**REGISTRO DE ACTIVIDADES DE TRATAMIENTO DE LA COMUNIDAD DE PROPIETARIOS**

**Responsable del Tratamiento**
El responsable del tratamiento de sus datos es:
COMUNIDAD DE PROPIETARIOS \*\*\*\*\*\*\*\*\*\*\*\*\*\*

CIF: H\*\*\*\*\*\*\*\*\*\*

Información de contacto:

C/Santiago Rusiñol, 32 bajo 46019 en VALENCIA

Teléfonos: 96 338 5730 - 96 288 8642 - 96 001 1234
Correo electrónico: info@afiser.com

**Finalidad del tratamiento**

* Realizar las comunicaciones obligatorias para cumplir con la Ley de Propiedad Horizontal, así como otras de tipo informativo que sean necesarias o recomendables para la buena marcha y gestión de la Comunidad de propietarios, como gestionar incidencias y siniestros, gestionar devoluciones, cobros e impagados, gestionar relaciones laborales con empleados en su caso, así como realizar comunicaciones relacionadas con consultas y reclamaciones de propietarios.

**Categorías de interesados y destinatarios**

* Propietarios de la Comunidad.
* Representante Legal de la Comunidad (Presidente)
* Encargado del tratamiento y Administrador de la Comunidad de propietarios.
* Proveedores de servicios para reparaciones, mantenimientos y vigilancia.
* Compañías de Seguros y profesionales de las mismas para la atención de siniestros.
* Profesionales contratados por la Comunidad como Arquitectos, Abogados. Procuradores, Asesores laborales y fiscales.
* Empleados de la Comunidad como porteros-conserjes, personal de limpieza y jardineros en su caso.
* Entidades Bancarias en el caso de las personas autorizadas en la cuenta bancaria de la Comunidad de propietarios
* La Administración Pública, Jueces y Tribunales, cuando sean requeridos legalmente.

**Categorías de los datos personales**

* Nombre y apellidos
* NIF / CIF
* Datos de contacto como teléfonos, e-mails, direcciones de correspondencia
* Números de cuenta bancaria IBAN
* Datos económico-financieros de los recibos, cobros y pagos de los propietarios y proveedores.
* En el caso de que la Comunidad tenga empleados, los datos de la seguridad social y los económicos-financieros contemplados en la nómina de los empleados, así como los datos de formación, profesionales y porcentaje de minusvalía.

**Plazos previstos de supresión de las diferentes categorías de los datos**

A excepción de los datos económico-financieros recopilados por la Comunidad de propietarios que deberán de ser custodiados por el Responsable del Tratamiento durante el plazo que la Legislación fiscal estipule respecto a la prescripción de responsabilidades, el resto de Categorías de datos personales se suprimirán una vez el propietario deje de se cotitular de un inmueble en la Comunidad de Propietarios o uno de los empleados finalice su relación laboral con la Comunidad de Propietarios.

**Medidas técnicas y organizativas de seguridad**

Este documento ha sido diseñado para tratamientos de datos personales de bajo riesgo de donde se deduce que el mismo no podrá ser utilizado para tratamientos de datos personales que incluyan datos personales relativos al origen étnico o racial, ideología política religiosa o filosófica, afiliación sindical, datos genéticos y biométricos, datos de salud, y datos de orientación sexual de las personas así como cualquier otro tratamiento de datos que entrañe alto riesgo para los derechos y libertades de las personas.

El artículo 5.1.f del Reglamento General de Protección de Datos (RGPD) determina la necesidad de establecer garantías de seguridad adecuadas contra el tratamiento no autorizado o ilícito, contra la pérdida de los datos personales, la destrucción o el daño accidental. Esto implica el establecimiento de medidas técnicas y organizativas encaminadas a asegurar la integridad y confidencialidad de los datos personales y la posibilidad (artículo 5.2) de demostrar que estas medidas se han llevado a la práctica (responsabilidad proactiva).

A tenor del tipo de tratamiento que ha puesto de manifiesto cuando ha cumplimentado este formulario, las medidas mínimas de seguridad mínimas que debería tener en cuenta son las siguientes:

**MEDIDAS ORGANIZATIVAS**

INFORMACIÓN QUE DEBERÁ SER CONOCIDA POR TODO EL PERSONAL CON ACCESO A DATOS PERSONALES

Todo el personal con acceso a los datos personales deberá tener conocimiento de sus obligaciones con relación a los tratamientos de datos personales y serán informados acerca de dichas obligaciones. La información mínima que será conocida por todo el personal será la siguiente:

**DEBER DE CONFIDENCIALIDAD Y SECRETO**

* Se deberá evitar el acceso de personas no autorizadas a los datos personales, a tal fin se evitará: dejar los datos personales expuestos a terceros (pantallas electrónicas desatendidas, documentos en papel en zonas de acceso público, soportes con datos personales, etc.), esta consideración incluye las pantallas que se utilicen para la visualización de imágenes del sistema de videovigilancia. Cuando se ausente del puesto de trabajo, se procederá al bloqueo de la pantalla o al cierre de la sesión.
* Los documentos en papel y soportes electrónicos se almacenarán en lugar seguro (armarios o estancias de acceso restringido) durante las 24 horas del día.
* No se desecharán documentos o soportes electrónicos (cd, pen drives, discos duros, etc.) con datos personales sin garantizar su destrucción.
* No se comunicarán datos personales o cualquier información personal a terceros, se prestará atención especial en no divulgar datos personales protegidos durante las consultas telefónicas, correos electrónicos, etc.
* El deber de secreto y confidencialidad persiste incluso cuando finalice la relación laboral del trabajador con la empresa.
* Tanto los empleados de AFISER SERVICIOS INMOBILIARIOS (Encargado del Tratamiento), como el Representante Legal de la Comunidad de Propietarios (PRESIDENTE), firmarán un COMPROMISO DE CONFIDENCIALIDAD.

**DERECHOS DE LOS TITULARES DE LOS DATOS**

Se informará a todos los trabajadores acerca del procedimiento para atender los derechos de los interesados, definiendo de forma clara los mecanismos por los que pueden ejercerse los derechos (medios electrónicos, referencia al Delegado de Protección de Datos si lo hubiera, dirección postal, etc.) teniendo en cuenta lo siguiente:

* Previa presentación de su documento nacional de identidad o pasaporte, los titulares de los datos personales (interesados) podrán ejercer sus derechos de acceso, rectificación, supresión, oposición y portabilidad. El responsable del tratamiento deberá dar respuesta a los interesados sin dilación indebida.
* Para el derecho de acceso se facilitará a los interesados la lista de los datos personales de que disponga junto con la finalidad para la que han sido recogidos, la identidad de los destinatarios de los datos, los plazos de conservación, y la identidad del responsable ante el que pueden solicitar la rectificación supresión y oposición al tratamiento de los datos.
* Para el derecho de rectificación se procederá a modificar los datos de los interesados que fueran inexactos o incompletos atendiendo a los fines del tratamiento.
* Para el derecho de supresión se suprimirán los datos de los interesados cuando los interesados manifiesten su negativa u oposición al consentimiento para el tratamiento de sus datos y no exista deber legal que lo impida.
* Para el derecho de portabilidad los interesados deberán comunicar su decisión e informar al responsable, en su caso, sobre la identidad del nuevo responsable al que facilitar sus datos personales.

El responsable del tratamiento deberá informar a todas las personas con acceso a los datos personales acerca de los términos de cumplimiento para atender los derechos de los interesados, la forma y el procedimiento en que se atenderán dichos derechos.

**VIOLACIONES DE SEGURIDAD DE DATOS DE CARÁCTER PERSONAL**

* Cuando se produzcan violaciones de seguridad DE DATOS DE CARÁCTER PERSONAL, como por ejemplo, el robo o acceso indebido a los datos personales se notificará a la Agencia Española de Protección de Datos en término de 72 horas acerca de dichas violaciones de seguridad, incluyendo toda la información necesaria para el esclarecimiento de los hechos que hubieran dado lugar al acceso indebido a los datos personales. La notificación se realizará por medios electrónicos a través de la sede electrónica de la Agencia Española de Protección de Datos en la dirección: <https://sedeagpd.gob.es>

**CAPTACIÓN DE IMÁGENES CON CÁMARAS Y FINALIDAD DE SEGURIDAD (VIDEOVIGILANCIA)**

* UBICACIÓN DE LAS CÁMARAS: Se evitará la captación de imágenes en zonas destinadas al descanso de los trabajadores.
* UBICACIÓN DE MONITORES: Los monitores donde se visualicen las imágenes de las cámaras se ubicarán en un espacio de acceso restringido de forma que no sean accesibles a terceros.
* CONSERVACIÓN DE IMÁGENES: Las imágenes se almacenarán durante el plazo máximo de un mes, con excepción de las imágenes que sean aportadas a los tribunales y las fuerzas y cuerpos de seguridad.
* DEBER DE INFORMACIÓN: Se informará acerca de la existencia de las cámaras y grabación de imágenes mediante un distintivo informativo donde mediante un pictograma y un texto se detalle el responsable ante el cual los interesados podrán ejercer su derecho de acceso. En el propio pictograma se podrá incluir el texto informativo. En la página web de la Agencia disponen de modelos, tanto del pictograma como del texto.
* CONTROL LABORAL: Cuando las cámaras vayan a ser utilizadas con la finalidad de control laboral según lo previsto en el artículo 20.3 del Estatuto de los Trabajadores, se informará al trabajador o a sus representantes acerca de las medidas de control establecidas por el empresario con indicación expresa de la finalidad de control laboral de las imágenes captadas por las cámaras.
* DERECHO DE ACCESO A LAS IMÁGENES:Para dar cumplimiento al derecho de acceso de los interesados se solicitará una fotografía reciente y el Documento Nacional de Identidad del interesado, así como el detalle de la fecha y hora a la que se refiere el derecho de acceso.No se facilitará al interesado acceso directo a las imágenes de las cámaras en las que se muestren imágenes de terceros. En caso de no ser posible la visualización de las imágenes por el interesado sin mostrar imágenes de terceros, se facilitará un documento al interesado en el que se confirme o niegue la existencia de imágenes del interesado.

Para más información puede consultar las guías de videovigilancia de la Agencia Española de Protección de Datos que se encuentran a su disposición en la sección de publicaciones de la web [www.agpd.es.](http://www.agpd.es.)

**MEDIDAS TÉCNICAS**

**IDENTIFICACIÓN**

* Cuando el mismo ordenador o dispositivo se utilice para el tratamiento de datos personales y fines de uso personal se recomienda disponer de varios perfiles o usuarios distintos para cada una de las finalidades. Deben mantenerse separados los usos profesional y personal del ordenador.
* Se recomienda disponer de perfiles con derechos de administración para la instalación y configuración del sistema y usuarios sin privilegios o derechos de administración para el acceso a los datos personales. Esta medida evitará que en caso de ataque de ciberseguridad puedan obtenerse privilegios de acceso o modificar el sistema operativo.
* Se garantizará la existencia de contraseñas para el acceso a los datos personales almacenados en sistemas electrónicos. La contraseña tendrá al menos 8 caracteres, mezcla de números y letras.
* Cuando a los datos personales accedan distintas personas, para cada persona con acceso a los datos personales, se dispondrá de un usuario y contraseña específicos (identificación inequívoca).
* Se debe garantizar la confidencialidad de las contraseñas, evitando que queden expuestas a terceros. Para la gestión de las contraseñas puede consultar la guía de privacidad y seguridad en internet de la Agencia Española de Protección de Datos y el Instituto Nacional de Ciberseguridad. En ningún caso se compartirán las contraseñas ni se dejarán anotadas en lugar común y el acceso de personas distintas del usuario.
* En cualquier caso sólo se podrá acceder a los datos de carácter personal accediendo al servicio de alojamiento de archivos en la Nube, aplicaciones móviles y aplicaciones Web accediendo a través de un usuario y contraseña personal a los que únicamente tienen acceso los empleados de AFISER SERVICIOS INMOBILIARIOS (Encargado del Tratamiento)

**DEBER DE SALVAGUARDA**

A continuación se exponen las medidas técnicas mínimas para garantizar la salvaguarda de los datos personales:

* ACTUALIZACIÓN DE ORDENADORES Y DISPOSITIVOS: Los dispositivos y ordenadores utilizados para el almacenamiento y el tratamiento de los datos personales deberán mantenerse actualizados en la media posible.
* MALWARE: En los ordenadores y dispositivos donde se realice el tratamiento automatizado de los datos personales se dispondrá de un sistema de antivirus que garantice en la medida posible el robo y destrucción de la información y datos personales. El sistema de antivirus deberá ser actualizado de forma periódica.
* CORTAFUEGOS O FIREWALL: Para evitar accesos remotos indebidos a los datos personales se velará para garantizar la existencia de un firewall activado en aquellos ordenadores y dispositivos en los que se realice el almacenamiento y/o tratamiento de datos personales.
* CIFRADO DE DATOS: Cuando se precise realizar la extracción de datos personales fuera del recinto donde se realiza su tratamiento, ya sea por medios físicos o por medios electrónicos, se deberá valorar la posibilidad de utilizar un método de encriptación para garantizar la confidencialidad de los datos personales en caso de acceso indebido a la información.
* COPIA DE SEGURIDAD: Periódicamente se realizará una copia de seguridad en un segundo soporte distinto del que se utiliza para el trabajo diario. La copia se almacenará en lugar seguro, distinto de aquél en que esté ubicado el ordenador con los ficheros originales, con el fin de permitir la recuperación de los datos personales en caso de pérdida de la información.
* Por parte de AFISER SERVICIOS INMOBILIARIOS (Encargado del Tratamiento), se contratarán con los servicios de Alojamiento de archivos en la Nube, así como con las distintas aplicaciones móviles y aplicaciones Web, un sistema de copias de seguridad y recuperación de datos fiable.

*Última modificación: 20/05/2018*