SOGEPIMA S.A.
Sociedad de Gestión del Patrimonio
Inmobiliario Municipal de Alcobendas

SOGEPIMA S.A. *

POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Tabla de contenido

1. Propósito, alcance y usuarios

SOGEPIMA, se esfuerza por cumplir con las leyes y reglamentos aplicables relacionadas con la protección de datos personales en el municipio de Alcobendas. Esta política establece los principios básicos por los cuales SOGEPIMA trata los datos personales de ciudadanos, clientes, proveedores, socios comerciales, empleados y otras personas, e indica las responsabilidades de sus departamentos comerciales y empleados mientras trata los datos personales.

Esta política se aplica a SOGEPIMA y sus subsidiarias controladas de forma directa o indirecta que realizan negocios dentro del Área Económica Europea (AEE) o procesan los datos personales de los interesados dentro del AEE.

Los usuarios de este documento son todos los empleados, permanentes o temporales, y todos los contratistas que trabajan en nombre de la Compañía.

2. Documentos de referencia

- El RGPD UE 2016/679 (Reglamento (EU) 2016/679 del Parlamento Europeo y del Consejo del 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 y por el que se deroga la Directiva 95/46/CE)
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales
- Política de protección de datos personales de los empleados
- Política de conservación de datos
- Directrices para el inventario de datos y actividades de tratamiento
- Procedimiento de solicitud de acceso de los interesados
- Directrices para la evaluación de impacto de protección de datos
- Procedimiento de transferencia transfronteriza de datos personales
- ENS nivel MEDIO. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y del Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Procedimiento de aviso de quiebra de seguridad

3. Definiciones

Las siguientes definiciones de términos utilizados en este documento provienen del Artículo 4 del Reglamento General de Protección de Datos de la Unión Europea:

Datos personales: toda información sobre una persona física identificada o identificable("**Interesado**") cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social.

Datos personales sensibles: Datos personales que, por su naturaleza, son particularmente sensibles en relación con los derechos y las libertades fundamentales, ya que el contexto de su tratamiento podría entrañar importantes riesgos para los derechos y las libertades fundamentales. Debe incluirse entre tales datos personales los datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas o filosóficas, afiliaciones sindicales, datos genéticos, datos biométricos, dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física.

Responsable de los datos: La persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento.

Encargado de los datos: La persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

Tratamiento: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Anonimización: Eliminar de forma irreversible la identificación de datos personales de modo que la persona no pueda ser identificada utilizando un tiempo, coste y tecnología razonables, ya sea por el responsable o por cualquier otra persona para identificar a ese individuo. Los principios de tratamiento de datos personales no se aplican a datos anónimos ya que ya no son datos personales.

Seudonimización: El tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable. La seudonimización reduce, pero no elimina completamente, la capacidad de asociar datos personales a un interesado. Como los datos seudonimizados aún se consideran datos personales, el tratamiento de estos datos debe de cumplir con los principios de tratamiento de datos personales.

Tratamiento transfronterizo de datos personales: El tratamiento de datos personales realizado en el contexto de las actividades de establecimientos en más de un Estado miembro de un responsable o un encargado del tratamiento en la Unión, si el responsable o el encargado está establecido en más de un Estado miembro; o el tratamiento de datos personales realizado en el contexto de las actividades de un único establecimiento de un responsable o un encargado del tratamiento en la Unión, pero que afecta sustancialmente o es probable que afecte sustancialmente a interesados en más de un Estado miembro.

Autoridad de control: la autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51;

Autoridad principal de control: La autoridad de control con la responsabilidad principal de tratar con una actividad de tratamiento de datos transfronterizos, por ejemplo cuando un interesado presenta una reclamación sobre el tratamiento de sus datos personales; es responsable, entre otros, de recibir los avisos de quiebra de seguridad de datos, ser notificado sobre la actividad de tratamiento de riesgo y tendrá plena autoridad en lo que respecta a sus deberes para garantizar el cumplimiento de las disposiciones del RGPD UE.

Cada **"autoridad de control local"** mantendrá en su propio territorio y supervisará cualquier tratamiento de datos local que afecte a los interesados o que sea realizado por un responsable o encargado de la UE, o no perteneciente a la UE, cuando el tratamiento se dirige a interesados que residan en su territorio. Sus tareas y poderes incluyen llevar a cabo investigaciones y aplicar medidas administrativas y multas, promover la conciencia pública sobre los riesgos, reglas, seguridad y derechos en relación con el tratamiento de datos personales, así como obtener acceso a las instalaciones del responsable y el encargado, incluido cualquier equipo y medio de tratamiento de datos.

"Principal establecimiento con respecto a un responsable" con establecimientos en más de un estado miembro, es decir el lugar de su administración central en la Unión, a menos que las decisiones sobre los fines y los medios del tratamiento de datos personales se tomen en otro establecimiento del responsable del tratamiento en la Unión y este último tenga el poder para que se implementen tales decisiones, en cuyo caso el establecimiento que haya tomado tales decisiones se debe considerar como el establecimiento principal.

"Principal establecimiento con respecto a un encargado" con establecimientos en más de un estado miembro, es decir el lugar de su administración central en la Unión o, si el encargado careciese de una administración central en la Unión, el lugar en el que se lleven a cabo las principales actividades de tratamiento en el contexto de la las actividades de un establecimiento del encargado tienen lugar en la medida en que el encargado está sujeto a obligaciones específicas en virtud del presente Reglamento.

4. Principios básicos sobre el tratamiento de datos personales

Los principios de protección de datos describen las responsabilidades básicas de las organizaciones que tratan datos personales. El artículo 5 (2) del RGPD estipula que *"el responsable del tratamiento será responsable del cumplimiento de los principios y será capaz de demostrarlo"* de:

4.1. Legalidad, imparcialidad y transparencia

Los datos personales deben ser tratados de forma legal, imparcial y transparente en relación al interesado.

4.2. Limitación de la finalidad

Los datos personales deben ser recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines.

4.3. Minimización de los datos

Los datos personales solicitados serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados. La base jurídica legitimadora principal del tratamiento de datos personales por SOGEPIMA será el cumplimiento de una misión en interés público encargada por el AYUNTAMIENTO DE ALCOBENDAS. SOGEPIMA aplicará anonimización o seudonimización a los datos personales si es posible para reducir el riesgo concerniente a los interesados.

4.4. Exactitud

Los datos personales deben ser exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

4.5. Limitación del plazo de conservación

Los datos personales no deben ser conservados más de lo necesario para los fines para los cuales los datos personales son tratados.

4.6. Integridad y confidencialidad

Teniendo en cuenta el estado de la tecnología y otras medidas de seguridad disponibles, el coste de implementación y la probabilidad y gravedad de los riesgos de los datos personales, SOGEPIMA debe aplicar medidas técnicas u organizativas apropiadas para tratar los datos personales, de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental.

4.7. Responsabilidad proactiva

Los responsables del tratamiento serán responsables del cumplimiento de los principios descritos anteriormente y serán capaces de demostrarlo.

5. Desarrollo de protección de datos en actividades empresariales

Para poder demostrar el cumplimiento con los principios de protección de datos, una organización tiene que desarrollar la protección de datos en sus actividades empresarial.

5.1. Aviso a los interesados

(Ver directrices de tratamiento lícito.)

5.2. Elección y consentimiento del interesado

(Ver directrices de tratamiento lícito.)

5.3. Recogida

SOGEPIMA se esforzará por recoger la menor cantidad posible de datos personales. Si los datos personales se recogen de un tercero, el DPD (Delegado de Protección de Datos) debe de asegurar que los datos personales son recogidos legalmente.

5.4. Uso, conservación, y eliminación

La finalidad, los métodos, la limitación de almacenamiento y el período de conservación de datos personales deben ser coherentes con la información contenida en el Aviso de privacidad. La Compañía debe mantener la precisión, integridad, confidencialidad y pertinencia de los datos personales en función de la finalidad del tratamiento. Se deben utilizar mecanismos de seguridad adecuados diseñados para proteger los datos personales para evitar el robo, uso indebido o abuso de los datos personales y evitar quiebras de seguridad de datos personales. El CISO es responsable del cumplimiento de los requisitos enumerados en esta sección.

5.5. Comunicación a terceros

Siempre que SOGEPIMA utilice un proveedor externo o un socio empresarial para tratar datos personales en su nombre, El Comité de Seguridad de la Información debe asegurar que este encargado proporcionará medidas de seguridad para salvaguardar los datos personales que sean adecuadas a los riesgos asociados. Para tal fin, debe usarse el Cuestionario de cumplimiento del RGPD del encargado.

SOGEPIMA debe exigir de forma contractual al proveedor o al socio empresarial que proporcione el mismo nivel de protección de datos. El proveedor o socio empresarial sólo debe tratar los datos personales para cumplir sus obligaciones contractuales con SOGEPIMA o siguiendo las indicaciones de SOGEPIMA y no para otros fines. Cuando SOGEPIMA trate datos personales junto con un tercero independiente, SOGEPIMA debe especificar de manera explícita sus respectivas responsabilidades y las de un tercero en el pertinente contrato o cualquier otro documento legal vinculante, como el Acuerdo de tratamiento de datos del proveedor.

5.6. Transferencia transfronteriza de datos personales

Antes de transferir datos personales fuera del Área Económica Europea (AEE) deben de emplearse garantías adecuadas incluida la firma de un acuerdo de transferencia de datos, tal como indica la Unión Europea y, si es necesario, debe obtenerse la autorización de la autoridad de protección de datos correspondiente. La entidad que recibe los datos personales debe cumplir con los principios de tratamiento de datos personales establecidos en el Procedimiento de transferencia de datos transfronterizos.

5.7. Derechos de acceso de los interesados

Al actuar como responsable de los datos, SOGEPIMA es responsable de proporcionar a los interesados un mecanismo de acceso razonable que les permita acceder a sus datos personales, así como actualizar, rectificar, borrar o transmitir sus datos personales, cuando corresponda o sea requerido por la ley. El mecanismo de acceso se detallará más en el procedimiento de solicitud de acceso al interesado.

5.8. Portabilidad de datos

Los sujetos de los datos tienen derecho a recibir, previa solicitud, una copia de los datos que nos proporcionaron en un formato estructurado y a transmitir esos datos a otro responsable, de forma gratuita. SOGEPIMA es responsable de garantizar que dichas solicitudes se procesen en un mes, que no sean excesivas y que no afecten a los derechos de los datos personales de otras personas.

5.9. Derecho al olvido

Previa solicitud, los interesados tienen derecho a obtener de SOGEPIMA el borrado de sus datos personales. Cuando SOGEPIMA actúa como responsable, SOGEPIMA debe tomar las medidas necesarias (incluidas medidas técnicas) para informar a terceros que usan o procesan esos datos para cumplir con la solicitud.

6. Directrices de tratamiento lícito

Los datos personales deben ser tratados sólo cuando sea autorizado de forma explícita por la GERENCIA de SOGEPIMA.

SOGEPIMA debe decidir si realizar la evaluación de impacto de protección de datos para cada actividad de tratamiento de datos de acuerdo con Directrices de evaluación de impacto de protección de datos.

6.1. Aviso a los interesados

En el momento de la recogida o antes de recoger datos personales para cualquier tipo de actividades de tratamiento, incluidas, entre otras, la prestación de servicios o actividades comerciales, SOGEPIMA es responsable de informar adecuadamente a los interesados sobre los siguientes tipos de datos personales: los tipos de datos personales recogidos, los fines del tratamiento, los métodos de tratamiento, los derechos de los interesados con respecto a sus datos personales, el período de conservación, las posibles transferencias de datos internacionales, si los datos serán compartidos con terceros y las medidas de seguridad de SOGEPIMA para proteger los datos personales. Esta información es proporcionada a mediante un aviso de privacidad.

Ante múltiples actividades de tratamiento de datos, SOGEPIMA desarrollará avisos diferentes que variarán dependiendo de la actividad de tratamiento y de las categorías de datos personales recogidos; por ejemplo, un aviso puede escribirse para envío por correo electrónico y otro diferente para envío postal.

Cuando los datos personales son compartidos con un tercero, SOGEPIMA asegurará de que los interesados han sido notificados de ello mediante un aviso de privacidad.

Cuando los datos personales se transfieran a un tercer país de acuerdo con la política de transferencia transfronteriza de datos, el aviso de privacidad reflejará claramente dónde y a qué entidad se transfieren los datos personales.

Cuando se recojan datos personales confidenciales, DPD (el delegado de protección de datos) se asegurará de que el Aviso de privacidad indique de forma explícita el propósito para el que se recopilan estos datos personales sensibles.

6.2. Obtención del consentimiento

Siempre que el tratamiento de datos personales se base en el consentimiento del interesado u otros motivos legales, el DPD es responsable de conservar un registro de dicho consentimiento. El DPD es responsable de facilitar a los interesados las opciones para proporcionar el consentimiento y debe informar y garantizar que su consentimiento (siempre que se utilice el consentimiento como base legal para el tratamiento) pueda retirarse en cualquier momento.

Cuando la recogida de datos personales se relaciona con un menor de 16 años, SOGEPIMA se asegurará que el consentimiento paterno se entrega antes de la recogida utilizando la solicitud de consentimiento paterno.

Cuando existan solicitudes para corregir, modificar o destruir los registros de datos personales, SOGEPIMA debe asegurarse de que estas solicitudes se tramiten dentro de un marco de tiempo razonable. SOGEPIMA también registrará las solicitudes y mantendrá un registro de éstas.

Los datos personales solo se deben tratar para el propósito para el que se recogieron inicialmente. En el caso de que SOGEPIMA quiera tratar los datos personales recogidos para otro fin, SOGEPIMA buscará el consentimiento de sus interesados en un escrito claro y conciso. Cualquier solicitud de este tipo debe incluir la finalidad inicial para la que se recogieron los datos, y también el (los) nuevo (s) fin (es) adicional (es). La solicitud también debe incluir el motivo del cambio en la (las) finalidad (es). El delegado de protección de datos es responsable de cumplir con las reglas de este párrafo.

Ahora y en el futuro, SOGEPIMA garantizará que los métodos de recogida cumplan con las leyes pertinentes, las buenas prácticas y las normas en vigor.

SOGEPIMA es responsable de crear y conservar un registro de los avisos de privacidad.

7. Organización y responsabilidades

La responsabilidad de garantizar el tratamiento adecuado de los datos personales recae en todos los que trabajan para SOGEPIMA o con ella y tienen acceso a los datos personales tratados por SOGEPIMA.

Las áreas clave de responsabilidades para el tratamiento de datos personales recaen sobre los siguientes puestos de la organización:

La GERENCIA DE SOGEPIMA, junto con el Consejo de Administración toman decisiones y aprueban las estrategias generales de SOGEPIMA en temas de protección de datos personales.

El **delegado de protección de datos (DPD),** es responsable de gestionar el programa de protección de datos personales y del desarrollo y promoción de políticas de protección integral de datos personales, como se define en la descripción de puesto de delegado de protección de datos;

El **Departamento/asesor de asuntos legales junto con el delegado de protección de datos,** supervisa y analiza los cambios en las leyes y reglamentos sobre datos personales, desarrolla el cumplimiento de los requisitos, y ayuda a los departamentos comerciales en alcanzar sus objetivos de datos personales.

El **CISO,** es responsable de:

- Cumplimiento del ENS nivel MEDIO
- Asegurar todos los sistemas, servicios y equipo utilizado para el almacenamiento de datos cumplan con estándares de seguridad aceptables.
- Llevar a cabo comprobaciones y escaneos regulares para asegurar que el hardware y el software funcionan correctamente.

El **GERENCIA**, es responsable de:

- Aprobar cualquier declaración de protección de datos incluida en comunicaciones tales como correos electrónicos y cartas.
- Abordar cualquier consulta de protección de datos de periodistas o medios de comunicación como periódicos.
- Cuando sea necesario, trabajar con el delegado de protección de datos para garantizar que las iniciativas de marketing cumplan con los principios de protección de datos.

La **Directora de Recursos Humanos** es responsable de:

- Mejorar el conocimiento de todos los empleados sobre la protección de datos personales del usuario.
- Organizar formaciones sobre conocimiento especializado y concienciación en materia de protección de datos personales para los empleados que trabajan con datos personales.
- La protección integral de datos personales de los empleados. Debe asegurar que los datos personales de los empleados se traten en base a fines y necesidades de negocio legítimas de SOGEPIMA.

Los encargados de compras son los responsables de:

- Transmitir las responsabilidades de protección de datos personales a los proveedores, y mejorar los niveles de conocimiento de los proveedores en materia protección de datos personales, así como reducir los requisitos de datos personales a cualquier tercero que esté utilizando un proveedor.

- El departamento de compras debe asegurar que SOGEPIMA se reserva el derecho a auditar a sus proveedores.

8. Respuesta a quiebras de seguridad de datos.

Cuando SOGEPIMA se percata de una quiebra de seguridad de datos personales tanto presunta como real, El CISO, junto el DPD debe realizar una investigación interna y tomar las medidas correctivas adecuadas a tiempo, de acuerdo con la política de quiebra de seguridad de datos. Cuando exista un riesgo para los derechos y las libertades de los interesados, SOGEPIMA notificará a las autoridades de protección de datos relevantes sin dilación indebida y, cuando sea posible, dentro de las 72 horas.

9. Auditoria y responsabilidad proactiva

El departamento JURÍDICO es responsable de auditar qué el resto de los departamentos implementen esta política.

Cualquier empleado que viole esta política estará sujeto a medidas disciplinarias y el empleado también puede estar sujeto a responsabilidades civiles o penales si su conducta viola leyes o reglamentos.

10.Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación	Persona responsable de su almacenamiento	Controles para la protección de registros	Tiempo de conservación
Solicitud de consentimiento del interesado	INTRANET	Delegado de protección de datos	Sólo personal autorizado puede acceder a las solicitudes	10 años
Solicitud de retirada del consentimiento del interesado	INTRANET	Delegado de protección de datos	Sólo personal autorizado puede acceder a las solicitudes	10 años
Acuerdos de tratamiento de datos del proveedor	INTRANET	Delegado de protección de datos	Sólo personal autorizado puede acceder la carpeta	5 años después de que el acuerdo haya expirado
Registro de avisos de privacidad	INTRANET	Delegado de protección de datos	Sólo personal autorizado puede acceder la carpeta	Permanente