

La consulta plantea varias cuestiones, relativas a la tramitación de su procedimiento sancionador, invocando la Ley 27/2006, de 18 de julio por la que se regulan los derechos de acceso a la información de participación pública y de acceso a la justicia en materia de medio ambiente.

No obstante, del tenor de la consulta no se desprende cuestiones concretas respecto al derecho fundamental a la protección de datos de carácter personal y dado que la competencia de esta Agencia se circunscribe a la protección del mencionado derecho, tan sólo analizaremos las cuestiones de ese ámbito, en relación con la Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.

Por ello, podemos destacar que la solicitud de información de un particular en un procedimiento sancionador en el que no sea parte, supone desde el punto de vista de la protección de datos una cesión de datos de carácter personal, definida por el artículo 3 i) de la Ley Orgánica 15/1999, como “toda revelación de datos realizada a una persona distinta del interesado”.

Por otro lado, como bien razona el propio escrito de consulta, es preciso señalar, como punto de partida, que el artículo 11.1 de la Ley Orgánica 15/1999 dispone que “los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado”.

No obstante, el artículo 11.2 dispone que “El consentimiento exigido en el apartado anterior no será preciso:

- a) Cuando la cesión está autorizada en una Ley.
- b) Cuando se trate de datos recogidos de fuentes accesibles al público.
- c) Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
- d) Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la



comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.

e) Cuando la cesión se produzca entre Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.

f) Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.”

Teniendo en cuenta lo que se acaba de indicar, la comunicación de datos planteada, requerirá el consentimiento del interesado a menos que la misma pueda ampararse en alguno de los supuestos excepcionados por el citado artículo 11.2. y atendiendo a lo dispuesto en la consulta, podrá fundamentarse la excepción en la Ley 27/2006, pero siempre limitado a la finalidad de la misma.

Además es preciso destacar que la aplicación de la Ley Orgánica 15/1999, queda concretada respecto a los datos de carácter personal, pues así lo dispone el artículo 2.1, párrafo primero de la Ley Orgánica 15/1999 dispone que “la presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”, siendo datos de carácter personal, conforme al artículo 3 a) “Cualquier información concerniente a personas físicas identificadas o identificables”.

De dichos preceptos se deduce claramente que la protección conferida por la Ley Orgánica 15/1999 no es aplicable a las personas jurídicas, ni a otros conceptos que no estén vinculados a las personas físicas.

Por último respecto a las personas que pueden acceder a los expedientes sancionadores, es preciso destacar que el Real Decreto 1720/2007, de 21 de diciembre por el que se desarrolla la Ley Orgánica 15/1999, y que entrará en vigor el 19 de abril de este año dispone en el artículo 88 relativo al documento de seguridad que “1. El responsable del fichero o tratamiento elaborará 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.

2. El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado



para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

3. El documento deberá contener, como mínimo, los siguientes aspectos:

a) Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.

b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.

c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan

e) Procedimiento de notificación, gestión y respuesta ante las incidencias.

f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.

g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

4. En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

a) La identificación del responsable o responsables de seguridad.

b) Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento.

5. Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

6. En aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad. Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados.

En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

7. El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos

realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

8. El contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.”

En consecuencia, la concreción de quienes pueden acceder a los expedientes sancionadores es una cuestión de organización interna de la entidad que deberá reflejarse en el documento de seguridad. Mas concretamente respecto del control de acceso el artículo 91 del citado Reglamento señala que “1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.

2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.

3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.

4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.

5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.”

En cuanto a los ficheros no automatizados, indicar que las medidas de seguridad a adoptar en los mismos se encuentran recogidas en el artículo 105 y siguientes del Real Decreto 1720/2007.