales está sujeta a las finalidades determinadas, explícitas y legítimas para los que dichos datos hayan obtenido, y no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubiera sido recogidos (art. 4.1 y 4.2 LOPD). Los tribunales han interpretado que finalidad incompatible es toda aquella diferente de la finalidad para la que se hubiera recogido los datos.

No constando el consentimiento del interesado habrá que considerar que el tratamiento de datos en que consiste la cesión de los datos personales del interesado por la empresa de aguas a un tercero (servicios sociales o Consorcio) o por los servicios sociales a la empresa de aguas es contrario a la normativa de protección de datos.

Por lo tanto, para que dicho tratamiento de datos (la cesión) sea considerada acorde con la legislación de protección de datos habrá que obtener el consentimiento previo del interesado, tal y como establece el artículo 11.1 LOPD.

III

A continuación la consulta inquiere sobre las medidas de seguridad, ya que, añade, los datos son recibidos y enviados por el Consorcio en formato papel.

Ante dicha circunstancia, habrá que estar a lo dispuesto en el art. 9 LOPD:

Artículo 9. Seguridad de los datos.

1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.
3. Reglamentariamente se establecerán los requisitos y condiciones que deban reunir los ficheros y las personas que intervengan en el tratamiento de los datos a que se refiere el artículo 7 de esta Ley.

Así como a lo establecido en el Título VIII del Reglamento de desarrollo de la LOPD, aprobado por Real Decreto 1720/2007, de 21 de diciembre (RLOPD), comenzando por el artículo 79, que establece que: *Los responsables de los tratamientos o los ficheros y los encargados del tratamiento* ***deberán*** *implantar las medidas de seguridad con arreglo a lo dispuesto en este Título,* ***con independencia de cuál sea su sistema de tratamiento.***

Por lo tanto el hecho de que los datos se reciban en formato papel, con independencia de que no existiendo el consentimiento se trataría de un incumplimiento de la normativa de protección de datos, no exime al responsable del tratamiento de la implantación de las medidas de seguridad necesarias de conformidad con lo establecido en el RLOPD.

El artículo 81 RLOPD establece que ***todos*** los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad

calificadas de nivel básico (en la forma establecida para los ficheros y tratamientos no automatizados en el capítulo IV del citado título VIII: ver art. 105 RLOPD). Además, según el caso de que estemos en los ficheros a que hace referencia el apartado 2, o 3, de dicho artículo 81 RLOPD habrán de aplicarse las medidas propias del nivel medio, pues su caso del nivel alto.

Deberá además, de conformidad con el artículo 88 RLOPD, elaborarse por el responsable del fichero o tratamiento un **documento de seguridad,** que recogerá las medidas de índole técnica y organizativa acordes a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los sistemas de información. El documento de seguridad deberá contener como mínimo lo establecido en el artículo 88.3 RLOPD.

Por último, el capítulo IV del título VIII RLOPD contiene las medidas de seguridad aplicables a los ficheros y tratamientos no automatizados (ya que según relata la consulta los datos son recibidos y enviados en formato papel). Habrá que estar a todo lo dispuesto en el artículo 105 y siguientes RLOPD, estableciendo las medidas de seguridad necesarias según estemos ante tratamientos que requieran de un nivel de seguridad básico, medio o alto (este último caso procedería por ejemplo cuando las razones que se aleguen por el interesado están basadas en razones de salud, vida sexual, violencia de género (art. 81.3 RLOPD). En este caso habrá que adoptar las medidas correspondientes de nivel alto para salvaguardar dichos datos.

Dado que es posible que no a todos los datos de carácter personal le sea aplicable unas medidas de seguridad de nivel medio o de nivel alto (en su caso), cabe recordar lo dispuesto en el art. 81.8 RLOPD:

> *8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de* ***un nivel de medidas de seguridad diferente al del sistema principal****,* ***podrán segregarse*** *de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.*

IV

Hay que poner de manifiesto por último que lo que se ha descrito es el sistema de medidas de seguridad establecido en la normativa española actualmente aplicable, constituida por la LOPD y el RLOPD. No obstante, el 25 de mayo de 2018 entrará en vigor 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, RGPD), en el cual no se contiene una "lista" o "relación" de medidas de seguridad que hayan obligatoriamente de adoptarse, sino que se parte de un principio diferente. Corresponde al responsable del tratamiento determinar y aplicar "*teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas,* ***[las] medidas técnicas y organizativas apropiadas*** *a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario".* Lo que supone, en definitiva, que corresponde al responsable realizar el análisis adecuado del riesgo de los tratamientos para determinar las medidas "técnicas y organizativas" necesarias.

El art. 32 RGPSD añade:

Seguridad del tratamiento

1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, ***el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo****, que en su caso incluya, entre otros:*

a) la seudonimización y el cifrado de datos personales;

b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;

d un proceso de verificación, evaluación y valoración regulares de

) *la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.*

2. Al ***evaluar la adecuación del nivel de seguridad*** *se tendrán particularmente en cuenta los riesgos que presente el tratamiento de datos, en particular como consecuencia de la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.*

3. La adhesión a un código de conducta aprobado a tenor del artículo 40 o a un mecanismo de certificación aprobado a tenor del artículo 42 podrá servir de elemento para demostrar el cumplimiento de los requisitos establecidos en el apartado 1 del presente artículo.

4. El responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable, salvo que esté obligada a ello en virtud del Derecho de la Unión o de los Estados miembros.

En definitiva, el RGPD determina que corresponde al responsable del tratamiento la responsabilidad del análisis de las circunstancias del tratamiento, para establecer las medidas necesarias al mismo que sean “oportunas y eficaces”.