



La consulta plantea diversas dudas sobre la aplicación de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (en lo sucesivo LOPD) en relación con una plataforma de depósito de documentos originales existente en la Administración Autonómica consultante, cuya finalidad es almacenar y custodiar los documentos electrónicos generados tanto por los ciudadanos (solicitudes) como por la Administración.

## I

Se consulta, en primer lugar, si es necesario declarar la plataforma como un fichero y, en este caso, cual sería su finalidad, ya que puede comprender todo tipo de documentos generados con motivo de los procedimientos tramitados por la Comunidad Autónoma.

El concepto de fichero se encuentra en el artículo 3 b) de la LOPD que lo define como *“todo conjunto organizado de datos de carácter personal, cualquiera que fuera la forma o modalidad de su creación, almacenamiento, organización y acceso.”*

El concepto de fichero debe ponerse en relación con el de responsable del mismo definido en la letra d) del artículo 3 de la LOPD como *“la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento.”*

Por tanto, es responsable del fichero quien decide su creación, contenido y finalidad, creación que, en el caso de las Administraciones públicas, debe hacerse por medio de disposición general publicada en el Boletín Oficial del Estado o Diario oficial correspondiente, de conformidad con lo previsto en el artículo 20 de la LOPD.

Dado que en la consulta se indica que los documentos electrónicos en los que se contienen datos personales *“no son tratados por la plataforma sino por los sistemas de información declarados en cada caso en los centros directivos que son los que procesan los datos”*, ese conjunto de documentos alojados en la plataforma no integrarían un nuevo fichero, sino que cada uno de ellos formaría parte de los ficheros creados por las diferentes Consejerías para el ejercicio de sus competencias, lo cual resulta conforme con el concepto de fichero contenido en el artículo 3 de la LOPD, para el cual, el dato esencial es

que se trate de un conjunto organizado de datos de carácter personal, esto es, un conjunto de datos personales estructurados y tratados para unos fines concretos, con independencia de la forma o modalidad de creación, almacenamiento, organización o acceso y, sería, de la misma manera, acorde con la definición de responsable del tratamiento, respondiendo a esta figura las diferentes Consejerías que han decidido la creación, contenido y uso de los ficheros.

En consecuencia, si como parece desprenderse de la consulta, la Consejería consultante tiene encomendada la gestión de la plataforma, limitándose su actuación a la prestación de un servicio de almacenamiento y custodia de los documentos, no tendría, respecto de los ficheros de otras Consejerías, la condición de responsable sino de encargado del tratamiento, a quien la letra g del artículo 3 de la LOPD configura como “la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, sólo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento.”

La existencia de un encargado del tratamiento viene delimitada por la concurrencia de dos características: la imposibilidad de decisión sobre la finalidad, contenido y uso del tratamiento y la inexistencia de una relación directa entre el afectado por el tratamiento y el encargado, que deberá en todo caso obrar en nombre y por cuenta del responsable como si la relación fuese entre éste y el afectado. En este sentido dispone el artículo 20.1 del Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, que “se considerará que existe comunicación de datos cuando el acceso tenga por objeto el establecimiento de un nuevo vínculo entre quien accede a los datos y el afectado”.

Para que la relación entre responsable y encargado del tratamiento pueda darse y se ajuste a la Ley, es preciso que se cumplan los requisitos expresados en el artículo 12 de la LOPD, considerando los siguientes aspectos:

En primer lugar, será preciso que la actuación del encargado del tratamiento se limite a la prestación de un servicio al responsable del fichero y que dicha relación de servicios se encuentre contractualmente establecida. En lo que atañe a los requisitos formales de este tipo de contratos, el artículo 12.2 de la LOPD impone que *“la realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento,*

*que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas”.*

El hecho de que la relación derivada del contrato sea la existente entre un responsable y un encargado del tratamiento implicará que al término de la relación sea aplicable lo establecido en el artículo 12.3 de la LOPD, de forma que *“una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento”.*

El incumplimiento de esta previsión llevará aparejada la consecuencia, prevista en el artículo 12.4 de la LOPD, de que *“En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado, también, responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente”.*

Esta Agencia Española de Protección de Datos ha venido indicando que el deber de devolución al que se refiere el artículo 12.3 de la LOPD podrá verificarse mediante la entrega directa de los datos al propio responsable del tratamiento o mediante la realización de dicha entrega al encargado del tratamiento que este designase, toda vez que en este segundo caso el encargado actuaría como mero mandatario del responsable, siendo precisamente éste el que establece a quién han de entregarse los datos en su nombre y por su cuenta. Y así se recoge en el artículo 20.3 del Reglamento antes citado *“no obstante, el encargado del tratamiento no incurrirá en responsabilidad cuando, previa indicación expresa del responsable, comunique los datos a un tercero designado por aquél, al que hubiera encomendado la prestación de un servicio conforme a lo previsto en el presente capítulo.”*

Por su parte, el artículo 22 del aludido Reglamento dispone respecto de la conservación de los datos lo siguiente:

*“1. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento o al encargado que éste hubiese designado, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.*

*No procederá la destrucción de los datos cuando exista una previsión legal que exija su conservación, en cuyo caso deberá procederse a la devolución de los mismos garantizando el responsable del fichero dicha conservación.*

*2. El encargado del tratamiento conservará, debidamente bloqueados, los datos en tanto pudieran derivarse responsabilidades de su relación con el responsable del tratamiento.”*

## II

En lo que se refiere a las medidas de seguridad que hayan de ser adoptadas por quienes realicen trabajos de tratamiento de datos por cuenta de tercero, habrán de ser, en principio, las mismas que las impuestas al responsable del fichero, tal y como se desprende de lo previsto en los artículos 9 y 12.2 de la Ley Orgánica.

De esta manera se aplicarán a cada documento las medidas de seguridad correspondientes al fichero del que forman parte, de conformidad con lo previsto en el Reglamento de desarrollo de la LOPD que las clasifica en diferentes niveles en función de la naturaleza de los datos tratados. No obstante debe recordarse aquí que el artículo 81.8 del citado Reglamento permite aplicar diferentes niveles de seguridad a un fichero o un sistema de información siempre que se den las condiciones que dicho precepto exige. Dispone dicho artículo: *“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.”*

Por último, debe tenerse en cuenta que el artículo 85 del Reglamento prevé respecto del acceso a datos a través de redes de comunicaciones que *“Las medidas de seguridad exigibles a los accesos a datos de carácter personal a través de redes de comunicaciones, sean o no públicas, deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local, conforme a los criterios establecidos en el artículo 80.”*