



# Manual de Procedimientos Jurídicos

## Cláusulas y procedimientos relativos al tratamiento de datos personales

Uso público

## Información del documento

Título:	Manual de Procedimientos Jurídicos
Descripción:	Cláusulas y procedimientos relativos al tratamiento de datos personales
Calificación	Uso público
Responsable:	Delegado de Protección de Datos
Aprobador por:	Junta de Gobierno Local
Autor/es:	Servicio Transformación Digital y Delegado de Protección de Datos
Fichero:	20240226-STIC-RGPD-01 Manual de Procedimientos Jurídicos-v1.0
Versión:	1.0
Fecha:	26/02/2024

## Control de cambios

Versión	Fecha	Cambios realizados
1.0	26/02/2024	Versión inicial del documento

# Índice

Información del documento.....	I
Control de cambios.....	I
Índice.....	II
1 Introducción.....	1
2 Registro de actividades de tratamiento.....	4
2.1 Procedimiento de actualización del Registro de Actividades de Tratamiento.....	5
3 Organización de la seguridad del tratamiento de los datos.....	6
3.1 Procedimiento general de información.....	6
3.2 Funciones y obligaciones.....	7
3.3 Funciones y obligaciones como Responsable del Tratamiento.....	7
3.4 Funciones y Obligaciones del Delegado de Protección de Datos (DPD).....	8
3.5 Funciones y obligaciones del Responsable de Seguridad.....	10
3.6 Responsables funcionales de los Tratamientos.....	10
3.7 Funciones y obligaciones de los Usuarios.....	11
3.8 Encargados del tratamiento.....	12
3.9 Consecuencias del incumplimiento.....	12
4 Principios relativos al tratamiento y consentimiento del interesado.....	13
4.1 Principios relativos al tratamiento.....	13
4.2 Información que deberá facilitarse al interesado.....	15
5 Derechos del interesado.....	18
5.1 Procedimiento de ejercicio de los derechos de los interesados.....	19
5.2 Derecho de acceso.....	19
5.3 Derecho de rectificación.....	20
5.4 Derecho de supresión («el derecho al olvido»).....	20
5.5 Derecho a la limitación del tratamiento.....	21
5.6 Derecho a la portabilidad de los datos.....	22
5.7 Derecho de oposición.....	22
5.8 Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles.....	23
6 Encargados de Tratamiento.....	24
7 Terceros sin acceso a datos personales.....	26
8 Violación de la seguridad de los datos personales: notificación y comunicación.....	27
9 Análisis y Gestión de Riesgos.....	28
9.1 Procedimiento.....	28
9.1.1 Enfoque de la evaluación de riesgos.....	28
9.1.2 Identificación de riesgos:.....	28
9.1.3 Análisis y valoración de riesgos.....	29
9.2 Procedimiento de Gestión de Riesgos.....	29
9.2.1 Selección de los objetivos de control y los controles para el tratamiento de riesgos.....	30
9.2.2 Formulación del Plan de Tratamiento de Riesgos.....	30
9.3 Implementación del Plan de Tratamiento de Riesgos y de Controles.....	30
10 Evaluación de impacto relativa a la protección de datos personales y consulta previa.....	31



# 1 Introducción

El presente documento proporciona diversas cláusulas y procedimientos de naturaleza jurídica con el objetivo de facilitar modelos de cumplimiento a cuanto, con carácter obligatorio, se establece en el 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 y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos, en adelante, RGPD), y a la Ley 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de derechos digitales, en adelante LOPDgdd. En concreto, se trata de satisfacer el cumplimiento de los principios contemplados en los artículos 5 y ss. RGPD, así como los artículos 4 al 10 LOPDgdd, haciendo posible que los datos personales sean:

- Tratados de manera lícita, leal y transparente en relación con el interesado (principio de licitud, lealtad y transparencia).
- Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (principio de minimización de los datos).
- Exactos y, si fuera necesario, actualizados (principio de exactitud).
- Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (principio de limitación del plazo de conservación).
- Tratados 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, mediante la aplicación de medidas técnicas u organizativas adecuadas (principio de integridad y confidencialidad).

El Ayuntamiento de Roquetas de mar adoptará un enfoque de responsabilidad proactiva, comprometiéndose a implementar medidas anticipadas para garantizar el cumplimiento de la normativa de protección de datos. Esto incluye la realización de evaluaciones de impacto en la protección de datos cuando sea necesario, la designación de un responsable de protección de datos (DPO) si es requerido por la normativa, y la implementación de medidas técnicas y organizativas adecuadas para proteger la seguridad y privacidad de los datos personales de acuerdo con las disposiciones legales aplicables.

Concretamente, este manual comprende los siguientes aspectos:

**Apartado 2 del presente Manual:** registro de actividades de tratamiento que el Ayuntamiento de Roquetas de Mar (en adelante, el Ayuntamiento) está obligado a llevar en virtud de lo dispuesto en el artículo 30 del RGPD, y artículo 31 LOPDgdd.



**Apartado 3 del presente Manual:** funciones y obligaciones del personal del Ayuntamiento en materia de protección de datos. Se añaden modelos de designación de figuras como el Responsable de Seguridad y el Delegado de Protección de Datos.

**Apartado 4 del presente Manual:** modelos de formulario con las cláusulas relativas a la información que deberá facilitarse al interesado cuando los datos personales se obtengan directamente de él (artículo 13 RGPD, y artículos 11.1 y 11.2 LOPDgdd) y cuando los datos personales no se obtengan directamente de él (artículo 14 RGPD y artículo 11.3 LOPDgdd), acompañando la posibilidad de que este manifieste su consentimiento al tratamiento de sus datos personales.

**Apartado 5 del presente Manual:** modelos de solicitud y de respuesta a los derechos legalmente reconocidos a los interesados en los artículos 12 y 15 a 22 RGPD y artículos 12 a 18 LOPDgdd, así como el procedimiento a seguir para la tramitación interna de los mismos. Estos derechos son los siguientes:

- Artículo 15 RGPD / Artículo 13 LOPDgdd. Derecho de acceso del interesado.
- Artículo 16 RGPD / Artículo 14 LOPDgdd. Derecho de rectificación.
- Artículo 17 RGPD / Artículo 15 LOPDgdd. Derecho de supresión («el derecho al olvido»).
- Artículo 18 RGPD / Artículo 16 LOPDgdd. Derecho a la limitación del tratamiento.
- Artículo 19 RGPD / Artículo 32 LOPDgdd. Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento.
- Artículo 20 RGPD / Artículo 17 LOPDgdd. Derecho a la portabilidad de los datos.
- Artículo 21 RGPD / Artículo 18 LOPDgdd. Derecho de oposición.
- Artículo 22 RGPD / Artículo 11 LOPDgdd. Decisiones individuales automatizadas, incluida la elaboración de perfiles.

**Apartado 6 del presente Manual:** modelo con las cláusulas a incorporar en el contrato o en cualquier otro acto jurídico que vincule al encargado del tratamiento respecto del responsable del tratamiento y que establece aspectos tan relevantes como el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y las categorías de interesados, así como los derechos y las obligaciones del encargado del tratamiento y del responsable del tratamiento (artículos 28 y 29 RGPD, y artículos 28, 30 y 33 LOPDgdd).

**Apartado 7 del presente Manual:** modelo con las cláusulas a incorporar para regular la actuación que deben realizar quienes prestan sus servicios al responsable del tratamiento en el desarrollo de su actividad profesional y que, sin formar parte del objeto de su actividad, pueden llegar a conocer datos personales relativos a terceros.

**Apartado 8 del presente Manual:** procedimiento para notificar a la autoridad de control una violación de la seguridad de los datos personales, dentro del plazo y con el contenido legalmente establecido, para

aquellos casos en que esta sea preceptiva (artículo 33 RGPD). Junto al anterior, se acompaña el procedimiento a seguir para comunicar al interesado dicha violación de la seguridad cuando la misma entrañe un alto riesgo para sus derechos y libertades (artículo 34 RGPD).

**Apartado 9 del presente Manual:** procedimiento a seguir para llevar a cabo el Análisis de Riesgos del que surgirán las medidas de seguridad que se deberán implantar para garantizar un nivel de seguridad adecuado (artículo 32 RGPD, y Disposición Adicional Primera LOPDgdd).

**Apartado 10 del presente Manual:** procedimiento a seguir para realizar una evaluación de impacto en la protección de datos personales en aquellas actividades de tratamiento en que sea probable que un tipo de tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas (artículo 35 RGPD, y artículo 28 LOPDgdd). Conectado con este, se añade el procedimiento que contiene las indicaciones a llevar a cabo para consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto muestre que el tratamiento entrañaría un alto riesgo si el responsable del tratamiento no toma las medidas necesarias para mitigarlo (artículo 36 RGPD, y artículo 28 LOPDgdd).

Los modelos que se han incluido en el presente documento deberán ser adaptados a las distintas situaciones concretas que se produzcan en función del tratamiento realizado sobre los datos personales, de las distintas finalidades de dicho tratamiento, de la naturaleza de los datos y de los destinatarios de los mismos.

## 2 Registro de actividades de tratamiento

El artículo 30 del RGPD, y artículo 31 LOPDgdd, obligan al responsable del tratamiento a llevar un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Este registro deberá constar por escrito y en formato electrónico, de manera que esté disponible y a disposición de la autoridad de control que lo solicite

Además, el Ayuntamiento deberá hacer público el Registro de Actividades de Tratamiento, a través de medios electrónicos, conteniendo toda la información establecida en el artículo 30 RGPD.

Dicho registro deberá contener:

- El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- Los fines del tratamiento.
- Una descripción de las categorías de interesados y de las categorías de datos personales.
- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- En su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 RGPD, apartado 1, párrafo segundo, la documentación de garantías adecuadas.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32 RGPD, apartado 1.

Además, el responsable del tratamiento deberá llevar un registro de todas las categorías de actividades de tratamiento efectuadas como encargado del tratamiento.

Este registro deberá contener:

- El nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos.
- Las categorías de tratamientos efectuados por cuenta de cada responsable.
- En su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49 RGPD, apartado 1, párrafo segundo, la documentación de garantías adecuadas.

- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30 RGPD, apartado 1.

El Ayuntamiento cuenta con este registro, que se encuentra publicado en <https://roquetasdemar.es/transparencia/registro-actividades-de-tratamiento/>

## 2.1 Procedimiento de actualización del Registro de Actividades de Tratamiento

Es de vital importancia mantener actualizado el Registro de actividades de tratamiento, regulado en el artículo 30 RGPD, y artículo 31 LOPDgdd, acorde a la realidad del tratamiento de datos personales que se lleve a cabo en el Ayuntamiento, ya que será necesario ponerlo a disposición de la Autoridad de Control en el supuesto de que ésta lo solicite.

Cuando el Delegado de Protección de Datos detecte o se le comunique algún cambio en la estructura de los datos tratados (por ejemplo, creación de un nuevo formulario de recogida de información, desuso de determinada información o solicitud de un nuevo desarrollo), deberá ponerlo en conocimiento del Responsable del Tratamiento para analizarlo e iniciar las modificaciones correspondientes en el Registro de Actividades de Tratamiento.

Asimismo, se fija un periodo de revisión obligatoria anual, a efectos de mantener debidamente actualizado dicho Registro de Actividades de Tratamiento.



### 3 Organización de la seguridad del tratamiento de los datos

El personal del Ayuntamiento con responsabilidad en el tratamiento de los datos personales es el siguiente:

Cargos	Responsables
Responsable del tratamiento	Ayuntamiento de Roquetas de Mar
Responsable de Seguridad	Designado por Decreto de Alcaldía
Delegado de Protección de Datos	Designado por Decreto de Alcaldía con dirección de correo electrónica de contacto: <a href="mailto:dpd@aytoroquetas.org">dpd@aytoroquetas.org</a>
Usuario	Todo el personal con acceso a los datos personales

Tabla 1 - Responsables en el tratamiento de datos personales

#### 3.1 Procedimiento general de información

Todo el personal con responsabilidad en la seguridad de la información tendrá acceso al contenido del presente Manual jurídico, así como a aquella documentación adicional que le fuese necesaria para el ejercicio de sus funciones.

Se deberán adoptar medidas concretas y específicas de formación y divulgación en torno a este Manual jurídico entre el personal del Ayuntamiento tales como:

- El Manual jurídico completo será facilitado a toda persona responsable de la seguridad.
- A cada nueva incorporación se le entregará la normativa a cumplir por toda la plantilla respecto al uso de datos personales.
- Para las incorporaciones que presten servicios y cuya contratación no pase por Recursos Humanos, se le facilitará información sobre sus funciones respecto al tratamiento de datos personales, independientemente de si necesita o no acceso a ellos para el desarrollo de sus funciones.
- Existirán planes de formación periódicos.
- Se utilizará el correo electrónico para divulgar la derogación y/o la entrada en vigor de normativas internas.

#### 3.2 Funciones y obligaciones

Todo el personal que acceda a los datos personales estará obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que expresamente desarrolle, en los términos y condiciones que se establecen en el presente Manual jurídico.

Todas las personas pertenecientes al Ayuntamiento deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de sus funciones.

### 3.3 Funciones y obligaciones como Responsable del Tratamiento

El responsable del tratamiento es la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determina los fines y medios del tratamiento, es decir, el Ayuntamiento de Roquetas de Mar, representado por el Alcalde-Presidente.

El Ayuntamiento debe, entre otras cosas:

- Garantizar la observancia de los principios relativos al tratamiento y aprobar la política, normativa y procedimientos concernientes a la protección de datos personales.
- Designar a quien ejerza como Responsable de Seguridad, y al Delegado de Protección de Datos.
- Adoptar las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos personales y evitar su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural. En particular, difundirá entre el personal las normas de seguridad que afecten al desarrollo de sus funciones, así como las consecuencias en que pudieran incurrir en caso de incumplimiento.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en el Ayuntamiento.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.
- Adoptar las medidas correctoras adecuadas.

### 3.4 Funciones y Obligaciones del Delegado de Protección de Datos (DPD)

El Delegado de Protección de Datos (DPD) es una figura que nace a raíz del Reglamento General de Protección de Datos. El DPD es el punto de conexión entre el Responsable del Tratamiento, los interesados y la autoridad de control.

Será obligatorio designar DPD cuando el responsable del tratamiento:

- Sea una autoridad u organismo público.

- Sus actividades principales consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala.
- Sus actividades principales consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales.

En consecuencia, el Ayuntamiento tendrá la obligación de nombrar un Delegado de Protección de Datos. Una vez designado, deberá ser declarado a la Agencia Española de Protección de Datos. El canal realizar para realizar esta declaración se encuentra en la Sede Electrónica de la Agencia, en concreto en el siguiente e: <https://sedeagpd.gob.es/sede-electronica-web/vistas/formDelegadoProteccionDatos/procedimientoDelegadoProteccion.jsf>

El Delegado de Protección de Datos en el Ayuntamiento de Roquetas de Mar será nombrado por la Alcaldía-Presidencia con dirección de correo electrónica de contacto: [dpd@aytoroquetas.org](mailto:dpd@aytoroquetas.org).

En todo caso, las funciones concretas asociadas al Delegado de Protección de Datos serían:

- Informar y asesorar al Ayuntamiento y a todos los empleados que se ocupen del tratamiento de datos personales, de las obligaciones que se deriven del Reglamento General de Protección de Datos y la LOPDgdd de otras disposiciones relacionadas con la protección de datos.
- Supervisar el cumplimiento del Reglamento General de Protección de Datos y la LOPDgdd en el Ayuntamiento.
- Asesorar acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación.
- Cooperar con la Autoridad de control.
- Actuar como punto de contacto de la Autoridad de Control y de la ciudadanía.

Además, el Delegado de Protección de Datos asesorará y supervisará en el marco de las siguientes tareas:

- Cumplimiento de principios relativos al tratamiento, como los de limitación en la finalidad, minimización o exactitud de los datos.
- Identificación de las bases jurídicas de los tratamientos.
- Valoración de compatibilidad de finalidades distintas de las que originaron la recogida inicial de los datos.
- Existencia de normativa sectorial que pueda determinar condiciones de tratamiento específicas distintas de las establecidas por la normativa general de protección de datos.
- Diseño e implantación de medidas de información a los afectados por los tratamientos de datos.
- Establecimiento de mecanismos de recepción y gestión de solicitudes de ejercicio de derechos por parte de los interesados.

- Valoración de las solicitudes de ejercicio de derechos por parte de los interesados.
- Contratación de encargados de tratamiento, incluido el contenido de los contratos o actos jurídicos que regulen la relación Organización – encargado de tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características del Ayuntamiento y de las razones que justifiquen la transferencia.
- Diseño e implantación de políticas de protección de datos.
- Auditorías de protección de datos.
- Establecimiento y gestión de los registros de actividades de tratamiento.
- Análisis de riesgo de los tratamientos realizados.
- Implantación de las medidas de protección de datos desde el diseño y protección de datos por defecto adecuadas a los riesgos y naturaleza de los tratamientos.
- Implantación de las medidas de seguridad adecuadas a los riesgos y naturaleza de los tratamientos.
- Establecimiento de procedimientos de gestión de violaciones de seguridad de los datos, incluida la evaluación del riesgo para los derechos y libertades de los afectados y los procedimientos de notificación a las autoridades de supervisión y a los afectados.
- Determinación de la necesidad de realización de evaluaciones de impacto sobre la protección de datos.
- Realización de evaluaciones de impacto sobre la protección de datos.
- Relaciones con las autoridades de supervisión.
- Implantación de programas de formación y sensibilización del personal del Ayuntamiento en materia de protección de datos.

El DPD desempeñará todas estas funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.

### 3.5 Funciones y obligaciones del Responsable de Seguridad

Deberá designarse un Responsable de Seguridad encargado de coordinar y controlar las medidas de seguridad definidas en el presente Manual jurídico. En ningún caso, esta designación supone una exoneración de la responsabilidad que corresponde al responsable o encargado del tratamiento.

Si bien la designación del Responsable de Seguridad no es una obligación que se derive expresamente del RGPD, se trata de una figura fundamental para llevar a cabo el cumplimiento del principio de responsabilidad proactiva establecido en dicho texto legal.

El Ayuntamiento cuenta con un Responsable de Seguridad, que deberá llevar a cabo la planificación para la implantación de las medidas de seguridad en materia de protección de datos personales, y que en base a la Disposición Adicional Primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, estas medidas a aplicar a los tratamientos de datos personales se corresponden con las medidas de seguridad del Esquema Nacional de Seguridad.

En base a lo anterior, se definen las siguientes funciones para el Responsable de Seguridad:

- Mantener la seguridad de la información manejada y de los servicios prestados por los sistemas de información en su ámbito de responsabilidad, de acuerdo con lo establecido en la Política de Seguridad de la Información de la organización. La seguridad de los datos personales queda englobada en la seguridad de la información.
- Promover la formación y concienciación en materia de seguridad de la información dentro de su ámbito de responsabilidad, incluyendo la formación en materia de privacidad y protección de datos, en coordinación con el Delegado de Protección de Datos.
- Asesorar al Delegado de Protección de Datos en cuanto a los riesgos de seguridad de los tratamientos de datos personales, en base a los activos de información utilizados para el tratamiento de los datos personales (aplicaciones, elementos hardware, soportes, redes de comunicaciones, dispositivos de red, etc.), aplicando a tal efecto las medidas de seguridad del Esquema Nacional de Seguridad.

### 3.6 Responsables funcionales de los Tratamientos

El Ayuntamiento deberá establecer qué unidades o servicios son los responsables funcionales de los tratamientos. En el caso del Ayuntamiento, los Responsables funcionales de los Tratamientos serán las distintas áreas de gobierno y delegaciones de servicios.

Cada Responsable Funcional del Tratamiento velará por el cumplimiento de sus funciones y obligaciones en su concreto ámbito de actuación.

En términos generales, las funciones y obligaciones de los responsables funcionales del tratamiento vienen designadas y heredadas de las funciones del responsable del tratamiento, y por tanto son:

- Garantizar la observancia de los principios relativos al tratamiento.
- Garantizar el cumplimiento de las medidas técnicas y organizativas definidas.
- Garantizar el cumplimiento de las políticas y normativas aprobadas e implementadas en el Ayuntamiento.
- Asegurar que la realización de tratamientos por cuenta de terceras partes esté regulada en un contrato, que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que la persona encargada del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin

distinto al que figure en dicho contrato, ni los comunicará (ni siquiera para su conservación) a otras personas.

- Adoptar las medidas correctoras adecuadas.
- Mantener actualizado el Registro de Actividades de Tratamiento, en coordinación con el Delegado de Protección de Datos que le asesorará en todo momento, debiendo detectar e informa sobre cualquier modificación necesaria en dicho registro, como pudiera ser la existencia de un nuevo tratamiento, la implantación de nuevos formularios para recabar información, la identificación de tratamiento de datos personales concretos no contemplados anteriormente, la implantación de una nueva aplicación que trate datos personales, la utilización de los datos personales para otras finalidades no contempladas inicialmente, etc.

### 3.7 Funciones y obligaciones de los Usuarios

Todo el personal que acceda a datos personales está obligado a conocer y observar las medidas, normas, protocolos, reglas y estándares que afecten a las funciones que desarrolla. Esto incluye las Normativas y Procedimientos de Seguridad que emanan de la Política de Seguridad en el ámbito del Esquema Nacional de Seguridad, y que puedan aplicar a los tratamientos de datos personales.

Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo. Esta obligación de guardar secreto subsistirá aun después de finalizar las relaciones contractuales con el Ayuntamiento.

Ante cualquier duda respecto a cómo actuar frente al tratamiento de determinada información, siempre se debe consultar a quien ejerce como Responsable de Seguridad, o al Delegado de Protección de Datos si la duda se refiere al tratamiento de datos personales.

El usuario, además, deberá cumplir con lo estipulado en la norma de buen uso de los medios tecnológicos que el Ayuntamiento ponga a su disposición para el desempeño de sus funciones, incluyendo normas de buen uso de:

- Correo Electrónico
- Internet
- Portátil y dispositivos móviles
- Memorias USB
- Impresoras, fotocopiadoras y faxes
- Repositorios y carpetas de red

Finalmente, el usuario se compromete al cumplimiento de las normas y políticas de mesas limpias y puesto despejado referido a cualquier información, incluidos los datos personales, así como al bloqueo de su puesto de trabajo cuando no esté presente.

### 3.8 Encargados del tratamiento

Los encargados del tratamiento deben mantener la confidencialidad de los datos que manejan, tienen la obligación de seguir las instrucciones del Ayuntamiento y deben responsabilizarse del correcto tratamiento informático de los datos del Ayuntamiento.

El Ayuntamiento, cuando actúe como encargado del tratamiento, aplicará las mismas medidas y controles que cuando lo haga como responsable del tratamiento.

Se deberá firmar un contrato o convenio entre el Ayuntamiento y el encargado del tratamiento, en el que se utilicen las cláusulas necesarias para definir la relación entre ambos relativa al tratamiento y acceso a los datos personales por parte del encargado (ver Apartado 6 del presente documento).

### 3.9 Consecuencias del incumplimiento

El personal que intervenga en cualquier fase del tratamiento de los datos personales y que incumpla lo descrito en el presente Manual jurídico o, en su caso, en los documentos, normas o procedimientos relacionados con el Manual jurídico y con la protección de datos personales, deberá saber que podrá ser sometido al régimen sancionador/disciplinario existente en el Ayuntamiento, sin perjuicio de las posibles consecuencias civiles y penales a que hubiera lugar, en su caso.

## 4 Principios relativos al tratamiento y consentimiento del interesado

### 4.1 Principios relativos al tratamiento

Los usuarios con acceso a datos personales deberán tratarlos conforme a los siguientes principios esenciales, que pretenden garantizar el cumplimiento del fin último de protección de las personas físicas en lo que respecta al tratamiento de los datos personales:

- **Licitud, lealtad y transparencia:** los datos serán tratados de manera lícita, leal y transparente en relación con el interesado.
- **Licitud:** el tratamiento sólo será lícito si cumple, al menos alguna de las circunstancias de licitud recogidas en el artículo 6.1 del RGPD (consentimiento, ejecución de un contrato, obligación legal, protección de intereses vitales, interés público, ejercicio de poderes públicos o interés legítimo):
  - El interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos.

El Ayuntamiento deberá ser capaz de demostrar que el interesado consintió el tratamiento de sus datos personales.

En cualquier caso, la persona afectada tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de todo ello. Será tan fácil retirar el consentimiento como darlo.

Si el consentimiento del interesado se diese en el contexto de una declaración escrita que también se refiera a otros asuntos, el Ayuntamiento estará a lo estipulado en el artículo 6 de la LOPDgdd: la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. Esta declaración no será vinculante si constituye infracción del RGPD/LOPDgdd.

Es necesario solicitar el consentimiento para cesiones de datos a otras entidades, siempre que dicha cesión no se encuentre establecida por Ley.

No podrá supeditarse la ejecución del contrato a que el afectado consienta el tratamiento de los datos personales para finalidades que no guarden relación con el mantenimiento, desarrollo o control de la relación contractual.

- El tratamiento es necesario para la **ejecución de un contrato** en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.



- El tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable al Ayuntamiento.
  - El tratamiento es necesario para proteger **intereses vitales** del interesado o de otra persona física.
  - El tratamiento es necesario para el cumplimiento de una misión realizada en **interés público** o en el **ejercicio de poderes públicos** conferidos al Ayuntamiento.
  - El tratamiento es necesario para la satisfacción de **intereses legítimos** perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.
- **Lealtad**: toda persona tiene derecho a saber cuáles de sus datos personales se tratan y con qué finalidad, y que dicho tratamiento se hace de acuerdo a la ley y no de forma fraudulenta.
  - **Transparencia**: exige que el Ayuntamiento tome todas las medidas que sean oportunas para poder facilitar al interesado información relativa al tratamiento en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo. Esta información podrá ser facilitada por escrito o por otros medios (electrónicos o verbales).
  - **Limitación de la finalidad**: los datos personales serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados posteriormente de manera incompatible con dichos fines. El tratamiento posterior de estos datos no se considerará incompatible con los fines iniciales si se realizan con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos.
  - **Minimización de los datos**: los datos personales serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados.
  - **Exactitud**: los datos personales deberán ser exactos y, si fuera necesario, actualizados. Se adoptarán medidas para que se supriman o rectifiquen sin dilación aquellos que sean inexactos con respecto a los fines para los que se tratan.
  - **Limitación del plazo de conservación**: los datos personales serán mantenidos de forma que sea posible la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento. Los datos personales podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas. Se deben definir los plazos de conservación de los datos personales según las necesidades del Ayuntamiento y lo dispuesto por la legislación vigente, en especial, por la normativa de archivo y documentación.

- **Integridad y confidencialidad:** los datos personales serán tratados de tal manera que se garantice una seguridad adecuada, incluida la protección contra el tratamiento no autorizado y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas.

Por último, el RGPD establece la obligación de cumplir con el principio de **responsabilidad proactiva**. En este sentido, el Ayuntamiento será responsable del cumplimiento de todos estos principios del tratamiento señalados anteriormente y, además, deberá ser capaz de demostrar dicho cumplimiento.

## 4.2 Información que deberá facilitarse al interesado

Los artículos 13 y 14 RGPD, y el artículo 11 de la LOPDgdd, obligan al responsable del tratamiento a informar al interesado de todo cuanto, en principio, rodea el tratamiento que se va a realizar de sus datos personales. Como es lógico, la información que se habrá de proporcionar en el supuesto en el que los datos personales no se obtengan directamente del interesado será mayor, pues, en términos generales, incluirá, además de la información recogida en el artículo 13 RGPD, las categorías de datos personales del interesado objeto de tratamiento y la fuente de la que proceden tales datos.

De acuerdo con el artículo 13 y 14 RGPD, y el artículo 11 de la LOPDgdd, cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento deberá facilitarle, en el momento en que tales datos personales se obtengan, toda la información, aplicable al caso concreto de que se trate.

Cuando los datos no se obtengan directamente del interesado, la información deberá ser facilitada:

- Dentro de un plazo razonable, y a más tardar dentro de un mes.
- Si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado.
- Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.

La información que se facilite al interesado será la siguiente:

- La identidad y los datos de contacto del responsable del tratamiento y, en su caso, de su representante.
- Los datos de contacto del delegado de protección de datos, en su caso.
- Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
- Cuando el tratamiento sea necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, cuáles son esos intereses legítimos.
- Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.
- En su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de

las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, todos ellos RGPD, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.

- El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos.
- Cuando el tratamiento esté basado en el consentimiento del interesado, la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada.
- El derecho a presentar una reclamación ante una autoridad de control.
- La fuente de la que proceden estos datos personales y, en su caso, si proceden de fuentes de acceso público.
- Si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos.
- La existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, RGPD, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.
- Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente recogida en el artículo 14.2 RGPD.

La obligación de información anterior no será pertinente en la medida en que el interesado ya disponga de la información.

Cuando la información no se obtenga directamente del interesado, la obligación de informar tampoco será pertinente en los siguientes casos:

- La comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, RGPD, o en la medida en que la citada obligación pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas

adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información.

- La obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado.
- Los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.

Para cumplir con el citado deber de información, el Ayuntamiento dispondrá de una relación de cláusulas informativas, que deberán ser integradas en los diferentes formularios de recogida de datos que se empleen para tal cometido, además de ser remitidas a los interesados cuyos datos sean obtenidos de fuentes o vías ajenas a los mismos.

Esta información podrá proporcionarse al interesado mediante dos niveles o capas:

- Una **capa básica** (o primer nivel de información), donde se recogerán resumidamente los aspectos relativos al tratamiento de datos personales. El deber de información se entenderá cumplido por el Ayuntamiento siempre y cuando de la opción al interesado a acceder a la segunda capa de información o información detallada.
- Una **capa detallada** (o segundo nivel de información), donde se recogerá toda la información exigida por el artículo 13 del RGPD, y artículos 11.1 y 11.2 de la LOPDgdd.

## 5 Derechos del interesado

Los artículos 15 a 22 RGPD, y artículos 12 a 18 LOPDgdd, reconocen al interesado la posibilidad de ejercitar una serie de derechos en relación con el tratamiento de sus datos personales.

Quien solicita el ejercicio del derecho debe ser la propia persona titular de los datos. Si se trata de los datos de una persona menor de edad y/o con discapacidad, el representante legal ejercerá los derechos en su nombre. La solicitud deberá ir dirigida al Ayuntamiento por un medio que permita acreditar el envío y la recepción de la misma.

En el caso de personas fallecidas, salvo que la persona fallecida lo hubiese prohibido expresamente o así lo establezca una ley, para el acceso, rectificación o supresión de los datos, podrán solicitar el acceso al ejercicio de los derechos las personas vinculadas al fallecido por razones familiares o de hecho, así como sus herederos o las personas o instituciones a las que el fallecido hubiese designado expresamente. Si la persona fallecida fuese menor de edad o persona con discapacidad, podrán ejercer esos derechos sus representantes legales o, en el marco de sus competencias, por el ministerio fiscal. Además, para las personas con discapacidad podrán ejercer los derechos de acceso, rectificación o supresión quienes hubiesen sido designados para el ejercicio de funciones de apoyo, siempre que el ejercicio de los derechos se entiendan comprendidos en las medidas de apoyo prestadas por el designado.

Se ha de dar respuesta a cualquier solicitud, aun cuando no se hubiera utilizado el procedimiento establecido, siempre que la persona interesada hubiera usado un medio que permita acreditar el envío y la recepción y siempre que la solicitud contenga los requisitos pertinentes.

La solicitud incluirá la siguiente información mínima para que sea cursada:

- Identificación de la persona titular de los datos: nombre, apellidos y fotocopia del DNI de la persona interesada o de su representante legal, si procede. No obstante, la fotocopia del DNI podrá ser sustituida siempre que se acredite la identidad por cualquier otro medio válido.
- Petición en que se concreta la solicitud.
- Domicilio a efectos de notificaciones, fecha y firma de la persona solicitante.
- Documentos acreditativos de la petición que se formula, en su caso.

Los medios y canales de recepción de peticiones, tanto de personal interno como de personal externo, podrán ser: correo electrónico, correo postal o cualquier otro tipo de comunicación formal o cumplimentación de formularios, dirigidos al Ayuntamiento.

Los plazos de resolución de cada una de las solicitudes de ejercicio de derechos serán, por regla general, de un mes (artículo 12.3 RGPD). Todas las solicitudes recibidas a través de las diferentes vías de entrada se trasladarán inmediatamente al delegado de protección de datos, quién deberá valorar si están completas o, por el contrario, carecen de algún requisito necesario para proceder a la ejecución del derecho. El

Ayuntamiento deberá contestar a la solicitud que se le dirija, debiendo utilizar cualquier medio que permita acreditar el envío y la recepción. Si la solicitud no reúne los requisitos necesarios, se deberá solicitar la subsanación de los mismos a la persona interesada.

El Ayuntamiento adoptará las medidas oportunas para garantizar que todo el personal del Ayuntamiento que acceda a datos personales puedan informar del procedimiento a seguir a la persona afectada para el ejercicio de sus derechos.

## 5.1 Procedimiento de ejercicio de los derechos de los interesados

El artículo 12.2 del RGPD, y el artículo 12 de la LOPDgdd, imponen al Responsable del Tratamiento, es decir, al Ayuntamiento de Roquetas de Mar, la obligación de facilitar al interesado el ejercicio de los derechos recogidos en el citado texto normativo.

Este ejercicio de derechos deberá hacerse efectivo de acuerdo con una serie de plazos y requisitos recogidos en el RGPD y en la LOPDgdd y en la demás normativa de protección de datos aplicable.

Para que el Ayuntamiento pueda cumplir con esta obligación, cuenta con un procedimiento a seguir con cada solicitud de ejercicio de derechos por parte de los interesados, así como los modelos de solicitud y respuesta, tanto en caso estimatorio como desestimatorio.

## 5.2 Derecho de acceso

Es el derecho del interesado a obtener del Ayuntamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:

- Los fines del tratamiento.
- Las categorías de datos personales de que se trate.
- Los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales.
- El plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.
- La existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento.
- El derecho a presentar una reclamación ante una autoridad de control.
- Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.

- la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, RGPD, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.

Además, cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 RGPD relativas a la transferencia.

### 5.3 Derecho de rectificación

El derecho de rectificación es el derecho del interesado a que se modifiquen los datos inexactos o incompletos que le conciernan. El interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.

Para el ejercicio de este derecho, el interesado debe indicar a qué datos se refiere, aportando la documentación que lo justifique.

### 5.4 Derecho de supresión («el derecho al olvido»)

El derecho de supresión es el derecho del interesado a que se supriman los datos personales cuando concurra alguna de las siguientes circunstancias:

- Los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- El interesado retira el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), RGPD, o el artículo 9, apartado 2, letra a), RGPD, y este no se base en otro fundamento jurídico.
- El interesado se opone al tratamiento con arreglo al artículo 21, apartado 1, RGPD, y no prevalecen otros motivos legítimos para el tratamiento, o el interesado se opone al tratamiento con arreglo al artículo 21, apartado 2, RGPD.
- Los datos personales han sido tratados ilícitamente.
- los datos personales deben suprimirse para el cumplimiento, en su caso, de una obligación legal establecida en el Derecho nacional o comunitario que se aplique al Ayuntamiento.
- Los datos personales se han obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1, RGPD.

Para el ejercicio de este derecho, el interesado debe indicar a qué datos se refiere, aportando la documentación que lo justifique.

Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto anteriormente, a suprimir dichos datos, el Ayuntamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.

Existe la posibilidad de la denegación del ejercicio del derecho de supresión en los siguientes supuestos:

- Para ejercer el derecho a la libertad de expresión e información.
- Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho nacional o comunitario al Ayuntamiento, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos, en su caso, al Ayuntamiento.
- Por razones de interés público en el ámbito de la salud pública, de conformidad con el artículo 9, apartado 2, letras h) e i), y apartado 3, RGPD.
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, RGPD, en la medida en que el derecho de supresión pudiera hacer imposible u obstaculizar gravemente el logro de los objetivos de dicho tratamiento.
- Para la formulación, el ejercicio o la defensa de reclamaciones.

## 5.5 Derecho a la limitación del tratamiento

Es el derecho del interesado a obtener del responsable del tratamiento la limitación del tratamiento de los datos. En este caso, el Ayuntamiento procederá a limitar el tratamiento cuando se cumpla alguna de las siguientes condiciones:

- El interesado impugna la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
- El tratamiento es ilícito y el interesado se opone a la supresión de los datos personales y solicita en su lugar la limitación de su uso.
- El Ayuntamiento ya no necesita los datos personales para los fines del tratamiento, pero el interesado los necesita para la formulación, el ejercicio o la defensa de reclamaciones.
- El interesado se opone al tratamiento en virtud del artículo 21, apartado 1, RGPD, mientras se verifica si los motivos legítimos del Ayuntamiento prevalecen sobre los del interesado.

Cuando el tratamiento de datos personales se haya limitado por concurrir alguna de las causas anteriores, dichos datos solo podrán ser objeto de tratamiento, con excepción de su conservación, con el consentimiento del interesado o para la formulación, el ejercicio o la defensa de reclamaciones, o con miras a la protección de los derechos de otra persona física o jurídica o por razones de interés público importante nacional o



comunitario. Todo interesado que haya obtenido la limitación del tratamiento será informado por el Ayuntamiento antes del levantamiento de dicha limitación.

## 5.6 Derecho a la portabilidad de los datos

Es el derecho del interesado a recibir los datos personales que le incumban y que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable del tratamiento al que los hubiera facilitado. Para ello, será necesario que concurra alguna de las siguientes circunstancias:

- Que el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), todos ellos del RGPD.
- El tratamiento se efectúe por medios automatizados.

Al ejercer su derecho a la portabilidad de los datos de acuerdo con las exigencias anteriores, el interesado tendrá derecho a que los datos personales se transmitan directamente del Ayuntamiento a otro responsable del tratamiento cuando sea técnicamente posible.

El ejercicio del derecho a la portabilidad de los datos se entenderá sin perjuicio del ejercicio del derecho de supresión. Tal derecho no se aplicará al tratamiento que sea necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos, en su caso, al Ayuntamiento.

El derecho a la portabilidad de los datos no afectará negativamente a los derechos y libertades de otros.

## 5.7 Derecho de oposición

Es el derecho del interesado a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6, apartado 1, letra e), RGPD) o en la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero (artículo 6, apartado 1, letra f), RGPD), incluida la elaboración de perfiles sobre la base de dichas disposiciones.

El Ayuntamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.

A más tardar en el momento de la primera comunicación con el interesado, el derecho de oposición será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.

En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.

Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, RGPD, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada, en su caso, por razones de interés público.

## 5.8 Derecho a no ser objeto de decisiones individuales automatizadas, incluida la elaboración de perfiles

Es el derecho del interesado a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.

Este derecho no se aplicará si la decisión:

- Es necesaria para la celebración o la ejecución de un contrato entre el interesado y el Ayuntamiento.
- Está autorizada por el Derecho nacional o comunitario que se aplique al Ayuntamiento y que establezca, asimismo, medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.
- Se basa en el consentimiento explícito del interesado.

En los casos a que se refieren los apartados a) y c) anteriores, el Ayuntamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener, en su caso, intervención humana por parte del Ayuntamiento, a expresar su punto de vista y a impugnar la decisión.

Las decisiones que permiten exceptuar la aplicación de este derecho no podrán basarse en categorías especiales de datos personales contempladas en el artículo 9, apartado 1, RGPD, salvo que se aplique el artículo 9, apartado 2, letra a) o g), RGPD, y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

## 6 Encargados de Tratamiento

De acuerdo con el artículo 28 RGPD, y los artículos 28, 30 y 33 LOPDgdd, cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiados, de manera que el tratamiento sea conforme con los requisitos del RGPD y garantice la protección de los derechos del interesado.

El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del Ayuntamiento y establezca 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. Dicho contrato o acto jurídico deberá establecer, en particular, que el encargado del tratamiento:

- Tratará los datos personales únicamente siguiendo instrucciones documentadas del Ayuntamiento inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al Ayuntamiento de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.
- Garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria.
- Tomará todas las medidas necesarias de conformidad con el artículo 32 RGPD, y que, en la Disposición Adicional Primera de la LOPDgdd, se concretan en la implantación de las medidas del Esquema Nacional de Seguridad aplicables a los datos personales.
- No recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del Ayuntamiento. En este último caso, el encargado informará al Ayuntamiento de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dándole, así, la oportunidad de oponerse a dichos cambios.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del Ayuntamiento, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el Ayuntamiento y el encargado del tratamiento inicial, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el Ayuntamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

- Asistirá al Ayuntamiento, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados.
- Ayudará al Ayuntamiento a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36 RGPD, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado del tratamiento.
- A elección del Ayuntamiento, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros.
- Pondrá a disposición del Ayuntamiento toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable. En este caso, el encargado del tratamiento informará inmediatamente al Ayuntamiento si, en su opinión, una instrucción infringe el RGPD u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 RGPD o a un mecanismo de certificación aprobado a tenor del artículo 42 RGPD podrá utilizarse como elemento para demostrar la existencia de las garantías suficientes a que se refiere el artículo 28 RGPD.

En cualquier caso, si un encargado del tratamiento infringe el RGPD al determinar los fines y medios del tratamiento, será considerado responsable del tratamiento con respecto a dicho tratamiento.

El Ayuntamiento ha elaborado modelos de contrato a celebrar con quienes traten datos personales por cuenta del Ayuntamiento en condición de encargados del tratamiento, las cláusulas que el Ayuntamiento deberá incluir en los pliegos, así como la cláusula de confidencialidad a firmar por los empleados del encargado del tratamiento que vayan a acceder a los datos del Ayuntamiento.

## 7 Terceros sin acceso a datos personales

Esta circunstancia se produce en el caso de contratación de un servicio por parte del Ayuntamiento que no conlleve el acceso a datos personales para su tratamiento, pero sí el acceso a los locales donde se encuentran los sistemas de tratamiento.

En estas circunstancias, el Ayuntamiento deberá establecer las medidas que limiten el acceso a los datos personales y la entidad que presta el servicio deberá comprometerse a cumplir con su deber de secreto respecto a los datos personales que pudiera conocer con motivo de la prestación del servicio.

Las medidas de seguridad previstas por el Ayuntamiento para limitar el acceso a datos personales son las siguientes:

- No se concederá acceso lógico a ningún servidor, equipo o documento que contenga datos personales.
- Cuando el personal que presta el servicio tenga que acceder a salas o locales donde se estén almacenando o tratando este tipo de datos, será acompañado siempre por personal del Ayuntamiento.
- No se dejarán documentos en papel que contengan datos personales desatendidos en las mesas u otros lugares.
- Las salas y/o despachos permanecerán siempre cerrados cuando no haya personal en su interior.
- El personal que desempeña funciones que no implican tratamiento de datos personales será convenientemente informado de su prohibición de acceder a este tipo de datos. No obstante, y para el caso en que finalmente deba acceder a los mismos, se obligará a firmar a este personal una cláusula de confidencialidad en el tratamiento de este tipo de datos.
- Cuando se trate de personal ajeno, el contrato de prestación de servicios deberá recoger expresamente la prohibición de acceder a los datos personales incluidos en los ficheros o tratamientos y la obligación de secreto respecto de los mismos que el personal hubieran podido conocer con motivo de la prestación del servicio.
- El Ayuntamiento ha elaborado un modelo de cláusula de confidencialidad para pliegos de condiciones de contratos que no impliquen acceso a datos del Ayuntamiento.

## 8 Violación de la seguridad de los datos personales: notificación y comunicación

El RGPD, en los artículos 33 y 34, obliga a los responsables del tratamiento a notificar a la Autoridad de Control competente cualquier brecha de seguridad de datos personales.

Se define como violación de seguridad de los datos personales a todas aquellas brechas de seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.

En caso de que la brecha de seguridad suponga un alto riesgo para los derechos y libertades de las personas físicas, el Ayuntamiento deberá notificar de tal circunstancia a los interesados que hayan podido quedar afectados por dicha brecha.

La notificación deberá realizarse en el plazo de 72 horas desde que se tuvo conciencia de la misma, por lo que es fundamental que el proceso de gestión de las brechas esté perfectamente definido, de manera que no dé a lugar a posibles dilaciones indebidas que provoquen incumplimientos de la normativa de protección de datos.

Esta obligación queda recogida. Para su cumplimiento, el Ayuntamiento dispondrá del Procedimiento de Notificación de Violaciones de Seguridad, donde se determinará los pasos a seguir para documentar y, en su caso, notificar cuando sea necesario este tipo de incidentes a la autoridad de control y a los interesados. Este procedimiento se encuentra englobado en el Procedimiento de Seguridad del ENS relativo a la Gestión de Ciberincidentes.

## 9 Análisis y Gestión de Riesgos

El artículo 32 del RGPD establece que, teniendo en cuenta, entre otros, los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo.

De este precepto legal se desprende la obligación de realizar un Análisis de Riesgos del que resulten las medidas de seguridad que serán necesarias aplicar en el Ayuntamiento para alcanzar un nivel de seguridad adecuado.

En la Disposición Adicional Primera de la LOPDgdd, se especifica que el Responsable del Tratamiento, es decir el Ayuntamiento de Roquetas de Mar, deberá aplicar a los tratamientos de datos personales las medidas de seguridad que correspondan de las previstas en el Esquema Nacional de Seguridad.

### 9.1 Procedimiento

El análisis de riesgos es de aplicación a los tratamientos de datos personales que realiza el Ayuntamiento cuyo alcance cubre los siguientes grupos de activos: Actividades/Servicios del Ayuntamiento, equipamiento informático, aplicaciones informáticas, infraestructura de comunicaciones (red LAN), personal afectado (usuario general y personal TIC).

A continuación, se describen los pasos a seguir para realizar el Análisis de Riesgos:

#### 9.1.1 Enfoque de la evaluación de riesgos

Se ha elegido la metodología MAGERIT para evaluar los riesgos, metodología que se considera adecuada en cuanto que cubre las necesidades del negocio en materia de seguridad de la información y contempla los requisitos legales y reglamentarios.

#### 9.1.2 Identificación de riesgos:

- Identificación de activos y de los propietarios de los mismos siguiéndose la metodología MAGERIT (entendiéndose como propietario a la persona o entidad con responsabilidades sobre el activo en términos de su administración, desarrollo, mantenimiento, uso, seguridad, no a la persona con derechos de propiedad sobre el activo).
- Identificación de amenazas por cada activo y de las vulnerabilidades bajo las que podrían actuar amenazas.
- Identificación de salvaguardas, es decir, de los mecanismos de protección de los activos. Estas salvaguardas serán tanto de carácter organizativo y técnico (anexo II del ENS) como jurídico (RGPD).

- Identificación del impacto de las amenazas sobre los activos en términos de la confidencialidad, integridad y disponibilidad.

Los pasos anteriores se llevan a cabo mediante la herramienta PILAR y con el personal TI del Ayuntamiento. Se dispone de un Informe de Valoración de Activos que incluye la relación de activos, así como la valoración de los activos esenciales respecto a criterios específicos.

### 9.1.3 Análisis y valoración de riesgos

- Evaluación de los efectos en la actividad del Ayuntamiento que pudiesen derivarse de la materialización de los fallos de seguridad en términos de pérdida de confidencialidad, integridad o disponibilidad.
- Evaluación de la probabilidad de fallos de seguridad considerando las amenazas identificadas, las vulnerabilidades, los impactos y los controles implementados sobre los activos.
- Estimación de los niveles de riesgos.
- Determinación de si los riesgos son aceptables o necesitan tratamiento de acuerdos a los criterios de aceptación.

La evaluación de la probabilidad de fallos y la estimación de los niveles de riesgo es llevada a cabo por el personal TI del Ayuntamiento y se realiza igualmente con la herramienta PILAR.

Como resultado de las actividades anteriores se dispone de un Plan de Tratamiento de Riesgos o Plan de Mejora de la Seguridad, que cuantifica el riesgo al que están sometidos los activos identificados e indica un riesgo residual, en vías de mejora, gracias a la actividad de gestión de riesgos.

## 9.2 Procedimiento de Gestión de Riesgos

Pasos a seguir para realizar una Gestión de Riesgos:

Pueden darse diversas opciones:

- Aplicación de controles.
- Asumir los riesgos conforme a los criterios de aceptación.
- Evitarlos.
- Transferirlo a otras partes (compañía de seguros, proveedores, ...).

El Ayuntamiento opta por la aplicación de controles o refuerzo de la efectividad de los ya existentes, y se asume todos aquellos niveles de riesgo por debajo de riesgo medio.



### 9.2.1 Selección de los objetivos de control y los controles para el tratamiento de riesgos

Se seleccionan los objetivos de control y controles necesarios para disminuir el riesgo o bien, se refuerza el nivel de eficacia de algunos que ya están implantados.

Se han seleccionado los controles de la norma de referencia dando lugar a una serie de líneas de actuación.

Como resultado de las actividades anteriores se dispone del Plan de Tratamiento de Riesgos o Plan de Mejora de la Seguridad en el que aparece el nivel de cumplimiento actual de cada uno de los controles de la norma y el nivel de cumplimiento planificado.

Dicho informe define las líneas de actuación necesarias para conseguir el aumento del grado de cumplimiento y el mapa de riesgos resultante (riesgo residual).

### 9.2.2 Formulación del Plan de Tratamiento de Riesgos

El Plan de Tratamiento de Riesgos o Plan de Mejora de la Seguridad incluye las líneas de acción previstas para disminuir los niveles de riesgo a los nuevos niveles residuales.

El Ayuntamiento acepta temporalmente el riesgo actual (calculado tras el análisis de riesgos) condicionado a la existencia del plan de tratamiento de riesgos. Asimismo, el Ayuntamiento aprueba los niveles de riesgo residual que se obtendrían como resultado del tratamiento de riesgos. La aceptación de ambos riesgos queda reflejada con la firma del documento Plan de Tratamiento de Riesgos.

El Ayuntamiento se considera además dueño del riesgo en el sentido que en ella recae la responsabilidad de aprobar el Plan de Tratamiento de Riesgos.

## 9.3 Implementación del Plan de Tratamiento de Riesgos y de Controles

Las mencionadas líneas de acción que se describen en el Plan de Tratamiento de Riesgos son tratadas y gestionadas a través de la herramienta PILAR.

## 10 Evaluación de impacto relativa a la protección de datos personales y consulta previa

El RGPD incorpora una nueva obligación para quien actúa como responsable del tratamiento: evaluar, antes del tratamiento, el impacto de las operaciones de tratamiento en la protección de los datos personales en aquellos supuestos en que sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y las libertades de las personas físicas. Al realizar esta evaluación de impacto, el responsable del tratamiento podrá recabar el asesoramiento del delegado de protección de datos, caso de que cuente con esta figura.

De acuerdo al artículo 35 RGPD, y al artículo 28 LOPDgdd, la evaluación de impacto se requiere, en particular, en los siguientes casos:

- Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar; tratamiento a gran escala de las categorías especiales de datos personales o de los datos personales relativos a condenas e infracciones penales; u observación sistemática a gran escala de una zona de acceso público.
- Tratamiento con fines de investigación en salud pública y, en particular, biomédica.

De conformidad con el artículo 35.4 RGPD, la autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos, que se recoge en la Guía para una Evaluación de Impacto en la protección de datos personales, elaborada por la Agencia Española de Protección de Datos:

- Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados.
- Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años.
- Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados, su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad), encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio o que puedan afectar a su dignidad o su integridad personal.

- Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things) o el desarrollo y la construcción de ciudades inteligentes (Smart Cities).
- Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad, como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro.
- Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados.
- Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibéndolos o poniéndolos en común de cualquier forma.
- Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la AEPD.
- Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas.
- Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica.
- Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos.

En los casos en que no esté claro si la evaluación de impacto es obligatoria, se recomienda hacerla, ya que se trata de un mecanismo para ayudar a los responsables de tratamientos a cumplir con la normativa en materia de protección de datos personales.

Como podemos advertir, la evaluación de impacto estará orientada a asegurar preventivamente que, cuando las operaciones de tratamiento puedan comportar un alto riesgo, se tomen medidas para reducir, dentro de lo posible, el peligro de afectar negativamente a los derechos y libertades de las personas físicas, impidiendo o limitando su ejercicio o contenido. Más concretamente, los objetivos básicos que persigue la evaluación de impacto son:

- Asegurar que el proyecto cumple con las exigencias normativas durante todo el ciclo del tratamiento.
- Identificar los riesgos y amenazas a los que pueden estar expuestos los tratamientos, a fin de eliminarlos o mitigarlos.

- Prevenir problemas futuros que puedan originar sanciones económicas, pérdidas y daños a la reputación del Ayuntamiento.

Por su parte, el artículo 36 RGPD, y el artículo 28 LOPDgdd, incorporan una nueva obligación para quien, actuando como responsable del tratamiento, debe realizar una evaluación de impacto para determinar si un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entraña un alto riesgo para los derechos y las libertades de las personas físicas.

Esta obligación consiste en consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto muestra que dicho tratamiento entrañaría un alto riesgo si el responsable del tratamiento no toma medidas para mitigarlo.

Cuando la autoridad de control considere que el tratamiento previsto podría infringir el RGPD, en particular cuando el responsable del tratamiento no haya identificado o mitigado suficientemente el riesgo, deberá, en un plazo de ocho semanas desde la solicitud de la consulta, asesorar por escrito al responsable del tratamiento y, en su caso, al encargado del tratamiento. Dicho plazo podrá prorrogarse seis semanas, en función de la complejidad del tratamiento previsto. La autoridad de control informará al responsable del tratamiento y, en su caso, al encargado del tratamiento de tal prórroga en el plazo de un mes a partir de la recepción de la solicitud de consulta, indicando los motivos de la dilación. Estos plazos podrán suspenderse hasta que la autoridad de control haya obtenido la información solicitada a los fines de la consulta.

El Ayuntamiento cuenta con una herramienta que se ha configurado para el análisis de necesidad de EIPD en base a una serie de cuestiones pertinentes al tratamiento. Adicionalmente, se han considerado las diferentes amenazas a las que pueden estar expuestos los tratamientos, así como las salvaguardas para mitigarlos. La herramienta permite el cálculo del nivel de riesgo actual, así como del riesgo residual en función de las medidas implantadas en el momento de realización del análisis.