DIPUTACIÓN DE ALMERÍA

Manual de Procedimientos Jurídicos

(RGPD)

Abril de 2020

HISTORIAL DE CAMBIOS

Nombre del fichero	Versión	Resumen de cambios producidos	Fecha
STIC-RGPD-01 Manual de Procedimientos Jurídicos	1.00	Primera versión.	22/04/2020

CLASIFICACIÓN

CONFIDENCIAL
Nota de confidencialidad: La información contenida en este documento es USO INTERNO. Es responsabilidad del Área o Departamento receptor de este documento su distribución interna en base a la necesidad de conocer la información aquí contenida.

CONTROL DE DIFUSIÓN

DISTRIBUCIÓN: **Diputación de Almería** Seguridad de la Información

Índice

1 Introducción

El presente documento proporciona diversas normas 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).

Concretamente, este manual se estructura en los siguientes apartados:

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

b) **Apartado 3 del presente Manual:** funciones y obligaciones del personal de la Diputación 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.

c) **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.

d) **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

e) **Apartado 6 del presente Manual**: según establece La disposición adicional séptima de la LOPDgdd es necesario establecer los criterios para la identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.

f) **Apartado 7 del presente Manual,** diferenciación de los roles de encargado de tratamiento, cesionario de datos, corresponsable de tratamiento o tercero sin tratamiento de datos personales.

g) **Apartado 8 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).

h) **Apartado 9** del presente Manual, en virtud de la normativa en materia de protección de datos la Diputación de Almería debe disponer de un procedimiento para para el cumplimiento de la cesión de datos.

i) **Apartado 10 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.

j) **Apartado 11 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).

k) **Apartado 12 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).

l) **Apartado 13 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).

m) **Apartado 14 del presente Manual** - El Articulo 39 del RGPD-UE establece entre las funciones del Delegado de Protección de Datos, en su punto 1.b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia

de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes..

n) **Apartado 15 del presente Manual:** 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, la Diputación deberá hacer público el Registro de Actividades de Tratamiento, a través de medios electrónicos, conteniendo toda la información establecida en el artículo 30 RGPD. Actualmente, el RAT está publicado en la página web corporativa de la Diputación de Almería, así como en su sede electrónica.

Dicho registro deberá contener:

a) 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,
b) los fines del tratamiento;
c) una descripción de las categorías de interesados y de las categorías de datos personales;
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;
e) 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;
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;

g) 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, la Diputación de Almería deberá llevar un registro de todas las categorías de actividades de tratamiento que asume como encargada del tratamiento.

Este registro deberá contener:

a) 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;
b) Las categorías de tratamientos efectuados por cuenta de cada responsable;
c) 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;
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30 RGPD, apartado 1.
e) La Diputación de Almería hará público el registro de Actividades de Tratamiento, a través de medios electrónicos, conteniendo toda la información establecida.

La Diputación hará público el Registro de Encargos de Tratamiento, a través de medios electrónicos, conteniendo toda la información establecida.

2.1 Procedimiento de actualización del Registro de Actividades de Tratamiento

Es de vital importancia tener 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 la Diputación, 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.

El procedimiento de actualización del RAT y del Registro de Encargos de Tratamiento se realizarán por Resolución de Presidencia.

3 Organización de la seguridad del tratamiento de los datos

El personal de la Diputación con responsabilidad en el tratamiento de los datos personales es el siguiente:

Cargos	Responsables
Responsable del tratamiento	Diputación de Almería
Responsable de Seguridad	Será designado por Resolución de Presidencia en el marco del cumplimiento del ENS y a la vez asumirá la secretaría del Comité de Seguridad de la Información.
Delegado de Protección de Datos	El Comité de Seguridad de la Información tiene asignadas las funciones de Delegado de Protección de Datos. Hasta que la Diputación de Almería designe al Delegado de Protección de Datos, todas las funciones que corresponden a éste serán desempeñados por el Comité de Seguridad de la Información Se designa al Jefe del Servicio de Organización e Información y Secretario del Comité de Seguridad de la Información de esta Diputación, como interlocutor para la Agencia de Protección de Datos Personales y/u otras autoridades de control y como persona de contacto para la ciudadanía, en lo que respecta al ejercicio de sus derechos en materia de protección de datos personales respecto de la propia Diputación de Almería, y de las entidades locales sobre las que el Comité de Seguridad de la Información asuma las funciones del Delegado de Protección de Datos.
Usuario	Todo el personal con acceso a los datos personales
Responsable funcional de Tratamientos de Datos	Designados por Resolución de Presidencia. Máxima jerarquía técnica sobre la que recae las funciones del Responsable del tratamiento en uno o más tratamientos concretos de la Organización.

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 de la Diputación tales como:

- El Manual Jurídico completo será facilitado a toda persona responsable de la seguridad.
- A cada nueva incorporación se le entregará un pack de bienvenida en el que se incluye la normativa a cumplir por toda la plantilla respecto al uso de datos personales.
- Para terceros 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 a propuesta del DPD tanto dentro del Plan Agrupado de Formación como acciones formativas propias de la Diputación.
- Se utilizará el correo electrónico, o el sistema de aviso de la aplicación de Gestión de protección de Datos (PRODATOS), para divulgar la derogación y/o la entrada en vigor de normativas internas.

3.2 Funciones y obligaciones

Todas las personas que trabajan en la Diputación deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de sus funciones.

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.

En el catálogo de funciones de la Diputación de Almería se recogerá una función genérica para todos los puestos en relación a esta obligatoriedad.

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, la Diputación de Almería, y más concretamente su Presidente.

La Diputación 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 por Resolución de Presidencia a quien ejerza como Responsable de Seguridad, quien deberá coordinar y controlar las medidas definidas en el Manual jurídico.
- Designar al Delegado de Protección de Datos, por Resolución de Presidencia.
- 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 la Diputación.
- 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:

a) Sea una autoridad u organismo público
b) Sus actividades principales consistan en operaciones de tratamiento que requieran una observación habitual y sistemática de interesados a gran escala
c) 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, la Diputación tiene la obligación de nombrar un Delegado de Protección de Datos. Una vez designado, deberá ser declarado al Consejo de Transparencia y Protección de Datos de Andalucía.

Las funciones del Delegado de Protección de Datos recaen en el Comité de Seguridad de la Información. El Jefe del Servicio de Organización e Información asume las funciones de interlocutor ante el Consejo de Transparencia y Protección de Datos de Andalucía y ante otras autoridades de control y para la ciudadanía, en lo que respecta al ejercicio de sus derechos de protección de datos personales respecto de la propia Diputación de Almería, y de las entidades locales sobre las que el Comité de Seguridad de la Información asuma las funciones del Delegado de Protección de Datos.

El DPD desempeñará las siguientes funciones concretas:

- Informar y asesorar a la Diputación y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del Reglamento General de Protección de Datos y de otras disposiciones de protección de datos.
- Supervisar el cumplimiento de lo dispuesto en el Reglamento General de Protección de Datos, de otras disposiciones de protección de datos y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales.
- Supervisar la asignación de responsabilidades, la concienciación y la formación del personal que participa en las operaciones de tratamiento de datos personales y las auditorías correspondientes.
- Ofrecer asesoramiento 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 para cuestiones relativas al tratamiento de datos personales, incluida la consulta previa a la que se refiere el artículo 36 del RGPD, además de cualquier otro tipo de consulta.
- Proponer los responsables funcionales de las actividades de tratamientos al Presidente de la Diputación de Almería.

Además, el DPD 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 Diputación de Almería – Encargado de Tratamiento.
- Identificación de los instrumentos de transferencia internacional de datos adecuados a las necesidades y características de la Diputación 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 de la Diputación 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

Por Resolución de Presidencia se designa el Responsable de Seguridad encargado de coordinar y controlar las medidas de seguridad definidas en el ENS y concretadas 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.

La Diputación ha designado un Responsable de Seguridad, cuya misión es coordinar e implantar las medidas de seguridad para cumplir con el ENS y con Disposición adicional primera. Medidas de seguridad en el ámbito del sector público, de la Ley Orgánica 3/2108 de 5 de diciembre LOPDGdd.

En concreto, se definen las siguientes funciones para los responsables de seguridad:

- Garantizar la seguridad de los datos, implantando y haciendo cumplir las medidas, procedimientos, instrucciones y normativas establecidas en el Manual jurídico y en sus anexos.
- Colaborar con el responsable del tratamiento en la difusión del Manual jurídico y de sus anexos.
- Mantener un listado actualizado del personal autorizado a acceder a los sistemas de información
- Realizar los controles periódicos establecidos para verificar el cumplimiento del Manual jurídico y de sus anexos.
- Analizar los informes de auditoría y proponer al responsable del tratamiento las medidas correctoras oportunas.
- Cumplir con el procedimiento de ejercicio de derechos de los interesados según las solicitudes recibidas.
- Autorizar la recuperación de datos tratados.

- Habilitar y mantener un registro de incidencias para la información que esté bajo su responsabilidad. Este registro deberá estar disponible para cualquier revisión o auditoría.

3.6 Funciones y obligaciones de los Responsables funcionales de los Tratamientos

La Diputación deberá establecer qué puestos de la estructura técnica son los responsables funcionales de cada una de las actividades de tratamiento incluidas en el Registro de Actividades de Tratamiento.

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 la Diputación.
- 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.
- Adoptar las medidas técnicas y organizativas necesarias para velar por el cumplimiento de la legislación vigente en materia de protección de datos personales, Transparencia y Esquema Nacional de Seguridad en las dependencias adscritas a su dirección/jefatura/coordinación.
- Autorizar permisos de acceso a los usuarios sobre los recursos, (automatizados y no automatizados) que se encuentran bajo su responsabilidad y que sean estrictamente necesarios para el desarrollo de las funciones del trabajador.
- Realizar un inventario y un registro de entrada y salida de soportes.
- Autorizar la salida de soportes con datos personales que se encuentren bajo su responsabilidad.
- Autorizar la generación de copias o reproducción de documentos.
- Mantener un listado de personal autorizado a la información en soporte papel.

- Revisar los permisos y perfiles de acceso de la información que se encuentra bajo su gestión.

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 la Diputación.

Ante cualquier duda respecto a cómo actuar frente al tratamiento de determinada información, siempre se debe consultar al Delegado de Protección de Datos.

3.7.1 Las obligaciones que recaen sobre todo usuario son las siguientes:

- Información a la que se tiene acceso:
  - Obtener la información por medios lícitos y no sacar información de la Diputación, salvo en los casos que lo requieran las funciones asignadas y, en su caso, previa autorización correspondiente.
  - No utilizar el ordenador para trabajos ajenos a los realizados en la Diputación ni introducir o instalar software ilegal o programas no autorizados.
  - Reducir al máximo el almacenamiento de información confidencial. Cuando esta haya dejado de ser necesaria debe ser eliminada. En caso de crear archivos para uso temporal que contengan datos personales, debe asegurarse su eliminación cuando estos hayan dejado de utilizarse.
  - No utilizar las unidades locales del PC para almacenar información con datos personales. Se recomienda el uso adecuado de carpetas de red y su empleo en lugar del disco duro como repositorio de información.
  - Cumplir con los procedimientos internos de la entidad, como, por ejemplo, la gestión de incidencias o tratamiento de soportes.
  - Proporcionar ayuda al Responsable de Seguridad en lo que se refiere a mantener la calidad de los datos, lo cual implica controlar:

  - Que la información contenida en cada Actividad de Tratamiento únicamente sea tratada en relación con las finalidades para las que se haya obtenido.
  - Que los datos sean exactos, estén actualizados y sean suprimidos cuando hayan dejado de ser necesarios.

- Identificación o autenticación (claves y contraseñas de usuario):
  - Los identificadores son personales e intransferibles. No comunicar a nadie los identificadores de usuario y palabras claves de acceso al sistema, ni anotarlos en lugares visibles o de fácil localización.
  - Bloquear el ordenador siempre que se ausente de su puesto de trabajo.
  - Responsabilizarse de la confidencialidad de sus contraseñas y, en caso de que sean conocidas fortuita o fraudulentamente por otras personas, debe comunicarlo como incidencia de seguridad y proceder a su cambio inmediato.
  - Se debe cumplir la política de contraseñas establecida para cada aplicación, siguiendo las sugerencias hechas por los responsables en el ámbito informático en cuanto a su formato, longitud y periodicidad de cambio.
  - Utilizar contraseñas que combinen números, letras (mayúsculas y minúsculas) y caracteres especiales.
  - Cuando se acceda por primera vez a un sistema o aplicación, modificar, inmediatamente después, la contraseña asignada por una contraseña propia.
  - Cambiar las contraseñas de acceso a las aplicaciones con una frecuencia, como mínimo, anual.
  - No solicitar por sí mismo el acceso a las aplicaciones ni la asignación de permisos. Para ello, se pondrá en contacto con su responsable jerárquico superior, quien realizará la solicitud si el acceso está justificado para la ejecución de sus funciones.
- Correo electrónico:
  - El correo electrónico es una herramienta del organismo, por lo que deberá ser utilizada para tales fines. Se prohíbe expresamente:
    - Que una persona empleada haga uso de una cuenta de correo ajena o permitir a una tercera persona el uso de la suya propia.
    - Envío de mensajes difamatorios, calumniadores, amenazantes o abusivos.
    - Transmitir material de la Diputación, a menos que esté adecuadamente protegido y autorizado.
    - Las personas empleadas no podrán realizar visitas a sitios web con pornografía o que promuevan actividades ilegales.

  - Transmitir identificadores, contraseñas, configuraciones de las redes locales o direcciones a través de Internet.
  - Abrir correos, adjuntos a correos o pulsar en links a menos que sean conocidos y de confianza.
- Se recomienda tener cuidado con el envío de datos personales por medio del correo electrónico, tanto en el cuerpo del mensaje como en anexos. Si se realiza, tratar esos mensajes y anexos como temporales y borrarlos en cuanto dejen de ser necesarios.

- Ficheros temporales

Los ficheros temporales que se creen extrayendo datos personales de las aplicaciones corporativas para la ejecución de una determinada tarea o proceso no deben mantenerse indefinidamente ni en el ordenador ni en un directorio de red y, una vez finalizada dicha tarea o proceso, hay que eliminarlos.

- Ordenadores portátiles y resto de infraestructura:
- Mantenerlos siempre controlados (no dejar en lugares públicos, taxis, etc.) para evitar su sustracción.
- Reducir y/o eliminar la información que no vaya a ser utilizada.

3.7.2 Respecto a Actividades de Tratamiento no automatizados (uso del papel) que contengan datos personales

La confidencialidad de los datos se consigue también a través del cuidado del entorno de trabajo, evitando que la información pueda ser de fácil acceso por cualquiera.

Para ello, se establecen varias actuaciones de obligado cumplimiento:

- **Mesas limpias**: el usuario, cada vez que se ausente de su mesa de trabajo o bien cuando termine su jornada laboral, deberá retirar toda aquella documentación que contenga información que pudiera tener carácter confidencial.
- **Utilización de impresoras**: el usuario deberá asegurarse de que no quedan documentos impresos en la bandeja de salida que contengan datos protegidos.
- **Utilización de fax**: cuando se vaya a enviar un fax, se debe avisar siempre al destinatario para que esté pendiente de la recogida de la información. Cuando se espera recibir por este medio información con datos personales, es importante solicitar a la persona que lo envía que nos avise para prestar atención a la llegada de la documentación.

- **Utilización de fotocopiadoras:** siempre que se utilicen para reproducir copias de determinada documentación, el usuario se debe asegurar que, al terminar, recoge todos los documentos, incluido el original.
- Utilizar los **dispositivos** destinados al efecto para desechar el material correspondiente, es decir, si se elimina documentación en las papeleras, esta deberá romperse previamente, de forma que la información en ella contenida quede ininteligible. En caso contrario, depositarla en los contenedores destinados al efecto o en las destructoras de papel.
- **Distribución de la documentación**: se deben adoptar medidas cautelares que eviten accesos no autorizados. Se pueden producir diferentes situaciones en el movimiento de los ficheros en papel:
- **Envíos fuera de la sede de trabajo**: para estos envíos, siempre debe salir en sobre cerrado o dispositivo de seguridad similar que evite accesos de terceros, de manera que no se pueda realizar consulta, copia o reproducción de la misma.
- **Envíos dentro de la sede de trabajo**: para envíos dentro del mismo edificio en el que se encuentra nuestro puesto de trabajo, se deben utilizar los medios implantados en la Diputación, de manera que se eviten accesos no deseados.
- Verificar que las personas a las que se entrega la documentación original o una copia de la misma la han recibido.
- No retirar de las dependencias soportes o ficheros no automatizados sin la debida autorización.

3.7.3 Compromiso de confidencialidad para empleados.

La Diputación Provincial de Almería deberá asegurarse de que todo el personal quede debidamente informado de todos los deberes y obligaciones que le apliquen en el ejercicio de sus funciones. Asimismo, el personal de Diputación Provincial de Almería deberá obligarse a cumplir dichas consideraciones mientras esté ligado contractualmente a la Diputación. Para ello se debe elaborar un documento de confidencialidad que contenga los derechos y obligaciones relativos a seguridad de la información.

Para asegurar el cumplimiento por parte del personal, el Servicio de Personal procederá de la siguiente manera:

a) Notificar a todo el personal en activo de la Resolución de Presidencia por la cual se aprueba el documento que recoge el compromiso de confidencialidad.

b) Toda persona que se incorporé a un puesto de la Diputación de Almería deberá firmar el documento de confidencialidad.

El documento de confidencialidad deberá recoger:

- Información al empleado del tratamiento que se va a realizar de sus datos personales.
- Declaración de compromiso de confidencialidad y deber de secreto.
- Obligado cumplimiento de las normativas de buen uso de los medios tecnológicos que sean puestos a su disposición (normativas externas y políticas internas propias de la Diputación Provincial de Almería)
- Monitorización de los activos por parte de la Diputación Provincial de Almería, y devolución de los mismos a la finalización del contrato

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 de la Diputación y deben responsabilizarse del correcto tratamiento informático de los datos de la Diputación.

Se deberá firmar un contrato o convenio entre la Diputación 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)

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

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 la Diputación de Almería, 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):
    a) El interesado dio su **consentimiento** para el tratamiento de sus datos personales para uno o varios fines específicos.

       La Diputación 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, la Diputación 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

b) 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.
c) El tratamiento es necesario para el cumplimiento de una **obligación legal** aplicable a la Diputación.
d) El tratamiento es necesario para proteger **intereses vitales** del interesado o de otra persona física.
e) El tratamiento es necesario para el cumplimiento de una misión realizada en **interés público** o en el **ejercicio de poderes públicos** conferidos a la Diputación.
f) El tratamiento es necesario para la satisfacción de **intereses legítimos**.

- Lealtad: para las personas físicas deberá quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

- Transparencia: exige que la Diputación 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. Sólo podrá prorrogarse ese plazo en caso de que se trate 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 de la Diputación 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, la Diputación 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.

La información que se facilite al interesado será la siguiente:

a) La identidad y los datos de contacto del responsable del tratamiento y, en su caso, de su representante.
b) Los datos de contacto del delegado de protección de datos, en su caso.
c) Los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento.
d) 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.

e) Los destinatarios o las categorías de destinatarios de los datos personales, en su caso.

f) 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.

g) El plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo.

h) 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.

i) 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.

j) El derecho a presentar una reclamación ante una autoridad de control.

k) 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;

l) 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.

m) 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.

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

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

a) Dentro de un plazo razonable, y a más tardar dentro de un mes

b) 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
c) Si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.
d) La fuente de la que proceden estos datos personales y, en su caso, si proceden de fuentes de acceso público.

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

a) 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;
b) 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, o
c) 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, la Diputación dispone de una relación de cláusulas informativas para cada una de las actividades de tratamiento aprobadas por Resolución de Presidencia, 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 la Diputación siempre y cuando dé 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.

En la primera capa se proporcionará información sobre los datos del Responsable de Tratamiento, la finalidad, el ejercicio de derechos RGPD, y los datos necesarios para acceder a la información adicional de la segunda capa.

En la segunda capa, se incluye toda la información necesaria para cumplir con lo estipulado en RGPD y LOPDgdd en relación con el deber de información: datos del Responsable del Tratamiento y del Delegado de Protección de Datos, finalidad, base jurídica (legitimación), periodo de conservación, información completa para solicitud de ejercicio de derechos, categorías de datos tratados, y destinatarios (cesiones).

- Consulta de datos personales en poder de otras administraciones

La Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, establece en su artículo 28, que la entrega de documentación en el marco de la tramitación de un procedimiento administrativo es un derecho y un deber.

Por un lado, de acuerdo con el apartado 1 del citado artículo, los interesados tienen el deber de aportar los datos y documentos exigidos por las Administraciones Públicas de acuerdo con lo dispuesto en la normativa aplicable.

Por otro lado, tal y como recoge el apartado 2, el interesado tiene el derecho a no aportar aquella información que, bien porque ha sido generada por las Administraciones Públicas o bien porque ha sido presentada anteriormente, ya está en poder de estas. De esta forma, se aplica el principio de una sola vez, clave en el desarrollo de la administración electrónica y que tiene por objeto eliminar la carga administrativa innecesaria que se produce cuando los usuarios deben suministrar la misma información más de una vez a distintos organismos del sector público.

La disposición adicional octava de la LOPDdgg dice: Cuando se formulen solicitudes por cualquier medio en las que el interesado declare datos personales que obren en poder de las Administraciones Públicas, el órgano destinatario de la solicitud podrá efectuar en el ejercicio de sus competencias las verificaciones necesarias para comprobar la exactitud de los datos. Así la Diputación Provincial de Almería para estos casos procederá según las orientaciones de la AEPD.

- Modelos de Carteles y Clausulas de información.

Para cumplir con la obligación de Informar, se han previsto para cada Actividad de Tratamiento modelos de cláusulas de información para los formularios de recogida de la misma, así como modelos de carteles informativos, que se pueden ver y descargar a través de un código QR línea con la correspondiente Actividad de Tratamiento.

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, los titulares de la patria potestad podrán ejercitar en nombre y representación de los menores de catorce años los derechos de acceso, rectificación, cancelación, oposición o cualesquiera otros que pudieran corresponderles en el contexto de la LOPDgdd. La solicitud deberá ir dirigida a la Diputación por un medio que permita acreditar el envío y la recepción de esta.

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: sede electrónica, presencialmente en cualquiera de las oficinas de registro de la Diputación de Almería, correo postal o cualquier otro tipo de comunicación formal o cumplimentación de formularios, dirigidos a la Diputación.

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; para ello, se cumplimentará el modelo creado al efecto, que permitirá valorar si están completas o, por el contrario, carecen de algún requisito necesario para proceder a la ejecución del derecho. La Diputación 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.

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

Cuando la Diputación cometiese alguna de las infracciones a los que se refieren los artículos 72 al 74 de la LOPDgdd, la autoridad de protección de datos que resulte competente dictará resolución sancionando a las mismas con apercibimiento. La resolución establecerá asimismo las medidas que proceda adoptar para que cese la conducta o se corrijan los efectos de la infracción que se hubiese cometido.

La resolución se notificará al responsable o encargado del tratamiento, al órgano del que dependa jerárquicamente, en su caso, y a los afectados que tuvieran la condición de interesado, en su caso.

Sin perjuicio de lo establecido en el apartado anterior, la autoridad de protección de datos propondrá también la iniciación de actuaciones disciplinarias cuando existan indicios suficientes para ello. En este caso, el procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario o sancionador que resulte de aplicación.

Asimismo, cuando las infracciones sean imputables a autoridades y directivos, y se acredite la existencia de informes técnicos o recomendaciones para el tratamiento que no hubieran sido debidamente atendidos, en la resolución en la que se imponga la sanción se incluirá una amonestación con denominación del cargo responsable y se ordenará la publicación en el Boletín Oficial del Estado o autonómico que corresponda.

Se deberán comunicar a la autoridad de protección de datos las resoluciones que recaigan en relación con las medidas y actuaciones a que se refieren los apartados anteriores.

Se comunicarán al Defensor del Pueblo o, en su caso, a las instituciones análogas de las comunidades autónomas las actuaciones realizadas y las resoluciones dictadas al amparo de este artículo.

Cuando la autoridad competente sea la Agencia Española de Protección de Datos, esta publicará en su página web con la debida separación las resoluciones referidas a las entidades del apartado 1 del artículo 77 de la LOPDgdd, con expresa indicación de la identidad del responsable o encargado del tratamiento que hubiera cometido la infracción.

Cuando la competencia corresponda al Consejo de Transparencia y Protección de Datos de Andalucía, se le dará publicidad a estas resoluciones según lo que disponga su normativa específica

La contestación al ciudadano se realizará a través de una notificación de la Resolución de Presidencia.

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, la Diputación de Almería, 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 a 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 la Diputación pueda cumplir con esta obligación, cuenta con el procedimiento ***"Ejercicio de derechos"***, 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 de la Diputación 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:

a) Los fines del tratamiento.
b) Las categorías de datos personales de que se trate.

c) 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.
d) De ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo.
e) 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.
f) El derecho a presentar una reclamación ante una autoridad de control.
g) Cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen.
h) 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, si procede, 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:

a) Los datos personales ya no son necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.

b) 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.
c) 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.
d) Los datos personales han sido tratados ilícitamente.
e) 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 a la Diputación.
f) 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, si procede, 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, la Diputación, 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:

a) Para ejercer el derecho a la libertad de expresión e información.
b) Para el cumplimiento de una obligación legal que requiera el tratamiento de datos impuesta por el Derecho nacional o comunitario a la Diputación, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos, en su caso, a la Diputación.
c) 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.

d) 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, la Diputación procederá a limitar el tratamiento cuando se cumpla alguna de las siguientes condiciones:

a) El interesado impugna la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos.
b) 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.
c) La Diputación 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.
d) El interesado se opone al tratamiento en virtud del artículo 21, apartado 1, RGPD, mientras se verifica si los motivos legítimos de la Diputación prevalecen sobre los del interesado.
e) Para la formulación o la defensa de las reclamaciones

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 la Diputación antes del levantamiento de dicha limitación.

5.6 Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento

La Diputación deberá comunicar cualquier rectificación o supresión de datos personales o limitación del tratamiento a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. De igual modo, la Diputación informará al interesado acerca de dichos destinatarios, si este así lo solicita.

5.7 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:

a) 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, y
b) 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 de la Diputación 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, a la Diputación.

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

5.8 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.

La Diputación 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.

5.9 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:

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

El Responsable del Tratamiento no debe llevar a cabo el tratamiento basado en decisiones individuales automatizadas, incluida la elaboración de perfiles, salvo que se aplique una de las excepciones descritas anteriormente. Dichas excepciones no aplicarán cuando éstas se basen en tratamiento de categorías especiales de datos personales, salvo en los casos en los que el interesado haya proporcionado su consentimiento explícito para el tratamiento de dichos datos personales, o cuando el tratamiento sea necesario por razones de un interés público esencial. No

obstante, en los casos en los que aplique la excepción, la Diputación debe adoptar medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.

En los casos a que se refieren los apartados a) y c) anteriores, la Diputación 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 de la Diputación, a expresar su punto de vista y a impugnar la decisión.

6 Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos

La disposición adicional séptima de la LOPDgdd, obliga a que el responsable del tratamiento, a la publicación de un acto administrativo que contuviese datos personales del afectado, identifique al mismo mediante su nombre y apellidos, añadiendo cuatro cifras numéricas aleatorias del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente. Cuando la publicación se refiera a una pluralidad de afectados estas cifras aleatorias deberán alternarse.

Cuando se trate de la notificación por medio de anuncios, particularmente en los supuestos a los que se refiere el artículo 44 de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, se identificará al afectado exclusivamente mediante el número completo de su documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

Cuando el afectado careciera de cualquiera de los documentos mencionados en los dos párrafos anteriores, se identificará al afectado únicamente mediante su nombre y apellidos. En ningún caso debe publicarse el nombre y apellidos de manera conjunta con el número completo del documento nacional de identidad, número de identidad de extranjero, pasaporte o documento equivalente.

La Diputación de Almería por Resolución de Presidencia, siguiendo las recomendaciones de la Agencia Española de Protección de Datos, ha adoptado las medidas para llevar a cabo esta anonimización de datos.

7 Evaluación de terceros

En cuanto a las relaciones con terceros, la normativa de protección de datos establece una serie de roles en función de la responsabilidad, tipo de acceso y obligaciones en el tratamiento de los datos.

En este sentido, los terceros ajenos a la Diputación Provincial de Almería, podrán ser considerados encargados del tratamiento, cesionarios de datos o, en caso de no hacer ningún tipo de tratamiento, terceros sin acceso a datos.

La determinación de estos roles no es tarea fácil, por lo que el objetivo de este documento es aportar una serie de pautas para ayudar a discernir en qué caso nos encontramos y, a partir de ahí, qué consecuencias se derivan de dicha relación.

Los posibles roles que puede asumir un tercero ajeno a la Diputación de Almería son:

- Encargado del Tratamiento: persona física o jurídica, autoridad pública u otro organismo que trate datos personales por cuenta de DIPUTACIÓN PROVINCIAL DE ALMERÍA y en su nombre.
- Cesionario de datos: la persona física o jurídica, autoridad pública u otro organismo a la que la Diputación Provincial de Almería cede datos en base a una de las causas de legitimación del artículo 6 del Reglamento General de Protección de Datos (en adelante, RGPD).
- Corresponsable del tratamiento: dos o más responsables que determinen conjuntamente los objetivos y los medios del tratamiento
- Tercero sin acceso a datos: terceros con los que DIPUTACIÓN PROVINCIAL DE ALMERÍA tiene una relación contractual de la cual no se deriva el tratamiento de datos personales.

8 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.

Para demostrar la existencia de las garantías suficientes, de los encargados de tratamiento, a que se refiere el artículo 28 RGPD, se puede utilizar los siguientes mecanismos:

- La adhesión del encargado del tratamiento a un código de conducta aprobado a tenor del artículo 40 RGPD.
- Un mecanismo de certificación aprobado a tenor del artículo 42 RGPD.
- Un informe de cumplimiento realizado por una empresa especializada en consultorías y/o auditorias sobre Protección de Datos Personales.
- En casos excepcionales se puede recurrir a una declaración jurada del posible encargado de tratamiento en la que indique que Medidas Técnicas y Organizativas lleva a cabo para cumplir con la protección de los datos personales

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 de la Diputación 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:

a) Tratará los datos personales únicamente siguiendo instrucciones documentadas de la Diputación 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 a la Diputación de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público.
b) 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.
c) 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.
d) No recurrirá a otro encargado sin la autorización previa por escrito, específica o general, de la Diputación. En este último caso, el encargado informará a la Diputación 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 de la Diputación, 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 la Diputación 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 la Diputación por lo que respecta al cumplimiento de las obligaciones del otro encargado.

e) Asistirá a la Diputación, 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.

f) Ayudará a la Diputación 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.

g) A elección de la Diputación, 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.

h) Pondrá a disposición de la Diputación 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 a la Diputación 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.

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.

Por Resolución de presidencia se aprobarán los modelos de cláusulas a utilizar por la Diputación de Almería para contratos a celebrar con quienes traten datos personales por cuenta de la Diputación en condición de encargados del tratamiento, las cláusulas que la Diputación 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 de la Diputación:

9 Cesión de datos personales

Como cualquier otra actividad de tratamiento, las cesiones de datos están sujetas al cumplimiento del 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 (en adelante, RGPD), y a la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (LOPDgdd), por lo que se deberán extremar cierta precauciones de cara a cumplir con las disposiciones de las citadas Normativas en relación a las cesiones de datos.

Se entiende por cesión de datos toda aquella transferencia de datos personales responsabilidad de la Diputación de Almería a otro responsable del tratamiento, para que este tercero trate los datos para sus propias finalidades y por su propia cuenta.

Es importante diferenciar que las transferencias de datos a encargados del tratamiento, es decir, entidades con las que la Diputación de Almería mantiene una relación contractual para que lleve a cabo una serie de acciones en nombre y por cuenta de ella, y que implican el tratamiento de datos personales, como por ejemplo gestorías de nóminas, asesorías jurídicas, consultoras, etc. no se considerarán cesiones de datos, por lo que no entran dentro del alcance de este procedimiento.

La Diputación de Almería contará con un procedimiento de Cesión de Datos a Terceros aprobado por Resolución de Presidencia.

Las responsabilidades en la cesión de datos serán de:

- **El Personal de la Entidad**. Serán los encargados de recibir la solicitud de datos por parte de terceros. Asimismo, deberán comunicar dicha circunstancia al responsable del servicio o departamento del que formen parte.
- **Los Responsables de Servicio/Departamento** deberán rellenar la ficha de solicitud de datos del Anexo I del procedimiento de cesión de datos personales y comunicarla al Delegado de Protección de Datos.

- **El/La Delegado de Protección de Datos** deberá asesorar, en virtud de cada caso, acerca de la estimación o desestimación de la petición de cesión de datos. Las funciones del Delegado de Protección de Datos han sido atribuidas al Comité de Seguridad de la Información, quién ha designado a la Jefatura del Servicio de Organización e Información como interlocutor para las comunicaciones con el órgano de control correspondiente y, con los interesados que ejerzan sus derechos relativos a protección de datos personales, y con las entidades locales sobre las que el Comité de Seguridad de la Información asuma las funciones del Delegado de Protección de Datos.
- **El/La Delegado de Protección de Datos** deberá asesorar y velar por que la cesión de datos se lleve a cabo respetando los principios del RGPD y LOPDgdd (seguridad, minimización, limitación a la finalidad, licitud, etc.)
- **El/La Responsable de Seguridad** asistirá al Delegado de Protección de Datos, en caso de que sea necesario, sobre la utilización de herramientas o medidas de seguridad para llevar a cabo la cesión.
- **Los Responsables de Servicio/Departamento** deberán llevar a cabo la cesión de los datos atendiendo a las indicaciones del Delegado de Protección de Datos.

10 Terceros sin tratamiento de datos personales

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

En estas circunstancias, la Diputación 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 la Diputación 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 de la Diputación.
- 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.

  Para atender adecuadamente estos supuestos, se dispondrá de un modelo de cláusula de confidencialidad para pliegos de condiciones de contratos que no impliquen acceso a datos de la Diputación.

11 Violación de la seguridad de los datos personales: notificación y comunicación

El RGPD, en los artículos 33 y 34 del Reglamento, 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, la Diputación 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 se coordinará con lo dispuesto sobre este tema en el ENS que, para su cumplimiento, La Diputación dispondrá del correspondiente Procedimiento de Notificación de Violaciones de Seguridad, donde se determinan 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 encontrará englobado en el Procedimiento de Seguridad del ENS relativo a la Gestión de Incidentes.

12 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 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 la Diputación para alcanzar un nivel de seguridad adecuado.

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

12.1 Procedimiento

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

La Diputación de Almería realizará una correspondencia entre las Actividades/Servicios y las Actividades de Tratamiento.

El Análisis de Riesgos se realizará desde 2 puntos de vista:

1. Análisis de los riesgos derivados del tratamiento de los datos con los sistemas de información que puedan vulnerar las dimensiones de Integridad, confidencialidad y disponibilidad. Riesgos que se analizaran y valoraran según los criterios del ENS.
2. Análisis de los riesgos derivados del incumplimiento normativos, estos riesgos se analizarán y valoraran según la Guía práctica de análisis de riesgos en el tratamiento de los datos personales publicada por la AEPD.

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

12.1.1 Enfoque de la evaluación de riesgos

Un riesgo se puede definir como la combinación de la posibilidad de que se materialice una amenaza y sus consecuencias negativas. El nivel de riesgo se mide según su probabilidad de materializarse y el impacto que tiene en caso de hacerlo. Las amenazas y los riesgos asociados están directamente relacionados, en consecuencia, identificar los riesgos siempre implica considerar la amenaza que los puede originar.

Evaluar un riesgo implica considerar todos los posibles escenarios en los cuales el riesgo se haría efectivo. La evaluación de riesgos consiste en valorar el impacto de la exposición a la amenaza, junto a la probabilidad de que esta se materialice. El impacto, por su parte, se determina en base a los posibles daños que se pueden producir si la amenaza se materializa, por ejemplo, un impacto sería despreciable si no tuviera consecuencias sobre el interesado o, por el contrario, un impacto sería significativo si el daño ocasionado sobre los derechos y libertades del interesado fuese crítico. Según la probabilidad y el impacto, asociados a las amenazas, es posible determinar el nivel de riesgo inherente.

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.

12.1.2 Identificación de riesgos:

- Identificar los Activos esenciales que, para la Protección de los Datos Personales, serán las Actividades de Tratamiento que se recogen en el Registro de Actividades de Tratamiento de la Diputación.
- Identificación de activos derivados de los esenciales 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 para las de carácter organizativo y técnico, y el impacto en termino de cumplimiento de los requisitos regulatorios relacionados con los derechos y libertades de los interesados las de carácter jurídico.

Los pasos anteriores se llevan a cabo mediante la herramienta PILAR para los que afectan al ENS, y con la herramienta ProDatos de Diputación los que afectan al cumplimiento normativo, para ello se contara con el apoyo de personal técnico de la Diputación. Se dispondrá de un Informe de Valoración de Activos que incluye la relación de activos que afectan tanto al ENS, como al RGPD, así como la valoración de los activos esenciales que respecto al RGPD es el Registro de Actividades de Tratamiento aprobado por la Diputación.

12.1.3 Análisis y valoración de riesgos

- Evaluación de los efectos en la actividad de la Diputación que pudiesen derivarse de la materialización de los fallos de seguridad en términos de pérdida de confidencialidad, integridad o disponibilidad, así como del incumplimiento normativo.
- 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 del impacto de los niveles de riesgo es llevara a cabo por los responsables técnicos de los tratamientos de datos personales de la Diputación y con el apoyo del personal técnico de la Diputación y se realiza con la herramienta PILAR para el ENS y con la herramienta ProDatos para cumplimiento normativo según RGPD.

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.

12.2 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, …)

La Diputación 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 un valor de 2.

12.2.1 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 MAGERIT para el ENS y los controles recomendados por la AEPD en su Guía de Evaluación de Impacto de Protección de Datos Personales para el cumplimiento normativo del RGPD y LOPDgdd.

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).

12.2.2 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.

La Diputación acepta temporalmente el riesgo actual (calculado tras el análisis de riesgos) condicionado a la existencia del plan de tratamiento de riesgos. Asimismo, la Diputación 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.

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

12.3 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 del ENS son tratadas y gestionadas a través de la herramienta PILAR. y el del Cumplimiento del RGPD y LOPDGdd se tratarán y gestionarán en la herramienta ProDatos implantada en la Diputación.

13 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:

a) 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.
b) Tratamiento a gran escala de las categorías especiales de datos personales o de los datos personales relativos a condenas e infracciones penales.
c) observación sistemática a gran escala de una zona de acceso público.
d) tratamiento con fines de investigación en salud pública y, en particular, biomédica

Por su parte, la Guía para una Evaluación de Impacto en la protección de datos personales, elaborada por la Agencia Española de Protección de Datos, establece una lista indicativa de situaciones en las que sería aconsejable llevar a cabo una evaluación de impacto:

- 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, recibiéndolos 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 de la Diputación.

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 artículo 35.4 RGPD prevé que cada autoridad de control establezca y publique una lista de los tipos de operaciones de tratamiento que requieran de una evaluación de impacto. Esta lista tiene, por tanto, la finalidad de ofrecer seguridad a los responsables respecto a cuáles son los tratamientos en que siempre se considerará que es probable que exista un alto riesgo. También de acuerdo con lo previsto por el RGPD, la lista ha sido comunicada al Comité Europeo de Protección de Datos, que ha emitido un dictamen favorable sobre ella, siguiendo los criterios establecidos en la valoración de todas las listas remitidas por las autoridades nacionales.

Por otra parte, para facilitar a los responsables de los tratamientos la identificación de aquellos tratamientos que no requieren una EIPD, el RGPD, en su artículo 35.5, dispone que las autoridades de control podrán publicar una lista con los tratamientos que no requieran de la elaboración de una EIPD. Dicha lista deberá ser comunicada al Comité Europeo de Protección de Datos (CEPD).

Se realizará un modelo 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. El modelo

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.

14 Actuaciones y Auditorias, externas e internas

El Articulo 39 del RGPD-UE establece entre las funciones del Delegado de Protección de Datos, en su punto 1.b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento y las auditorias correspondientes.

Para cumplir con esta obligación se realizarán Auditorias y Actuaciones, externas e internas para garantizar el cumplimiento de lo dispuesto en el RGPD y LODDGdd.

La Diputación Provincial de Almería dispondrá de un listado en el que se relacionen dichas actuaciones.

15 Anexos

La Diputación de Almería a través de Resolución de Presidencia aprobara todos aquellos procedimientos necesarios para el cumplimiento normativo del presente Manual y que se relacionan a continuación:

ANEXOS:

1. Registro de actividades de tratamiento. Procedimiento de actualización: Resolución de Presidencia 561/2019, de 14 de marzo
2. Política de Seguridad y Privacidad. Resolución de Presidencia 2007/2020
3. Política de Privacidad web
4. Procedimiento general de información:
    - Clausulas para formularios:
        - Con consentimiento

  - Obligación legal
  - Contrato
  - Interés público
- Clausulas para notificaciones
- Carteles informativos para el tratamiento de datos personales

5. Funciones y obligaciones
   - Designación del Delegado de Protección de Datos, funciones y obligaciones
   - Designación del Responsable de Seguridad, funciones y obligaciones
   - Funciones y obligaciones de los responsables funcionales del tratamiento de datos personales
   - Función genérica para todo el personal de la Diputación de Almería en materia de Protección de datos
   - Compromiso de confidencialidad para empleados
6. Procedimiento para el ejercicio de los derechos del ciudadano en materia de Protección de datos
7. Identificación de los interesados en las notificaciones por medio de anuncios y publicaciones de actos administrativos.
8. Guía para la evaluación de terceros:
   - Encargado
   - Cesionario
   - Corresponsable
9. Encargos de Tratamiento
   - Cláusula y Addenda para contratos con encargo de tratamiento
   - Cláusula para contratos sin tratamiento de datos personales, pero con acceso
10. Procedimiento para Cesión de datos personales
11. Procedimiento de la seguridad de los datos personales, gestión de incidentes: gestión violaciones de seguridad.
12. Manual para la realización del análisis y gestión de riesgos y medidas de seguridad a implantar.
13. Procedimiento para la realización de una evaluación de impacto.
14. Auditorias para evaluar el grado de cumplimiento del RGPDP (UE)