Guía Práctica sobre Protección de Datos para ADMINISTRADORES DE FINCAS y COMUNIDADES DE PROPIETARIOS

Administrador Fincas Colegiado

GrupoIWI protección de datos

grupoiwi.com

Administrador Fincas Colegiado

GrupoIWI protección de datos

Guía Práctica sobre Protección de Datos para **ADMINISTRADORES DE FINCAS** y **COMUNIDADES DE PROPIETARIOS**

Conforme al Reglamento Europeo
de Protección de Datos 679/2016 (RGPD)
y a la Ley Orgánica 3/2018, de 5 de diciembre,
de Protección de Datos Personales
y Garantía de los Derechos Digitales (LOPD-GDD)

índice

La presente guía recoge una serie de explicaciones y situaciones que tienen incidencia en Protección de Datos y que se pueden producir en las relaciones entre los administradores de fincas y sus administrados, proveedores externos de la comunidad, trabajadores, miembros de la Junta, etc.

El colectivo de administradores de fincas tiene unas características particulares que justifican el que su actividad sea objeto de una especial atención. Cuando los administradores de fincas intervienen en la gestión de los asuntos de las comunidades de propietarios asumen unas funciones de asesoramiento y consultoría que se extienden también al ámbito de la protección de los datos que las comunidades manejan.

Desde un punto de vista práctico, hemos analizado las situaciones más comunes que se pueden presentar, con ejemplos y explicaciones sobre cómo resolver dichas situaciones, siendo el objetivo de esta guía facilitar la tarea de los administradores de fincas, contribuyendo a mejorar el nivel de protección de los datos personales que manejan en el desempeño de sus funciones y, a su vez, de las comunidades de propietarios que gestionan.

Se ha tenido en cuenta la actual normativa sobre protección de datos derivada de 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 (RGPD), y de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPD-GDD).

1 ADMINISTRADORES DE FINCAS, COMUNIDADES DE PROPIETARIOS Y LA PROTECCIÓN DE DATOS PERSONALES

Los administradores de fincas, dentro de los servicios que prestan a las comunidades de propietarios, tienen acceso a numerosa información de carácter personal necesaria para la gestión ordinaria de las mismas relativa a propietarios, empleados, proveedores, etc.

> “A los efectos de la normativa sobre protección de datos, la comunidad de propietarios tiene la consideración de “responsable del tratamiento”, mientras que el administrador o gestor de la finca tendrá la consideración de “encargado del tratamiento”.

Precisamente es su condición de encargado del tratamiento, lo que legitima al administrador de fincas para tratar datos de carácter personal cuando actúa por cuenta de la comunidad. En el caso de las comunidades de propietarios, la legitimación la encontramos en la obligación legal de cumplir con la Ley de Propiedad Horizontal (LPH).

Por tanto, el administrador de fincas es un mero encargado que actúa en nombre y por cuenta de la comunidad que le ha contratado, siempre que no se exceda de sus funciones, como veremos más adelante, incluso aun en el caso de que la documentación de la comunidad se encuentre en su despacho profesional, lo cual ocurrirá en la mayoría de las ocasiones. Si bien el administrador de fincas, como encargado del tratamiento, deberá asesorar a la comunidad en el cumplimiento de la normativa de protección de datos y ser partícipe en la aplicación de las medidas encaminadas a conseguir ese cumplimiento.

2 ¿DEBEN CUMPLIR LAS COMUNIDADES DE PROPIETARIOS CON LA NORMATIVA DE PROTECCIÓN DE DATOS?

La respuesta es clara, ¡por supuesto que sí! Las comunidades de propietarios realizan diversos tratamientos de datos personales tanto de los propietarios como de terceros con los que la comunidad se relaciona: nombres y apellidos, direcciones postales, teléfonos de contacto, números de DNI, direcciones de correo electrónico, etc.

Desde 2002, año en que comenzamos a prestar nuestros servicios de consultoría en protección de datos, no son pocas las ocasiones en las que nos hemos encontrado reticencias por parte de administradores de fincas o por parte de los propios presidentes para admitir la obligatoriedad de esta normativa para las comunidades de propietarios.

> "Existe una idea equivocada que supone que estas obligaciones son para empresas y autónomos o asocian esta obligación a actividades económicas o de negocio, y entienden que las comunidades de propietarios no constituyen actividad empresarial y, por lo tanto, no deben cumplir con la normativa sobre protección de datos.

Desde nuestro departamento jurídico, os aseguramos que esta creencia **no es correcta**, y no es que sea una opinión o criterio nuestro, si no que dicha afirmación se basa en el articulado del Reglamento General de Protección de Datos (RGPD) de la Unión Europea, la Ley Orgánica de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), y en los propios informes y resoluciones de la Agencia Española de Protección de Datos (AEPD).

3 ¿QUÉ DEBEN HACER LAS COMUNIDADES DE PROPIETARIOS PARA CUMPLIR CON LA PROTECCIÓN DE DATOS?

Las comunidades de propietarios poseen datos personales generados por la propia llevanza de los asuntos de la comunidad, por tanto, todas deberán cumplir, entre otras, con las siguientes obligaciones:

3.1 Identificar los tratamientos de datos personales

El tratamiento más usual de una comunidad de propietarios es el que incorpora información con los datos de carácter personal de las personas físicas integrantes de la propia comunidad, es decir, los propietarios.

Este tratamiento incluye normalmente: nombres y apellidos, teléfonos de contacto, direcciones postales, números de DNI, direcciones de correo electrónico, datos bancarios. Suele denominarse a este tratamiento **"gestión de la comunidad de propietarios"** o **"propietarios"**, y la comunidad se sirve de él para su gestión contable, fiscal y administrativa, asegurando el cumplimiento por los propietarios de las obligaciones impuestas por la LPH y el ejercicio de los derechos que corresponden a los copropietarios en la comunidad.

Asimismo, si la comunidad tiene trabajadores/as contratados dispondrá de un tratamiento relativo a **"recursos humanos"** o **"trabajadores"**, referente a los datos necesarios para la formalización y el mantenimiento de la relación laboral.

De igual modo, si la comunidad de propietarios aprueba la instalación de sistemas de cámaras o videocámaras, dando lugar al tratamiento de imágenes de personas físicas identificadas o identificables, existiría un tratamiento que se puede denominar **"videovigilancia"**, cuya finalidad principal es la seguridad y control de accesos y/o vigilancia de las instalaciones y elementos comunes del inmueble.

3.2 Elaborar un registro de actividades de tratamiento

Las comunidades de propietarios, una vez identificados los tratamientos de datos que llevan a cabo, deben llevar por escrito un registro de las actividades de tratamiento que efectúan, el cual contendrá la siguiente información:

- Nombre y datos de contacto del responsable (o de su representante).
- Fines del tratamiento.
- Categorías de datos personales.
- Categorías de afectados.
- Descripción de las medidas técnicas y organizativas de seguridad, cuando sea posible.
- Categorías de destinatarios de comunicaciones, incluidos terceros países u organizaciones internacionales.
- Transferencias internacionales (en su caso).
- Cuando sea posible, plazos previstos para las supresión de las diferentes categorías de datos.

Este registro de actividades deberá estar a disposición de la Agencia Española de Protección de Datos si lo solicita.

3.3 Regular la relación entre la comunidad de propietarios y el administrador de fincas

Para que la relación entre comunidad de propietarios -responsable- y el administrador -encargado del tratamiento- se ajuste a la normativa de protección de datos, es preciso que

la relación contractual conste por escrito, o en alguna otra forma que permita acreditar su celebración y contenido, según el Art. 28 del RGPD, así como el título V, Capítulo I y II de la LOPD-GDD.

Dicho contrato deberá contener, como mínimo, el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable.

En particular, el contrato de encargo de tratamiento establecerá que el administrador debe:

- Tratar los datos únicamente siguiendo las instrucciones del responsable.
- Garantizar que tanto él como el personal que trabaje para él, se compromete a respetar la confidencialidad en el tratamiento de los datos personales.
- Tomar todas las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado.
- Asistir a la comunidad en el cumplimiento de su obligación de responder a las solicitudes de ejercicio de los derechos de los interesados.
- Devolver a la comunidad, al finalizar su relación, todos los soportes y/o documentos en los que consten datos de carácter personal objeto de tratamiento.
- Ayudar a la comunidad en el cumplimiento de sus obligaciones en aquellos supuestos en que se produzca una brecha de seguridad.

Si el administrador de fincas incumple las obligaciones recogidas en el contrato de encargo destinando los datos a otra finalidad que no sea la recogida en el mismo, se le podrá considerar responsable del tratamiento, respondiendo personalmente de las posibles infracciones.

El uso de los datos personales tratados para cualquier otra gestión o servicio distinto de los encomendados por la LPH, deberá contar con el consentimiento específico, informado e inequívoco de los afectados.

3.4 Cumplir con el deber de información

La comunidad de propietarios, como responsable del tratamiento, debe informar a los afectados, que pueden ser propietarios, empleados de la comunidad u otras personas físicas de las cuales trata datos personales, conforme a lo establecido por los Arts. 13 y 14 de RGPD, ya sea mediante carteles informativos o con cláusulas en documentos de recogida de información a los interesados.

A grandes rasgos, dicha información contendrá la identidad y datos de contacto del responsable del tratamiento, finalidad y base jurídica del mismo, así como una referencia a los derechos que tienen reconocidos los afectados y su ejercicio.

3.5 Atender los derechos de protección de datos

El RGPD permite a los afectados ejercitar los derechos de acceso, rectificación, supresión ("derecho al olvido"), oposición, portabilidad, limitación del tratamiento y derecho de oposición a las decisiones automatizadas (incluyendo la elaboración de perfiles).

Estos derechos se ejercitarán ante la comunidad de propietarios como responsable del tratamiento. Ahora bien, también es posible, y lo habitual, que sea el administrador de fincas quien se encargue de su gestión.

3.6 Implantar medidas de seguridad adecuadas

Aunque lo más frecuente en las comunidades de propietarios es que sea el propio administrador quien se encargue de la custodia de la documentación de la comunidad en su despacho profesional, hay ciertas medidas organizativas y técnicas que deben ser tenidas en cuenta por los miembros de la comunidad, especialmente por su presidente dadas las funciones de su cargo y su participación en el tratamiento de los datos personales:

- Si el ordenador se usa tanto para la gestión de la comunidad como para uso personal, disponer de 2 perfiles de usuario diferentes.
- Asegurarse de que el acceso a los datos personales requiere el uso de una contraseña.
- Mantener los ordenadores y otros dispositivos utilizados para las gestiones de la comunidad actualizados en la medida de lo posible, utilizando un antivirus para reducir el riesgo de robo y destrucción de la información y de los datos personales.
- Informar de sus obligaciones a otros miembros de la Junta así como, en su caso, a los trabajadores de la comunidad sobre su deber de confidencialidad en relación a los datos personales que conozcan en el desarrollo de sus funciones.

Controlar los accesos a la información de carácter personal de forma que no se produzcan accesos por parte de terceros no autorizados.

4 ¿DEBEN ADAPTARSE LOS ADMINISTRADORES DE FINCAS A LA NORMATIVA SOBRE PROTECCIÓN DE DATOS?

Parece evidente que lo expuesto anteriormente para las comunidades de propietarios, es igualmente aplicable a los despachos profesionales dedicados a la administración de fincas.

Por eso, las principales obligaciones para los administradores de fincas en materia de protección de datos van a ser similares a las de una comunidad, pero con las peculiaridades correspondientes a su actividad profesional.

4.1 Identificación de los tratamientos

El administrador de fincas, en su gestión diaria, se sirve de diferentes tipos de datos de carácter personal con los que realiza diversos tratamientos, respecto a los cuales tendrá la consideración de responsable del tratamiento.

El tratamiento más usual será el de la "prestación del servicio" referente a los clientes (comunidades de propietarios) que gestiona y del cual se sirve para llevar a cabo su servicio así como su gestión contable, fiscal y administrativa. Además, si tiene trabajadores contratados realizará un tratamiento relativo a "recursos humanos" o "trabajadores", como pudimos ver anteriormente cuando hablamos de las obligaciones de las comunidades.

En todo caso, habrá que analizar en profundidad al administrador de fincas, análisis que podrá determinar si dispone de otros tratamientos, como proveedores, comunicaciones comerciales, videovigilancia, curriculums, etc., ya que, a diferencia de lo que ocurre habitualmente

con las comunidades de propietarios, los tratamientos de datos personales llevados a cabo por un administrador son más variados.

4.2 Registro de las actividades de tratamiento

Una vez identificados los tratamientos, de igual manera que las comunidades de propietarios, los administradores de fincas deberán proceder a realizar el registro de actividades de tratamiento por escrito o digital, con el mismo contenido que hemos visto anteriormente.

Además, el administrador de fincas como encargado del tratamiento también tendrá que configurar un registro de actividades de tratamiento en relación con las comunidades a las que presta su servicio, es decir, que además del registro con el contenido ya visto, deberá tener otro en el que se recojan todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable (comunidad) conforme al Art. 30 del RGPD.

4.3 Firma del contrato entre la comunidad de propietarios y el administrador de fincas

Como ya hemos visto, es preciso que la relación contractual entre la comunidad y el administrador conste por escrito o en alguna otra forma que permita acreditar su celebración y contenido según el Art. 28 del RGPD, así como el Título V, Capítulo I y II de la LOPD-GDD.

Para el administrador no se trata de una cuestión baladí ya que el contrato de encargo de tratamiento es el documento por el cual el administrador de fincas se configura como encargado del tratamiento y, por tanto, puede usar los datos responsabilidad de la comunidad de propietarios para el desempeño de las funciones encomendadas. Fuera de este contrato, todo tratamiento de datos personales deberá contar con el consenti-

miento de los interesados o cualquier otra base de legitimación, que deberá ser demostrable por el administrador.

4.4 Deber de informar

El administrador de fincas, en el ejercicio de su actividad profesional, tiene la obligación de informar a los interesados sobre las circunstancias relativas al tratamiento de sus datos personales en el mismo momento en que se obtienen dichos datos, si es que los datos se obtienen directamente del interesado. Es por ello que es aconsejable que en la hoja de encargo o contrato de prestación de servicios, se incluyan textos legales sobre el deber de informar en materia de protección de datos, donde entre otras cosas se indicará quién es el responsable del tratamiento, la finalidad del mismo, los derechos que la normativa reconoce a los interesados o el plazo de conservación de los datos. También podría informarse mediante un documento específico, lo importante, en todo caso, es informar y poder acreditar que se hizo conforme al Art. 13 del RGPD. Si los datos no se obtienen directamente del interesado, habrá que atender a lo dispuesto por el Art. 14 del RGPD.

4.5 Implantar las medidas de seguridad apropiadas

El RGPD se caracteriza por la proactividad, de manera que tanto responsables como encargados, y ya hemos visto que el administrador tiene esta doble faceta, aplicarán las medidas técnicas y organizativas apropiadas para garantizar y demostrar que el tratamiento de datos personales se lleva a cabo de conformidad con la norma. Tales medidas se revisarán regularmente para valorar su eficacia y se actualizarán cuando sea necesario.

El administrador de fincas deberá:

- Recoger sólo los datos personales adecuados, pertinentes y limitados a lo necesario en relación para con las finalidades de que se trate, siempre relativas a la gestión ordinaria de asuntos de la comunidad de propietarios.
- Tratar los datos de los propietarios y de aquellos otros interesados de los que tenga conocimiento de forma lícita, leal y transparente.
- No usar los datos ulteriormente para finalidades incompatibles con aquellas para los que se obtuvieron.
- No conservar los datos personales por un tiempo mayor del necesario para los fines del tratamiento.
- Implantar las medidas necesarias para garantizar una seguridad adecuada de los datos personales.

5 LA **FIGURA DEL PRESIDENTE** EN LAS **COMUNIDADES DE PROPIETARIOS**

Fotograma de la serie "La que se avecina" de TeleCinco

Para empezar a analizar las implicaciones que tiene la protección de datos respecto al cargo de presidente de una comunidad de propietarios, debemos acudir a la Ley de Propiedad Horizontal para conocer sus atribuciones:

- Representar a la Comunidad en todos los asuntos que le afecten, tanto en juicio como fuera de él, ya sea para la reclamación de cuotas atrasadas, o de otra naturaleza.
- Desempeñar las funciones de secretario y administrador, salvo que los estatutos o la Junta dispongan la designación de estos cargos separadamente.
- Convocar Junta ordinaria al menos una vez al año, y cerrar el acta de la misma.
- Presidir las Juntas tanto ordinarias como extraordinarias.
- Ejecutar y hacer cumplir los acuerdos de la Junta de Propietarios.
- Contratar servicios de carácter urgente.

Resulta evidente que el presidente, dentro de sus funciones, accede a datos de carácter personal relacionados con su cargo. Es decir, como representante y miembro principal de la Junta, puede tener acceso y gestionar toda la documentación relativa a la llevanza de los asuntos relacionados con la comunidad.

Los datos personales deben ser solamente los adecuados, pertinentes y limitados a lo necesario para los fines propios de dicha comunidad, es decir, sólo los relacionados con la llevanza de los asuntos de la comunidad. Así, por ejemplo, suele ser habitual que los propietarios faciliten su dirección de email para comunicarse directamente con el administrador de fincas y, en este sentido, no creemos que sea un dato que el presidente tenga porque manejar. No obstante, si los propietarios ceden dicha información al presidente, será por su cuenta y riesgo.

Entre esa documentación por supuesto que se encontrará todo lo relacionado con los co-propietarios, pero también es posible que se refiera a cuestiones laborales, es decir, nóminas, contratos, seguros sociales, cuadrantes de horarios, etc., de los trabajadores de la comunidad, cuando los haya. Lo mismo pasa con los trabajadores subcontratados, con más razón si cabe por las exigencias de la Ley de Subcontratación y el Estatuto de los Trabajadores que proclaman que el empresario principal, esto es, la comunidad de propietarios, responderá solidariamente de las obligaciones de naturaleza salarial contraídas por los contratistas y subcontratistas con sus trabajadores (Art. 42 del ET). Ahora bien, hay que tener en cuenta que, junto a esta información, aparecerán otros datos como el domicilio, el número de cuenta bancaria donde se hacen los pagos e, incluso, datos especialmente protegidos referidos a salud o afiliación sindical; estos datos no son relevantes para controlar la gestión de la comunidad y el acceso a los mismos sin autorización supondría una vulneración de la normativa de protección de datos.

> **“En definitiva, el presidente debe ser consciente de las obligaciones de deber de secreto y diligencia que tiene en relación al acceso y utilización de dichas informaciones, es decir, que deberá guardar estricta confidencialidad respecto a aquellos asuntos, informaciones, datos personales, formas de deliberación en la adopción de acuerdos, etc., a los que tenga acceso en virtud de su cargo.**

En ningún caso se puede desvelar información a terceras personas, ni siquiera a otros propietarios, ya sea a través de una conversación, o por medios electrónicos como, por ejemplo, el reenvío de e-mails, salvo que haya una habilitación legal para ello o se tenga el consentimiento expreso de los afectados.

No podemos olvidar que toda persona que se entromete en la vida íntima o personal, o bien, en ámbitos de privacidad de otros, sin el correspondiente consentimiento de éstos, vulnera el derecho fundamental a la intimidad de la persona afectada en cuanto a la revelación y descubrimiento de secretos. El derecho a la intimidad está recogido en el artículo 18 de la Constitución Española, junto al derecho al honor y el derecho a la propia imagen, y se vincula a la esfera privada de la personas. La transgresión de estos derechos pueden ser constitutivos, incluso, de delito penal.

Independientemente de las posibles consecuencias y/o acciones penales que puede tener este tipo de conductas, en materia de protección de datos, la persona afectada y perjudicada puede emprender acciones legales denunciando ante la Agencia Española de Protección de Datos la situación concreta o la supuesta transgresión del deber de secreto, como, por ejemplo, cuando públicamente se facilita información sobre datos personales, situaciones, peticiones o conflictos de vecinos, o bien cuando se reenvían a terceras personas emails propios o ajenos... De hecho, el propio RGPD recoge el derecho de toda persona que haya sufrido daños y perjuicios, tanto materiales como inmateriales, a causa de una infracción de la normativa de protección de datos, a recibir del responsable o del encargado del tratamiento una indemnización por los daños y perjuicios sufridos (Art. 82.1 RGPD).

Debemos indicar que la Agencia Española de Protección de Datos siempre sancionará al responsable del tratamiento, es decir a la comunidad de propietarios, todo ello, evidentemente, sin perjuicio de las posibles acciones civiles y penales que puedan dirigirse posteriormente contra la persona que haya tenido tal conducta.

6 **CUESTIONES PRÁCTICAS** EN MATERIA DE PROTECCIÓN DE DATOS **PARA COMUNIDADES DE PROPIETARIOS**

En el día a día de las comunidades de propietarios, los presidentes y por ende, los administradores que gestionan la comunidad, se encuentran con cuestiones que afectan, y en gran medida, a la protección de datos. Dichas cuestiones precisan de una respuesta adecuada por parte de consultores especializados en esta materia. No son pocas las consultas que nos llegan cuando existen conflictos vecinales o cuando se llevan a cabo acciones que afectan a la protección de datos. Como ejemplo de todas estas cuestiones prácticas podemos enumerar las siguientes: morosidad, videovigilancia, acceso a la información, cesión de datos a terceros, etc.

Resulta evidente que hoy día, la correcta implantación y adecuación a la normativa en materia de protección de datos, no consiste únicamente en cumplir con una serie de obligaciones formales, sino que se requiere de un constante análisis y, en su caso, actualización, así como asesoramiento inmediato ante posibles conflictos, denuncias, peticiones de vecinos o terceras personas, en relación a la protección de datos o a aquellas situaciones en las que los administradores de fincas o presidentes piensen que pueden tener relación con esta materia. Esto es básico para cumplir con los principios de proactividad y protección de datos desde el diseño y por defecto que impone el RGPD.

6.1 Acceso a la información por parte de los propietarios

Es frecuente que los vecinos insistan a los Presidentes o a los Administradores de Fincas, para obtener acceso a información titularidad de la comunidad de propietarios, como, por ejemplo, acceder u obtener copia de contratos de suministros, nóminas o contratos de los empleados de la comunidad, a datos personales de otros vecinos como teléfono o e-mails, acceder al visionado de las cámaras de videovigilancia, etc.

Este tipo de acceso y obtención de copias por parte de los copropietarios puede responder a distintas finalidades, como, por ejemplo, conocer y comprobar la correcta gestión de la comunidad por parte del presidente o del administrador de fincas, o comprobar el contenido, alcance o coberturas de determinados contratos de prestación de servicios con proveedores de la comunidad.

Esta situación tan típica en las comunidades se encuentra fuera de los casos en los que la LPH obliga a la comunicación de datos a los comuneros, pero se entiende que puede existir un interés legítimo, que es la de corroborar la correcta administración y gestión de la finca.

El caso es que en la documentación de la comunidad de propietarios pueden encontrarse numerosas informaciones que pueden ser de carácter personal, tales como datos identificativos y de contacto de los propietarios, números de sus cuentas corrientes, coeficientes de participación, consumos individuales, ingresos efectuados por los propietarios o deudas que éstos mantengan con la comunidad, sentido del voto en la adopción de acuerdos, etc. Igualmente tendrá dicha consideración cualquier dato personal referido a los empleados que pudiera tener la comunidad de propietarios, como también la tendrán los datos relativos a honorarios de profesionales que abone la comunidad.

Centrándonos en los tratamientos de datos personales contenidos en los documentos que emplea la propia comunidad, estos pueden abarcar un amplio espectro de información personal relativa, incluso, a la vida privada y familiar de los afectados, así como a cualquier tipo de actividad desarrollada por una persona, como la referida a sus relaciones laborales o a su actividad económica o social.

La propia LPH posibilita el acceso a esta información, que a efectos del RGPD se encontraría legitimado en base al cumplimiento de una obligación legal. Así, el Art. 16.2 LPH regula cómo debe efectuarse la convocatoria de las Juntas, disponiendo que la convocatoria contendrá una relación de los propietarios que no estén al corriente en el pago de las deudas vencidas a la comunidad y advertirá de la privación del derecho de voto si se dan los supuestos previstos en el Art. 15.2 LPH. Por su parte, el Art. 19 de la misma ley prevé la remisión de las actas a los propietarios, señalando en su apartado segundo las menciones que deben contener, entre las que figuran diversos tipos de datos de carácter personal.

> “Pero, sin perjuicio de que puedan realizarse estas comunicaciones, se tiene que tener en consideración que deberán, en todo caso, respetar los principios del RGPD, sobre todo el principio relativo a la minimización de datos, recordando que toda comunicación de datos deberá limitarse a aquellos que, en cada caso, resulten “adecuados, pertinentes y limitados” para el cumplimiento de la finalidad que legitima el acceso a los mismos, que en estos supuestos viene referido al control del buen gobierno de la comunidad.

Así, a título de ejemplo, no cumple el requisito de idoneidad la comunicación de los directorios con los datos de domicilio de los propietarios o sus números de cuenta corriente, ya que en nada contribuyen a la finalidad de control de la buena administración de la comunidad de propietarios.

Igualmente, y en lo que se refiere a las nóminas de los empleados de la comunidad, debe tenerse en cuenta que, junto con la información referida a sus retribuciones, aparecerán otros datos, como el domicilio, la cuenta corriente de abono e, incluso, categorías especiales de datos referentes a salud o ideología, así como el descuento, en su caso, de la cuota sindical de los afiliados a un sindicato.

Estos datos no resultan relevantes para la finalidad de control de la gestión de la comunidad de propietarios, por lo que la exhibición de dichos directorios o de las nóminas, resultará contraria al principio de proporcionalidad y, en consecuencia, darán lugar a una vulneración de la normativa de protección de datos, sin perjuicio de que se deba informar a los propietarios de las retribuciones satisfechas a los empleados, con el adecuado desglose de conceptos retributivos.

Por todo ello, no existe una respuesta común a todos los supuestos en este sentido, por lo que podemos concluir que no se permite un acceso generalizado a toda la documentación obrante en los archivos de la comunidad que pueda contener datos personales, sino que habrá que analizar cada caso y sólo se dará acceso a aquellos datos que sean estrictamente pertinentes, adecuados y limitados en relación con los fines para los que son tratados y con la debida justificación de la solicitud, examinando en cada caso si se cumple con el principio de proporcionalidad, y si resulta idóneo, necesario y equilibrado para obtener la finalidad perseguida.

> “Deberá existir una causa objetiva, como sería recopilar toda la información necesaria para estudiar los temas a aprobar en una Junta de propietarios; en otro caso, no procederá el acceso directo al documento.

En cuanto a la obtención de copias, la LPH recoge varios supuestos en los que es obligatoria la remisión de determinados documentos, como ocurre con las actas de las Juntas de propietarios, pero en principio, el Art. 20 letra 3 de la LPH, habla de la obligación del administrador de custodiar a disposición de los titulares la documentación de la comunidad, por lo que en caso de solicitar copia de un documento, habrá que atender a la oportunidad y proporcionalidad de dicha copia, teniendo en cuenta las limitaciones derivadas de la aplicación de la normativa de protección de datos (medidas de seguridad, gestión y salida de documentos, etc.).

Podemos poner como ejemplo un cuadro general explicativo de tipos de documentos que puede manejar una comunidad de propietarios, pero insistimos en que habrá que analizar cada petición en concreto y la finalidad con la que se solicita.

EJEMPLOS DE ACCESO A INFORMACIÓN Y/O COPIA DE DOCUMENTOS DE LA COMUNIDAD DE PROPIETARIOS

DOCUMENTO	ACCESO	COPIA	EXPLICACIÓN
Actas de Juntas	Sí	Sí	El acta de las reuniones debe remitirse obligatoriamente a los propietarios conforme a la LPH
Facturas de proveedores	Sí	Sí	
Contratos de suministros de proveedores	Sí	Depende	Para controlar el buen gobierno de Administrador, saber el importe pagado, etc., sería suficiente con el acceso, si además quiere consultar el contenido/ condiciones /coberturas del contrato sí podría llevarse copia, nunca el original
Datos personales: Nombre y apellidos	Sí	Sí	Existe un interés legítimo de un propietario de conocer el nombre y apellidos del resto de propietarios
Datos personales: Teléfonos	No	No	
Datos personales: Datos bancarios	No	No	
Datos personales: Email	No	No	
Imágenes de cámaras de seguridad	No	Depende	Las imágenes sólo las verá el personal autorizado por la comunidad
Contratos de trabajo de los empleados de la Comunidad de Propietarios	Sí	No	Sólo cuando se hayan tomado precauciones para evitar que se vean datos no necesarios como domicilio particular, datos bancarios, nº de la seguridad social
Nóminas de los empleados de la Comunidad de Propietarios	Sí	No	Sólo cuando se hayan tomado precauciones para evitar que se vean datos no necesarios como domicilio particular, datos bancarios, nº de la seguridad social
Seguros sociales de los empleados de la Comunidad de Propietarios	Sí	No	Sólo cuando se hayan tomado precauciones para evitar que se vean datos no necesarios como domicilio particular, datos bancarios, nº de la seguridad social

DOCUMENTO	ACCESO	COPIA	EXPLICACIÓN
Currículum de candidatos	No	No	
Datos de morosidad	Sí	No	Sólo en momentos oportunos como en vísperas de la convocatoria de las juntas o cuando se haya aprobado por mayoría informes de morosidad periódicos
Gastos de consumos energéticos de la zonas comunes	Sí	Sí	
Gastos de consumos energéticos de propietarios	No	No	
Presupuestos	Sí	Sí	

Hay que tener en cuenta que la videovigilancia tiene como finalidad la seguridad de personas, bienes e instalaciones y sólo debe utilizarse cuando no sea posible acudir a otros medios que causen menos impacto en la privacidad, por eso, el acceso a las imágenes debe estar limitado a las personas que designe la Junta de propietarios, que es el órgano con potestad para realizar esta designación. Así, por ejemplo, en caso de producirse un robo en un vehículo dentro del garaje comunitario, se deberá acudir a la persona designada por la comunidad, en su defecto, el presidente, para que consulte las imágenes del día y a poder ser las horas, en las que se pudo producir el hecho, para que, en caso de que las imágenes sean de utilidad para el afectado, las mismas se conserven para aportarlas al procedimiento que se inicie con la denuncia. De otro modo, la privacidad de otras personas que puedan aparecer en las imágenes puede ser vulnerada. La AEPD establece que el acceso por parte de particulares, en este caso propietarios, a determinadas imágenes grabadas por las cámaras de videovigilancia debe caracterizarse por:

- Legitimación: las imágenes se utilizarán para la obtención de pruebas para formular una posterior denuncia por un delito, o reclamación por responsabilidad contractual o extracontractual a una compañía de seguros.
- Finalidad compatible: la comunicación de estos datos (imágenes) se encuentra dentro de la finalidad para la que se recogieron los datos, es decir, seguridad.
- Minimización de datos: las imágenes se limitarán al mínimo necesario en relación al incidente concreto y específico a que se refiere la petición.

6.2 Conflictos vecinales relacionados con la protección de datos personales

Hay situaciones que pueden suponer ciertos riesgos para la comunidad, como responsable del tratamiento, cuando alguno de los copropietarios quiere utilizar la protección de datos como excusa para denunciar a la comunidad, para lograr o impugnar acuerdos de la Junta, acciones derivadas de un mal uso de los listados con datos personales de los vecinos obtenidos cuando fueron cargos de la comunidad, etc.

En otras palabras, tener deficiencias en cuanto al cumplimiento normativo de esta materia, o llevar a cabo una aplicación parcial o incorrecta de la normativa de protección de datos, tiene

consecuencias, ya que una inspección de oficio por parte de la AEPD podría acarrear sanciones administrativas cuantiosas, y, si bien es cierto que, a tenor de lo desorbitado de las multas (hasta 20.000.000 €), uno podría llegar a pensar que están hechas para grandes empresas, la cuestión es que el importe de las sanciones es el que marca el RGPD, quedando en manos de la Agencia la graduación de las mismas.

Además, teniendo en cuenta el carácter garantista del Reglamento en relación a los derechos de los interesados, existe otro riesgo para la comunidad, el derecho a que toda persona que haya sufrido daños y perjuicios materiales o inmateriales como consecuencia de una infracción de la normativa de protección de datos pueda recibir una indemnización por los daños sufridos. Es decir, que un propietario, proveedor o, incluso, un trabajador, puede demandar a la comunidad ante los tribunales y exigir una indemnización a la que tendría que hacer frente si no puede demostrar que puso todos tus medios técnicos y organizativos para cumplir con el RGPD.

6.3 Deber de secreto en las comunidades de propietarios

En el ámbito de las comunidades de propietarios, es bastante común encontrarnos con situaciones en las que los vecinos que ostentan un cargo en la Junta como, por ejemplo, presidentes, vicepresidentes, secretarios, tesoreros, o bien personal de administración y servicios auxiliares, los propios trabajadores, o, incluso, el propio administrador de fincas, abusan de su situación predominante en cuanto al acceso a la información incumpliendo con el deber de secreto.

El deber de confidencialidad es uno de los principios recogidos el Art. 5 del RGPD y como deber aparece en el Art. 5 de la LOPD-GDD. Este deber, que incumbe a los responsables de las comunidades y a los administradores, y cualquier persona que trabaje para él y que intervengan en cualquier fase del tratamiento, comporta que no se puedan revelar los datos personales a los que tengan acceso. La obligación de secreto del administrador subsistirá aún después de finalizar sus relaciones con la comunidad de propietarios; del mismo modo queda obligado el presidente o cualquier otro interviniente en el tratamiento de los datos, una vez que cese en sus funciones.

6.4 Cesión de datos a terceros

¿Cómo y cuándo procede facilitar los datos de los vecinos para la prestación de servicios o tareas relacionadas con el mantenimiento de la comunidad, a pintores, técnicos de los porteros automáticos, instaladores de antenas, bancos, compañías de seguros, etc.?

La comunidad de propietarios tiene legitimidad para la cesión de los datos de los propietarios a entidades externas para la correcta llevanza, gobernabilidad y conservación de la comunidad, esto significa que podrá ceder los datos a las entidades prestadoras de servicios en el desempeño de sus funciones como gestora.

Es posible que, si dicho acceso a la información supone un encargo continuado por parte de la comunidad de propietarios, requiera de la formalización de los correspondientes contratos entre responsable y encargado del tratamiento, como, por ejemplo, que se encargue a otra entidad el cobro de los recibos de los propietarios.

6.5 Protección de datos y morosidad en las comunidades de propietarios

Para afrontar esta cuestión, debemos empezar hablando del contenido de la convocatoria de las Juntas de propietarios establecido en el Art. 16.2 LPH, según el cual deberá incluir una relación de los propietarios que no estén al corriente en el pago de las deudas vencidas a la comunidad, advirtiendo de la privación del derecho de voto si se dan determinadas circunstancias tasadas en el párrafo 2 del Art. 15 de la mencionada ley.

Esto es una garantía para que el resto de propietarios conozca el estado financiero de la comunidad y es necesario para determinar con exactitud el quórum requerido para la adopción de acuerdos de la Junta de propietarios.

Dada entonces la importancia de esta convocatoria y de su recepción por parte de todos los propietarios, debemos acudir al Art. 9 de la LPH, que recoge las obligaciones de cada propie-

tario, concretamente al apartado 1, letra h, donde se impone, a cada propietario, la obligación de comunicar a quien ejerza las funciones de secretario de la comunidad, por cualquier medio que permita tener constancia de su recepción, el domicilio en España a efectos de citaciones y notificaciones; en su defecto, se tendrá por domicilio a estos efectos, el piso o local perteneciente a la comunidad de la cual es propietario, surtiendo plenos efectos jurídicos las entregadas al ocupante del mismo.

Si aún así fuese imposible practicar la notificación al propietario, la citación o notificación se entenderá realizada mediante la colocación de la comunicación correspondiente en el tablón de anuncios de la comunidad, o en lugar visible de uso general habilitado al efecto, indicando expresamente la fecha y los motivos por los que se procede a esta forma de notificación, firmada por quien ejerza las funciones de secretario de la comunidad, con el visto bueno del presidente. La notificación así practicada producirá efectos jurídicos en el plazo de 3 días naturales.

A estas alturas del problema lo más probable es que se haya iniciado la acción judicial para la reclamación de cantidad, procedimiento judicial monitorio, etc., que, de hecho, requiere procesalmente esta notificación fehaciente al deudor.

Como vemos, lo que hace el legislador es establecer, en primer lugar, un sistema de notificaciones mediante la elección del lugar por el comunero, para, en su defecto, considerar como domicilio presunto a efectos de comunicaciones el del propio inmueble y es sólo a falta de que se verifique la posibilidad de llevar a cabo dichas comunicacionesa través de cualquiera de estos dos, cuando la LPH le permite recurrir al tablón de anuncios. Tablón que deberá estar cerrado con llave y dentro de la finca.

La gestión de la morosidad en las comunidades de propietarios ha dado para muchas resoluciones en la Agencia Española de Protección de Datos, además se entremezclan diversas legislaciones, por lo que se hace imprescindible contar con un asesoramiento continuado y especializado para conocer correctamente el procedimiento a seguir.

Existen numerosos procedimientos en relación a la publicación de datos de morosos en los tablones de anuncios de la comunidad, sobre la divulgación de dicha información a todos los vecinos, sobre la forma de publicación y forma del procedimiento monitorio por reclamación de cuotas impagadas.

Desde el punto de vista de la protección de datos, con carácter general, la publicación en el tablón de avisos de la finca de la identidad de los propietarios deudores y/o de las cuotas vencidas e impagadas por estos a la comunidad no está amparada por la normativa de protección de datos, ni siquiera cuando se indica solamente el dato relativo a la vivienda (piso y letra, por ejemplo), ya que este dato siempre va asociado a la identidad del titular de la vivienda y, por lo tanto, tiene la consideración de dato personal, con todo lo que conlleva.

En definitiva, solamente en los supuestos tasados por la LPH y con las condiciones anteriormente expuestas, se podrá dar publicidad a los datos de los deudores y de sus deudas con la comunidad sin el consentimiento de los mismos.

No obstante, la AEPD ha reconocido que si la Junta de propietarios acuerda expresamente la realización de una comunicación periódica y personal a cada uno de los propietarios relativa a la contabilidad de la comunidad, en la que se incluya una relación de aquellos que no están al corriente de pago en las cuotas, estaríamos ante una cesión de datos con consentimiento previo de los interesados, lo que, en principio, no vulneraría la normativa sobre protección de datos personales.

Dicho esto, tenemos que erradicar la costumbre de acudir al tablón directamente o incluso utilizarlo con fines persuasivos, o coercitivos para que el propietario sienta vergüenza y pague por temor a quedar en evidencia ante el resto de vecinos.

6.6 Videovigilancia en las comunidades de propietarios

La videovigilancia y todo lo relacionado con ella es uno de los temas más consultados, regulados y resueltos por la AGPD, siendo objeto de distintas regulaciones y obligaciones.

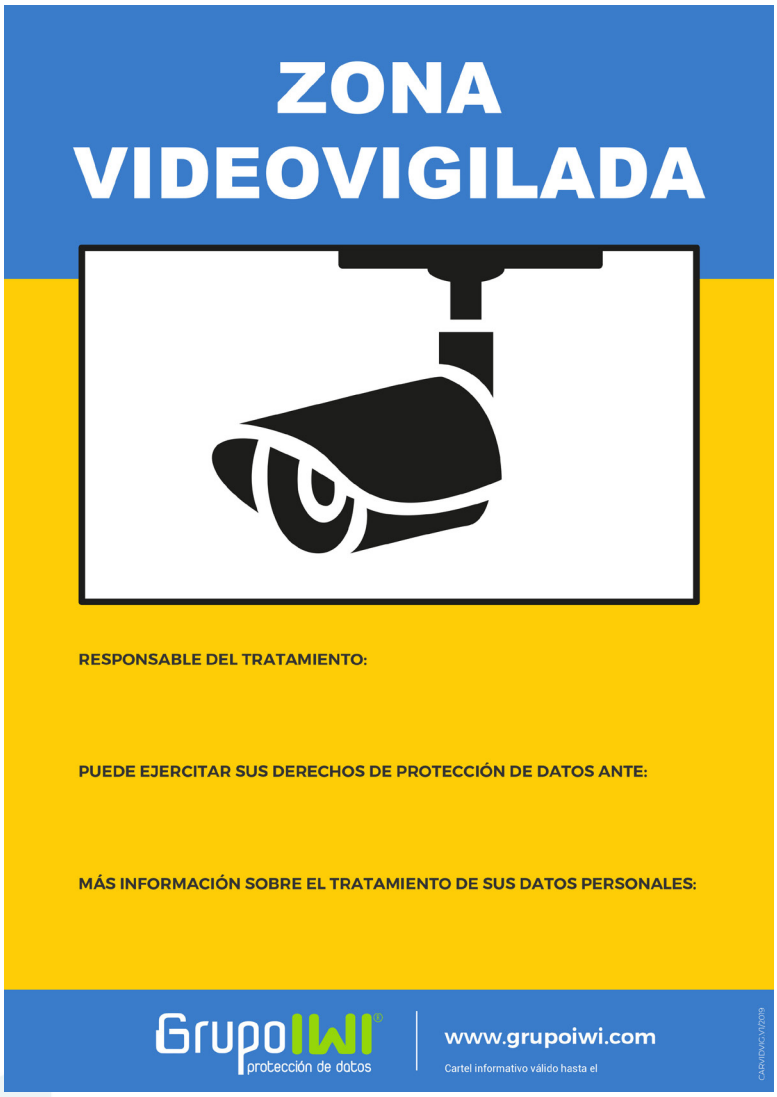
La casuística es numerosa: instalaciones de cámaras en los domicilios de vecinos, jardines, garajes, trasteros, ascensores, rellanos y pasillos, videoporteros, en pantallas individuales o en el canal de televisión comunitario, incluso en la mirilla de las puertas de entrada a los pisos. ¿Están legitimados los empleados de la comunidad para visualizar monitores de videovigilancia en espacios comunes? ¿Se pueden instalar cámaras en la piscina comunitaria? ¿Podemos revisar las videograbaciones para ver qué vecino saca la basura fuera de las horas establecidas?

Vayamos al principio. Para la instalación de cámaras en zonas comunes será necesario el acuerdo de la Junta de propietarios, que quedará reflejado en las actas de dicha Junta, conforme al Art. 17 de la LPH, aprobado con el voto favorable de las 3/5 partes del total de los propietarios que a su vez representen las 3/5 partes de las cuotas de participación.

Se recomienda, igualmente, que en el acuerdo se reflejen algunas de las características del sistema de videovigilancia, así como el número de cámaras o el espacio captado por las mismas.

La legitimación para el tratamiento de las imágenes captadas por las videocámaras reside en el interés público (Art. 6.1 RGPD), puesto que su finalidad es garantizar la seguridad de personas, bienes e instalaciones. En todo caso, la instalación de cámaras de seguridad ha de ser una medida proporcional en relación con la infracción que se pretenda evitar y, en ningún caso, debe suponer el medio inicial para llevar a cabo funciones de vigilancia.

Evidentemente esto supondrá un tratamiento específico que deberá incluirse en el registro de actividades de tratamiento de la Comunidad de Propietarios al que normalmente llamamos “Videovigilancia”.



Por otra parte, será imprescindible cumplir con el derecho de información. Para ello, se instalarán en los distintos accesos a la zona videovigilada y, en lugar visible, uno o varios carteles los cuales informarán, de forma clara, de que se está accediendo a una zona videovigilada, la identidad del responsable del tratamiento y ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos.

Asimismo, se pondrá a disposición de los afectados la restante información que

exige la legislación de protección de datos, que podrá estar disponible en conserjería, recepción, oficinas, tablones de anuncios o ser accesible a través de internet.

Si se pretende que las imágenes puedan ser utilizadas para el control de los trabajadores, en su caso, se les deberá informar expresamente de ello.

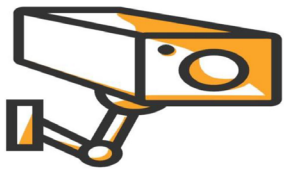
En cuanto a la grabación de las imágenes, es importante señalar que las cámaras sólo podrán captar imágenes de las zonas comunes de la comunidad. No podrán captarse imágenes de la vía pública a excepción de una franja mínima de los accesos al inmueble, pero en ningún caso podrán captarse imágenes del interior de un domicilio privado, ni de terrenos y viviendas colindantes o de cualquier otro espacio ajeno. Si se utilizan cámaras orientables y/o con zoom, será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos y viviendas de terceros.

> "El acceso a las imágenes estará restringido a las personas designadas por la comunidad de propietarios situándose el sistema de grabación en un lugar vigilado o de acceso restringido. Dicho acceso requerirá de un código de usuario y una contraseña. Una vez instalado el sistema, se recomienda el cambio regular de la contraseña, evitando las fácilmente deducibles. En ningún caso resultarán accesibles a los vecinos mediante canal de televisión comunitaria.

La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero, no exime a la comunidad del cumplimiento de la legislación de protección de datos, por lo que será responsable del tratamiento de las imágenes y, en su caso, deberá formalizarse el correspondiente contrato de encargo de tratamiento con la empresa de seguridad.

Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación. Las imágenes que se utilicen para denunciar delitos o infracciones se acompañarán a la denuncia y será posible su conservación para ser entregadas a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que las requieran, debiendo ser puestas a disposición de la autoridad competente en un plazo máximo de 72 horas desde que se tuvo conocimiento de la existencia de la grabación. No podrán utilizarse para otro fin. La petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. En este caso, la comunidad conservará la solicitud ya que este requerimiento será el documento que ampare esta comunicación de datos.

Estas y otras obligaciones han sido resumidas en varias fichas prácticas sobre videovigilancia en comunidades de propietarios y en plazas de garajes elaboradas por la AEPD que se muestran en las siguientes páginas.



FICHAS PRÁCTICAS DE VIDEOVIGILANCIA: I. INFORMACIÓN GENERAL

PRINCIPIOS BÁSICOS

- La captación y/o la grabación de imágenes de personas identificadas, o identificables, con fines de vigilancia mediante cámaras, videocámaras, o cualquier otro medio técnico análogo, constituye un tratamiento de datos personales sometido a la normativa de protección de datos.
- No está sometido a la normativa de protección de datos el tratamiento de imágenes en el ámbito exclusivamente personal o doméstico.
- No se podrán obtener imágenes de espacios públicos con fines de seguridad, actividad que está reservada en exclusiva a las Fuerzas y Cuerpos de Seguridad, salvo imágenes parciales y limitadas que resulten imprescindibles para la vigilancia o sea imposible evitarlas. Tampoco se pueden captar imágenes en baños, vestuarios o lugares análogos, ni de espacios ajenos.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- Previamente a su puesta en funcionamiento, se elaborará el registro de actividades referido a este tratamiento. Se trata de un documento interno. La AEPD ofrece en su Guía sobre el uso de videocámaras para seguridad y otras finalidades de un modelo de registro de actividades.
- La utilización de sistemas de videovigilancia que se limiten a una mera reproducción o emisión de imágenes en tiempo real, sin ser grabadas ni almacenadas, exige también configurar el registro de actividades de tratamiento.

DERECHO DE INFORMACIÓN

- En todos los casos se deberá informar de la existencia de un sistema de videovigilancia. A este fin se colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación y, si constituye un fichero, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales. La AEPD pone a su disposición un modelo de cartel. Igualmente, se pondrá a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del Reglamento General de Protección de Datos.

INSTALACIÓN

- La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a su titular del cumplimiento de la normativa de protección de datos.

SEGURIDAD Y SECRETO

- El responsable deberá adoptar las medidas de seguridad de carácter técnico y organizativo, en función del análisis de riesgos que se haya realizado previamente. Para facilitar esta labor, consulte la Guía de la AEPD sobre análisis de riesgos.
- Cuándo se trate de tratamientos de videovigilancia que entrañen un escaso riesgo, como podría ser el caso de uso en comunidades de propietarios o pequeños establecimientos, puede utilizarse la herramienta de esta AEPD denominada FACILITA_RGPD
- El responsable deberá informar a quién tenga acceso a las imágenes sobre sus obligaciones de seguridad (reserva, confidencialidad y sigilo) y de su deber de guardar secreto.
- Se deberán adoptar medidas que impidan el acceso a las imágenes por parte de personal no autorizado.

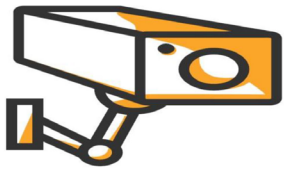
CONSERVACIÓN DE LAS IMÁGENES

- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.
- Cuando se produjese la grabación de un delito o infracción administrativa que deba ser puesta en conocimiento de una autoridad deberán conservarse las imágenes con el único fin de ponerlas a disposición de la citada autoridad sin que puedan ser utilizadas para ningún otro propósito.

NOTA IMPORTANTE

- Este documento se refiere únicamente a las obligaciones en materia de protección de datos personales. Pueden existir otras normas que impongan requisitos adicionales a la instalación de sistemas de videovigilancia que no han sido recogidos aquí.
- Para una mayor información, se puede consultar la Guía de la AEPD sobre el uso de videocámaras para seguridad y otras finalidades, así como los folletos específicos relativos a Comunidades de Propietarios; Viviendas; Garajes; Establecimientos Públicos y Control Empresarial.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



FICHAS PRÁCTICAS DE VIDEOVIGILANCIA: I. INFORMACIÓN GENERAL

PRINCIPIOS BÁSICOS

- La captación y/o la grabación de imágenes de personas identificadas, o identificables, con fines de vigilancia mediante cámaras, videocámaras, o cualquier otro medio técnico análogo, constituye un tratamiento de datos personales sometido a la normativa de protección de datos.
- No está sometido a la normativa de protección de datos el tratamiento de imágenes en el ámbito exclusivamente personal o doméstico.
- No se podrán obtener imágenes de espacios públicos con fines de seguridad, actividad que está reservada en exclusiva a las Fuerzas y Cuerpos de Seguridad, salvo imágenes parciales y limitadas que resulten imprescindibles para la vigilancia o sea imposible evitarlas. Tampoco se pueden captar imágenes en baños, vestuarios o lugares análogos, ni de espacios ajenos.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- Previamente a su puesta en funcionamiento, se elaborará el registro de actividades referido a este tratamiento. Se trata de un documento interno. La AEPD ofrece en su Guía sobre el uso de videocámaras para seguridad y otras finalidades de un modelo de registro de actividades.
- La utilización de sistemas de videovigilancia que se limiten a una mera reproducción o emisión de imágenes en tiempo real, sin ser grabadas ni almacenadas, exige también configurar el registro de actividades de tratamiento.

DERECHO DE INFORMACIÓN

- En todos los casos se deberá informar de la existencia de un sistema de videovigilancia. A este fin se colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación y, si constituye un fichero, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales. La AEPD pone a su disposición un modelo de cartel. Igualmente, se pondrá a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del Reglamento General de Protección de Datos.

INSTALACIÓN

- La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a su titular del cumplimiento de la normativa de protección de datos.

SEGURIDAD Y SECRETO

- El responsable deberá adoptar las medidas de seguridad de carácter técnico y organizativo, en función del análisis de riesgos que se haya realizado previamente. Para facilitar esta labor, consulte la Guía de la AEPD sobre análisis de riesgos.
- Cuándo se trate de tratamientos de videovigilancia que entrañen un escaso riesgo, como podría ser el caso de uso en comunidades de propietarios o pequeños establecimientos, puede utilizarse la herramienta de esta AEPD denominada FACILITA_RGPD
- El responsable deberá informar a quién tenga acceso a las imágenes sobre sus obligaciones de seguridad (reserva, confidencialidad y sigilo) y de su deber de guardar secreto.
- Se deberán adoptar medidas que impidan el acceso a las imágenes por parte de personal no autorizado.

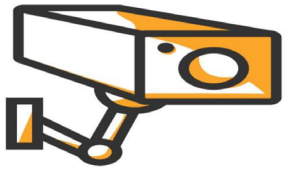
CONSERVACIÓN DE LAS IMÁGENES

- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.
- Cuando se produjese la grabación de un delito o infracción administrativa que deba ser puesta en conocimiento de una autoridad deberán conservarse las imágenes con el único fin de ponerlas a disposición de la citada autoridad sin que puedan ser utilizadas para ningún otro propósito.

NOTA IMPORTANTE

- Este documento se refiere únicamente a las obligaciones en materia de protección de datos personales. Pueden existir otras normas que impongan requisitos adicionales a la instalación de sistemas de videovigilancia que no han sido recogidos aquí.
- Para una mayor información, se puede consultar la Guía de la AEPD sobre el uso de videocámaras para seguridad y otras finalidades, así como los folletos específicos relativos a Comunidades de Propietarios; Viviendas; Garajes; Establecimientos Públicos y Control Empresarial.

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS



FICHAS PRÁCTICAS DE VIDEOVIGILANCIA: III. CÁMARAS PARA VIGILAR MI VIVIENDA

APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

- Cuando la captación de imágenes se limite exclusivamente al interior de la vivienda se considera que se realiza en el ejercicio de una actividad personal o doméstica, a la que no le es aplicable esta normativa.
- Sólo se aplicará cuando las cámaras puedan captar imágenes de personas en el exterior de la vivienda (entradas, fachadas, medianerías,...).

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- Previamente a su puesta en funcionamiento, se elaborará el registro de actividades referido a este tratamiento. Se trata de un documento interno. La AEPD ofrece en su Guía sobre el uso de videocámaras para seguridad y otras finalidades un modelo de registro de actividades.

DERECHO DE INFORMACIÓN

- En todos los casos se deberá informar de la existencia de un sistema de videovigilancia. A este fin se colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación y, si constituye un fichero, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales.
- La AEPD pone a su disposición un modelo de cartel. Igualmente, se pondrá a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del Reglamento General de Protección de Datos.

INSTALACIÓN

- Las imágenes captadas por las cámaras se limitarán a la vivienda de la que se sea titular. No podrán captarse imágenes de la vía pública a excepción de una franja mínima de los accesos a la vivienda. Tampoco podrán captarse imágenes de terrenos y viviendas colindantes o de cualquier otro espacio ajeno.
- Si se utilizan cámaras orientables y/o con zoom será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos y viviendas de terceros.
- La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a su titular del cumplimiento del Reglamento General de Protección de Datos.

MONITORES Y VISUALIZACIÓN DE IMÁGENES

- El acceso a las imágenes será exclusivamente del responsable del sistema sin que puedan ser accesibles por personas distintas.
- Si el acceso se realiza con conexión a Internet se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por la persona que pueda acceder a dichas imágenes.
- Una vez instalado el sistema, se recomienda el cambio de la contraseña, evitando las fácilmente deducibles.

SISTEMA DE GRABACIÓN

- El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes grabadas accederá sólo la persona autorizada que deberá introducir un código de usuario y una contraseña.
- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.
- Las imágenes que se utilicen para denunciar delitos o infracciones se acompañarán a la denuncia y serán conservadas para ser entregadas a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que lo requieran. No podrán utilizarse para otro fin.
- La petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al titular del tratamiento será el documento que ampare a éste para ceder datos a las mismas o los Juzgados y Tribunales que lo requieran.

NOTA IMPORTANTE

- Este documento se refiere únicamente a las obligaciones en materia de protección de datos personales. Pueden existir otras normas que impongan requisitos adicionales a la instalación de sistemas de videovigilancia que no han sido recogidos aquí.

FICHAS PRÁCTICAS DE VIDEOVIGILANCIA: IV. CÁMARAS PARA VIGILAR MI PLAZA DE GARAJE

APLICACIÓN DE LA NORMATIVA DE PROTECCIÓN DE DATOS

- Se aplicará siempre que el garaje forme parte de un espacio compartido por el que puedan transitar el resto de los propietarios o terceros que acceden al mismo.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

- Previamente a su puesta en funcionamiento, se elaborará el registro de actividades referido a este tratamiento. Se trata de un documento interno. La AEPD ofrece en su Guía sobre el uso de videocámaras para seguridad y otras finalidades ~~de~~ un modelo de registro de actividades.

DERECHO DE INFORMACIÓN

- En todos los casos se deberá informar de la existencia de un sistema de videovigilancia. A este fin se colocará un cartel suficientemente visible en los accesos a las zonas vigiladas, que indicará de forma clara la identidad del responsable de la instalación, ante quién y dónde dirigirse para ejercer los derechos que prevé la normativa de protección de datos, y dónde obtener más información sobre el tratamiento de los datos personales
- La AEPD pone a su disposición un modelo de cartel. Igualmente, se pondrá a disposición de los afectados el resto de la información a la que se refiere el artículo 13 del Reglamento General de Protección de Datos (RGPD).

INSTALACIÓN

- Las imágenes captadas por las cámaras se limitarán a la plaza de aparcamiento de la que sea titular el responsable del sistema y a una franja mínima de las zonas comunes que no sea posible evitar captar para la vigilancia de la plaza de garaje, previa autorización de la Junta de Propietarios que deberá constar en las actas correspondientes. No se captarán imágenes de plazas de aparcamiento ajenas.
- Tampoco podrán captarse imágenes de la vía pública, terrenos y viviendas colindantes o de cualquier otro espacio ajeno.
- Si se utilizan cámaras orientables y/o con zoom será necesaria la instalación de máscaras de privacidad para evitar captar imágenes de la vía pública, terrenos y viviendas de terceros.
- La contratación de un servicio de videovigilancia externo o la instalación de las cámaras por un tercero no exime a su titular del cumplimiento de la normativa de protección de datos.

MONITORES Y VISUALIZACIÓN DE IMÁGENES

- El acceso a las imágenes será exclusivamente del responsable del sistema sin que puedan ser accesibles por personas distintas.
- Si el acceso se realiza con conexión a Internet se restringirá con un código de usuario y una contraseña (o cualquier otro medio que garantice la identificación y autenticación unívoca), que sólo serán conocidos por la persona que pueda acceder a dichas imágenes.
- Una vez instalado el sistema, se recomienda el cambio de la contraseña, evitando las fácilmente deducibles.

SISTEMA DE GRABACIÓN

- El sistema de grabación se ubicará en un lugar vigilado o de acceso restringido. A las imágenes grabadas accederá sólo la persona autorizada que deberá introducir un código de usuario y una contraseña.
- Las imágenes serán conservadas durante un plazo máximo de un mes desde su captación, transcurrido el cual se procederá al borrado.
- Las imágenes que se utilicen para denunciar delitos o infracciones se acompañarán a la denuncia y serán conservadas para su posible entrega a las Fuerzas y Cuerpos de Seguridad o a los Juzgados y Tribunales que lo requieran. No podrán utilizarse para otro fin.
- La petición de imágenes por las Fuerzas y Cuerpos de Seguridad se realizará en el marco de actuaciones judiciales o policiales. El requerimiento al titular del tratamiento será el documento que ampare a éste para ceder datos a las mismas o a los Juzgados y Tribunales que lo requieran.

NOTA IMPORTANTE

- Este documento se refiere únicamente a las obligaciones en materia de protección de datos personales. Pueden existir otras normas que impongan requisitos adicionales a la instalación de sistemas de videovigilancia que no han sido recogidos aquí.
- Para una mayor información, se puede consultar la Guía de la AEPD sobre Protección de Datos y Administración de Fincas.

7 USO DE LAS **NUEVAS TECNOLOGÍAS** EN LAS **COMUNIDADES DE PROPIETARIOS**

Cuando hablamos de nuevas tecnologías, nos solemos referir a herramientas de comunicación como el correo electrónico (cuando el primer email se envió en 1971, nada menos) o WhatsApp (que tiene ya más de 2 mil millones de usuarios). Dentro de este concepto también podemos hablar de las videollamadas, sistemas de almacenamiento y compartición de datos en la nube, plataformas de gestión online, etc. Está claro que para la mayoría de las personas no se trata de técnicas nuevas ni tampoco desconocidas, con independencia de que tengamos un mayor o menor conocimiento de las mismas. Pero eso no es aplicable a nuestras leyes, desgraciadamente, donde nos encontramos graves carencias de actualización en este sentido.

A pesar de los riesgos que conllevan estas tecnologías, es innegable la comodidad y transparencia que pueden aportar a la gestión de la comunidad, por lo que es de esperar que las distintas normas por las que se regulan las comunidades de propietarios, vayan adaptándose a su utilización.

Pasemos a exponer algunas ideas al respecto de cómo podemos usar estas nuevas tecnologías en las relaciones entre la comunidad de propietarios, el administrador de fincas y los propietarios.

7.1 Juntas de Propietarios virtuales

Las reuniones o Juntas de vecinos celebradas de forma virtual, no se encuentran actualmente recogidas en la legislación vigente, limitándose la LPH a establecer que la asistencia a la Junta de propietarios será personal o por representación legal o voluntaria. Eso sí, la Ley Catalana de Propiedad Horizontal recoge la posibilidad de que los estatutos de la comunidad o la propia

Junta de propietarios acuerden la posibilidad de asistir por videoconferencia o por otros medios telemáticos de comunicación sincrónica similares.

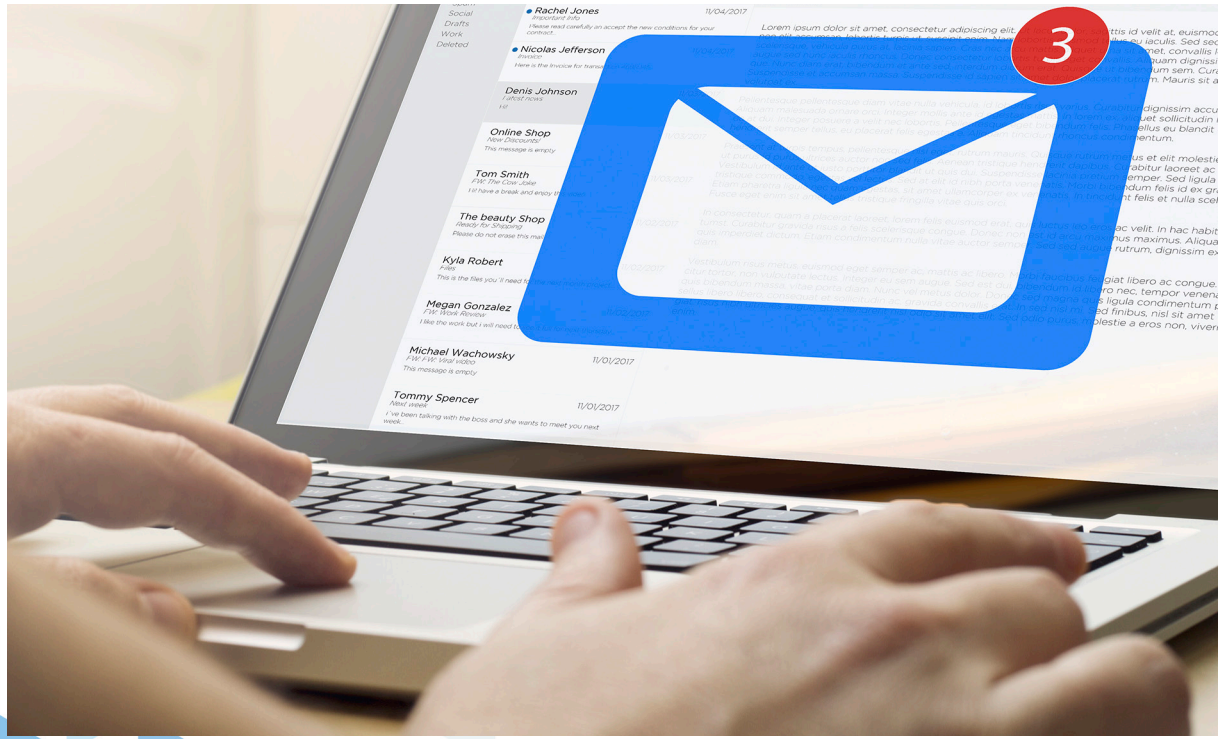
La realización de este tipo de reuniones virtuales conlleva riesgos para la privacidad de los comuneros. Aunque es cierto que la normativa de protección de datos no impide que la comunidad de propietarios disponga de todos aquellos datos que sean adecuados, pertinentes y limitados a lo necesario para los fines propios de dicha comunidad, entre los que se encuentran los necesarios para comunicarse con los propietarios, hay que intentar recurrir a aquellos medios que no supongan la cesión de datos entre los propios comuneros, es decir, que no expongan sus números de teléfono o direcciones de correo electrónico. Así, por ejemplo, se deberá recurrir a aplicaciones que creen salas de reunión a las que se acceda mediante un enlace facilitado a cada propietario con su correspondiente contraseña para evitar intromisiones por parte de terceros ajenos a la comunidad. Por ello es importante estudiar bien las numerosas opciones que existen actualmente para llevar a cabo este tipo de acciones, recurriendo solamente a aquellas que proporcionen un nivel adecuado de seguridad además de cumplir con todos los requisitos legales exigidos por la normativa de protección de datos.

Hay que tener cuidado si se quiere grabar las reuniones, ya que será necesario informar a los participantes para cumplir con el RGPD y, además, poder acreditarlo.

Siempre será una buena medida la creación de un protocolo para la realización de las Juntas virtuales con el objeto de informar a los propietarios de qué medios van a usarse y su funcionamiento así como las normas básicas de seguridad para proteger las videollamadas.

7.2 Notificaciones online

Al igual que ocurre con la posibilidad de asistir a las Juntas de propietarios mediante videollamadas o cualquier otro medio de comunicación bidireccional, la LPH no hace mención alguna a la posibilidad de que administrador y comuneros se comuniquen por correo electrónico, pero sí lo hace la Ley Catalana de Propiedad Horizontal, la cual señala que el envío de la con-



vocatoria podrá hacerse por correo postal o electrónico, o por otros medios de comunicación, siempre y cuando se garantice que la comunicación y su contenido son auténticos.

Ahora bien, somos conscientes del uso en la actualidad de las nuevas tecnologías de la comunicación en las relaciones administrador-propietarios, por lo que hay que tener en cuenta los riesgos que, en relación a la normativa de protección de datos, conlleva su uso. Ante todo, el correo electrónico es un dato personal y como tal podrá ser tratado por la comunidad de propietarios y, en virtud del encargo de tratamiento, por el administrador de fincas, para llevar a cabo todas aquellas comunicaciones que sean adecuadas y pertinentes para los fines de la comunidad, pero no para ser cedido a otros propietarios. De tal modo que una de las principales amenazas que conlleva el uso del envío de correos electrónicos, es vulnerar la confidencialidad de las direcciones de los propietarios haciendo envíos a múltiples destinatarios sin usar copia oculta. Los usos que se den a la dirección de correo electrónico de cada propietario deberá fijarlos el administrador con dicho propietario, siendo recomendable pasar un formulario donde se indiquen los datos del comunero y qué tipo de comunicaciones solicita que se le envíen por correo electrónico, siendo ésta la forma de acreditar en caso de ser necesario que se actuó siguiendo sus indicaciones.

7.3 Comunicaciones por WhatsApp

El uso de las aplicaciones de mensajería instantánea como Whatsapp Messenger y Whatsapp Business plantea numerosos inconvenientes para gestionar la relación con los propietarios, ya que son aplicaciones que actualmente no cumplen con medidas de seguridad suficientes para proteger la información confidencial de los interesados al depender de la política de privacidad de WhatsApp.

Por eso, hay que tomar una algunas precauciones si se decide su uso como medio de comunicación entre la comunidad, en la figura del administrador de fincas, y los comuneros:

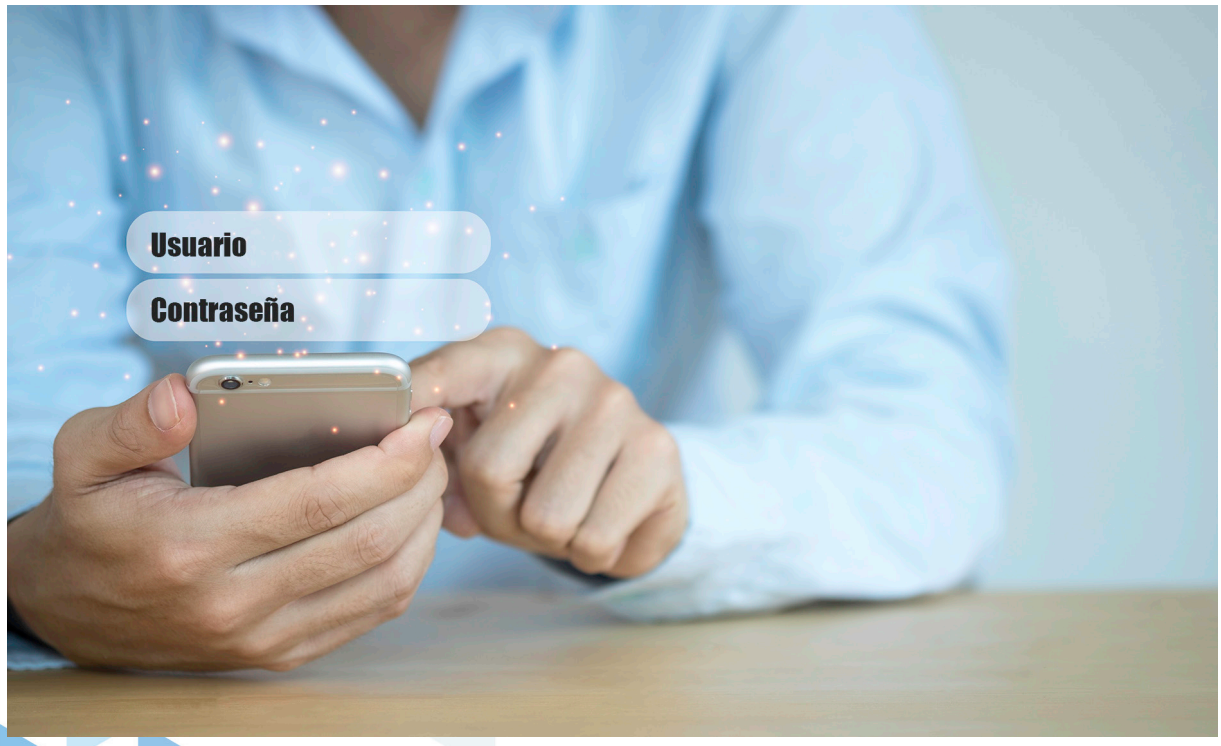
- Que el propietario manifieste su consentimiento expreso para la recepción de comunicaciones por esta vía, especialmente cuando se trate de grupos, ya que los números de teléfono de los intervinientes, así como su foto de perfil, son públicos para los miembros del grupo, lo que constituirá una cesión de datos personales.
- Evita enviar datos de carácter personal de todo tipo (nombre y apellidos, email, DNI, dirección postal, número de la Seguridad Social, datos bancarios...).
- Nunca envíes o solicites información relativa a categorías especiales de datos como son los referidos a salud.

Nuestra recomendación es hacer un uso responsable tanto de WhatsApp como de otras herramientas de mensajería instantánea. La aplicación Whatsapp se debe limitar estrictamente a ser un canal informativo que puede servir para comunicaciones de citas, recordatorios, reuniones, etc., pero nunca para intercambiar ningún tipo de información de datos personales o confidenciales.

7.4 Datos en la nube, apps y páginas web

El uso de herramientas digitales como la nube en las comunidades de propietarios, facilita la gestión del administrador de fincas y la vida de los propietarios. ¿Cómo va a influir en el trabajo desempeñado por el administrador? Con la utilización de la nube, los administradores de fincas podrán gestionar cualquier aspecto de la comunidad, desde el pago de cuotas y recibos, hasta el recuento de votos, manteniendo informados a los propietarios en todo momento sin tener que estar pendientes de citas en el despacho, reuniones de vecinos o uso de tablones de anuncios, directamente desde el ordenador, tablet o móvil del propio comunero.

Todo esto sería posible mediante la creación de un portal donde los usuarios se identifiquen de manera individual, es decir, cada propietario con su propio nombre de usuario y contraseña, para acceder a la información compartida. ¿A qué tipo de información va a poder acceder un propietario?



- Recibos.
- Consumos.
- Convocatorias y actas de Juntas.
- Avisos de diferente tipología, como calendario de obras en las zonas comunes o servicios de limpieza de garajes.

En general, se podrá compartir con los propietarios toda aquella información relacionada con la correcta llevanza de la gestión de la comunidad, eso sí, respetando en todo momento la normativa de protección de datos, tal y como se recoge en esta Guía cuando hablamos del acceso de los propietarios a la documentación.

Como hemos mencionado anteriormente, la utilización de la nube va a ayudar a compartir información, pero hay que tener en cuenta que no todo son ventajas, sino que también conlleva unos riesgos, como por ejemplo:

- Filtrado de contraseñas: Nuestras contraseñas pueden ser robadas o hackeadas pudiendo acceder a la información personas no autorizadas.
- Ataque al servidor: Los hackers en estos casos, pueden aprovechar las vulnerabilidades del servidor o de los equipos con acceso al mismo para realizar ataques que pongan en riesgo la información de la comunidad.
- Continuidad del servicio: Es posible que en ocasiones haya problemas con el funcionamiento del servidor, lo que provocaría que no pudiéramos acceder a la información durante el tiempo que dure la incidencia.
- Accesos no autorizados: una incorrecta gestión de los accesos a la información contenida en el servidor puede dar lugar a cesiones no autorizadas de datos y violaciones de la confidencialidad de los mismos.

Además del uso de plataformas online o en la nube, es cada vez más frecuente la oferta tanto a comunidades como a administradores, de aplicaciones móviles con las que los propietarios podrán gestionar su relación con la comunidad, tanto en cuanto al cobro o

pago de cuotas, como mantenerse informados de todo lo relacionado con gestión de la misma.

En definitiva, el uso de apps móviles, plataformas online o webs van a facilitar el trabajo del administrador de fincas a la hora de gestionar las comunidades de propietarios, a la vez que incrementan la transparencia en la información a los propietarios, ya que van a disponer casi en tiempo real y en cualquier momento que lo deseen, de acceso a las distintas gestiones llevadas a cabo, además de otras funciones que pueden ir asociadas al sistema elegido, como notificaciones de incidencias o desperfectos, creación de foros, envío de mensajes directos entre usuarios, etc. ahorrando a su vez recursos a la comunidad en cuanto a gastos y tiempo invertido en llevar a cabo las comunicaciones entre el administrador y los propietarios.

Pero insistimos, no todo son ventajas, hay que tener cuidado con la información que tanto el administrador como los propietarios comparten a través de la web o de la aplicación, ya que a hora de colgar cualquier tipo de información debemos de asegurarnos de que estamos legitimados para ello, aquí nos encontramos el caso de la publicación de imágenes de personas físicas en la web para la cual necesitamos consentimiento expreso, o la publicación de datos o información comprometida o que no forme parte de la buena llevanza de la comunidad (números de cuenta, teléfonos, correos electrónicos, etc) que suponen un incumpliento de la normativa de protección de datos susceptible de sanción.

> “Concluyendo, el uso de las llamadas nuevas tecnologías presenta numerosas ventajas, pero también una serie de riesgos que deben ser tenidos en cuenta, entre los que se encuentran la privacidad de la información almacenada, la continuidad de los servicios, los cambios legales y la pérdida de control de las herramientas utilizadas. Por ello es importante pararse a evaluar el riesgo que conlleva el sistema que queremos comenzar a utilizar y comprobar el cumplimiento normativo y la implantación de las medidas de seguridad requeridas por parte del proveedor.

8 INFORMES JURÍDICOS Y RESOLUCIONES DE LA AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS EN RELACIÓN A ADMINISTRADORES DE FINCAS Y COMUNIDADES DE PROPIETARIOS

Las razones por las que más se recurre a la Agencia Española de Protección de Datos en los casos de comunidades de vecinos son la videovigilancia, la difusión de datos personales de vecinos que tienen deudas con la comunidad y el ejercicio de derechos. Esto se materializa en informes jurídicos y resoluciones que se pueden consultar en la propia web de la Agencia,

A continuación enumeramos algunos de los informes jurídicos más relevantes relacionados con administradores de fincas y comunidades de propietarios. Si bien dichos informes se refieren a la anterior normativa, habrá que seguir atendiendo a los criterios expuestos en ellos por la AEPD en cuanto no sean incompatibles con lo dispuesto en la normativa de protección de datos vigente en el momento actual.

2015-0220 Cámaras de videovigilancia en comunidad de propietarios (Legitimación).

2013-0261 Cesión de datos de comunidad de propietarios a propietarios (Proporcionalidad e idoneidad).

2012-0066 Creación de un portal web para gestionar la comunidad.

2010-0081 Condición de responsable del fichero de administradores y gestores de fincas.

2010-0032 Videovigilancia (Legitimación para captar imágenes en zonas comunes).

2009-0636 Administrador de fincas encargado del tratamiento (Comunicación de datos al responsable).

2009-0303 Exhibición de libro de actas a entidades financieras.

2009-0292 Acceso a datos de propietarios morosos por empleados de la finca (Convocatoria entregada en sobre abierto y acta en tablón de anuncios).

2009-0084 Cesión de datos de propietarios por administrador acordada en Junta general de propietarios.

De igual modo, listamos algunos de los procedimientos administrativos más relevantes para administradores de fincas y comunidades de propietarios.

PS-00180-2019 Multa de apercibimiento por incluir en el tablón de anuncios de la comunidad piso y puerta de una vecina.

PS-00168-2019 Multa de apercibimiento por insertar en el tablón de anuncios un listado de propietarios a los que se les va a reclamar las cuotas impagadas.

PS-00084-2019 Multa de apercibimiento por publicar en el tablón de anuncios datos de morosidad.

E-09277-2018 Web del administrador de fincas que, al no disponer de las medidas de seguridad adecuadas ha vulnerado la confidencialidad de los datos de los propietarios, el procedimiento es archivado por el cierre de la web.

TD-01291-2018 Reclamación contra una comunidad de propietarios, por no haber sido debidamente atendido un derecho de acceso.

A-00126-2018 Multa de apercibimiento por exponer la convocatoria de la Junta General Ordinaria en los 29 portales de la comunidad.

PS-00538-2017 Sanción de 900 € por exponer en el tablón de anuncios una sentencia con datos personales.

PS-00377-2015 Sanción de 2.000 € por publicación en el tablón de anuncios de listado de morosos de forma reiterativa infringiendo el deber de secreto.

PS-00085-2016 Sanción de 6.000 € a un administrador de fincas por no devolver la documentación al cesar en su cargo.

El hecho de que en los procedimientos acaben con una sanción de apercibimiento, no debe llevarnos a pensar que el incumplimiento de la normativa de protección de datos no tiene repercusiones. El apercibimiento es una medida excepcional que la AEPD decide aplicar en lugar de una sanción económica, exigiéndole al responsable o encargado del tratamiento la adopción de medidas correctoras. Tras un apercibimiento, el infractor deberá demostrar que se han adoptado las medidas indicadas por la Agencia ya que, en caso contrario, se abrirá un procedimiento sancionador donde sí podría ser sancionado económicamente.

> “En definitiva, ahora más que nunca, es importante tomar conciencia de la relevancia de cumplir con la normativa en protección de datos de carácter personal y contar con el asesoramiento de expertos en esta materia que nos guíen en su cumplimiento y nos asesoren para evitar posibles sanciones, tanto en las comunidades de propietarios como en los despacho de los administradores de fincas.

En **GrupoIWI** queremos ser su **Solución en Protección de Datos**, por lo que todo nuestro equipo trabaja con esa finalidad, ofreciéndole un trato personalizado que nos permite dar respuesta a sus necesidades y resolver las dudas que le surjan en esta materia.

Para cualquier aclaración o cuestión que desee plantearnos no dude en ponerse en contacto con nosotros.

GrupoIWI®
protección de datos

www.grupoiwi.com

Av. Fernando de los Ríos, 11
Portal 2 · Oficina 6
18100 · Armilla (Granada)

cliente@grupoiwi.com

Telf.: **958 415 736**

GUPRAAFYCP.V2/2020