

La consulta plantea si resulta conforme con lo dispuesto por la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de datos de Carácter Personal, la cesión por parte de los Órganos de Gobierno de una comunidad de propietarios, a los propietarios que así lo soliciten, de la documentación relativa a la gestión y administración del inmueble.

La comunicación a los diferentes propietarios, por parte de los Órganos de Gobierno de la comunidad, de dichos documentos, en la medida en que éstos contengan datos de carácter personal, implicará 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”.

En relación con esta cuestión, el artículo 11.1 de la citada Ley 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”*, estableciendo en el artículo 11.2 una serie de excepciones que, a los efectos que interesan en el presente supuesto, quedan limitadas a la contenida en el apartado a) que prevé la posibilidad de cesión incontestada *“cuando la cesión esté autorizada por una Ley”*.

Por ello, sólo será posible admitir la cesión de los datos sin consentimiento del interesado en aquellos supuestos en los que exista una norma con rango de Ley, que habilite esta cesión.

A este respecto, el artículo 14 de la Ley 49/1960, de 21 de julio, sobre Propiedad Horizontal, establece que *“Corresponde a la Junta de propietarios: b) Aprobar el plan de gastos e ingresos previsibles y las cuentas correspondientes” y c) Aprobar los presupuestos y la ejecución de todas las obras de reparación de la finca sean ordinarias o extraordinarias, y ser informada de las medidas urgentes adoptadas por el administrador de conformidad con lo dispuesto en el artículo 20.c).”*

A su vez el artículo 20 de la misma Ley dispone que *“Corresponde al administrador: e) Actuar, en su caso, como secretario de la Junta y custodiar a disposición de los titulares la documentación de la comunidad”*.

Por ello, la cesión de datos personales que puede derivarse de la consulta se encontraría amparada por el artículo 11.2 a) de la Ley Orgánica 15/1999, por cuanto existe una norma con rango de Ley que establece que la documentación de la comunidad estará “a disposición” de los titulares, siendo

lícita la transmisión de los datos cuando la finalidad que justifique la comunicación de dicha documentación a los propietarios solicitantes se encuentre amparada por la Ley de Propiedad Horizontal. A dichos efectos, la consultante deberá estar al estricto cumplimiento de lo dispuesto por el artículo 4.2 de la Ley Orgánica 15/1999, que exige que los datos sean tratados únicamente para las finalidades que motivaron su recogida, en el presente caso, conocer y comprobar la correcta gestión de las cuentas de la comunidad, función atribuida a la Junta de propietarios por el artículo 14 de la Ley 49/1960, sin que quepa emplear los datos personales que en la documentación se contengan para finalidades distintas de la mencionada.

Debe tenerse en cuenta, asimismo, que el artículo 10 de la Ley 15/1999 sujeta al responsable del fichero, esto es a la propia comunidad de propietarios, a un deber de secreto, deber al que se encuentran igualmente sometidos los propietarios como miembros de la Junta de propietarios. Dispone dicho artículo 10 que *"El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo."*

En lo que se refiere a la forma en que puede darse acceso a dicha documentación, debe recordarse que la Ley Orgánica 15/1999 impone al responsable del fichero o tratamiento, la adopción de las medidas de seguridad a que se refiere el artículo 9 de la LOPD:

*"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 estén expuestos, ya provengan de la acción humana o del medio físico o natural."*

El Reglamento de desarrollo de la Ley Orgánica 15/1999, aprobado por Real Decreto 1720/2007, de 21 de diciembre, constituye en la actualidad la normativa vigente en materia de medidas de seguridad aplicables a los tratamientos de datos de carácter personal. El artículo 80 de esta norma clasifica las medidas de seguridad aplicables a los ficheros o tratamientos de datos en tres niveles, debiendo adoptarse, en cada caso, el nivel correspondiente en función de la naturaleza de los datos a tratar. Debe tenerse presente, además, que dichas medidas tienen un carácter acumulativo, de forma que las establecidas para cada nivel exigen incorporar las previstas para los niveles inferiores.

Estas medidas consisten, de conformidad con lo dispuesto en el mismo Reglamento, en la elaboración de un documento de seguridad que recoja las

medidas de índole técnica y organizativa acordes con la normativa de seguridad vigente, especificando entre otros aspectos: el ámbito de aplicación del documento, las medidas y procedimientos encaminados a garantizar el nivel de seguridad exigido, las funciones y obligaciones del personal, los procedimientos de notificación, gestión y respuesta ante las incidencias, la gestión de soportes o documentos y los procedimientos de realización de copias de respaldo y de recuperación.

De la consulta parece desprenderse que nos hallamos ante un fichero no automatizado al que serán aplicables, además de las disposiciones generales para todo tipo de ficheros y las normas específicas en materia de medidas de seguridad previstas para ficheros no automatizados, aquellas normas relativas a ficheros automatizados a que hace referencia el artículo 105 del Reglamento, interesando especialmente en el presente caso las medidas relativas a la gestión de soportes a que se refiere la letra d) del apartado segundo de dicho artículo.

Por consiguiente, al supuesto que nos ocupa resulta aplicable lo previsto al respecto en el artículo 92 del Reglamento, que establece en sus números 2, 3 y 4 lo que a continuación se transcribe:

*“2. La salida de soportes y documentos que contengan datos de carácter personal, incluidos los comprendidos y/o anejos a un correo electrónico, fuera de los locales bajo el control del responsable del fichero o tratamiento deberá ser autorizada por el responsable del fichero o encontrarse debidamente autorizada en el documento de seguridad.*

*3. En el traslado de la documentación se adoptarán las medidas dirigidas a evitar la sustracción, pérdida o acceso indebido a la información durante su transporte.*

*4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado, mediante la adopción de medidas dirigidas a evitar el acceso a la información contenida en el mismo o su recuperación posterior.”*

Igualmente, el artículo 87 del Reglamento prevé, con carácter general para todo tipo de ficheros, en relación con los ficheros temporales o copias de trabajo de documentos que *“1. Aquellos ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios establecidos en el artículo 81.*

*2. Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación”*

Por último, si los ficheros contienen datos personales a los que deban aplicarse medidas de seguridad de nivel alto, deberá asimismo tenerse en cuenta lo previsto en el artículo 112 , según el cual *“La generación de copias o la reproducción de los documentos únicamente podrá ser realizada bajo el control del personal autorizado en el documento de seguridad.”* Dispone asimismo en su número segundo que *“Deberá procederse a la destrucción de las copias o reproducciones desechadas de forma que se evite el acceso a la información contenida en las mismas o su recuperación posterior.”*

Debe igualmente tomarse en consideración que el artículo 114 requiere que se adopten *“medidas dirigidas a impedir el acceso o manipulación de la información objeto de traslado”*, siempre que se proceda al traslado físico de la documentación contenida en un fichero, de manera que se garantice la confidencialidad de la información contenida en los mismos.