Implicaciones del Reglamento Europeo de Protección de Datos en las Administraciones Locales

María de la Peña Cabrera Ruiz
Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones
Anna María Chúlia Cebolla

06/2018

Esta obra está sujeta a una licencia de Reconocimiento-NoComercial-SinObraDerivada 3.0 España de Creative Commons

FICHA DEL TRABAJO FINAL

Título del trabajo:	Implicaciones en las administraciones Locales del RGPD
Nombre del autor:	María Peña Cabrera Ruiz
Nombre del consultor:	Anna María Chúlia Cebolla
Fecha de entrega (mm/aaaa):	06/2018
Área del Trabajo Final:	Aspectos Legales de la Seguridad Informática
Titulación:	*Máster Universitario en Seguridad de las Tecnologías de la Información y de las Comunicaciones*

Resumen del Trabajo (máximo 250 palabras):

En el año 2016, la Unión Europea aprobó el Reglamento General de Protección de Datos (RGPD) siendo de aplicación a partir del 25 de mayo de 2018, en todos los estados miembros.

Con la aplicación del Reglamento Europeo de Protección de Datos, las administraciones locales deben adaptarse a esta nueva normativa.

El avance de las tecnologías de la información y de las comunicaciones en la administración local, unido a la gran cantidad de información de terceras personas en su poder, hacen del derecho fundamental a la protección de datos, un derecho de enorme relevancia en la actualidad.

En este trabajo se pretende recoger los puntos más relevantes, en cuanto a novedades y obligaciones, recogidos en el Reglamento, en su aplicación en las entidades locales, con el fin de cumplir con las suficientes garantías con dicha normativa, de obligado cumplimiento pero de absoluta necesidad.

Abstract :

In 2016 the European Union approved The General Data Protection Regulation (GDPR) which will become applicable from the May 25th 2018 in all member countries.

With the application of the General Data Protection Regulation the local administrations must adapt to these new rules.

The advances in Information Technologies and in local administration communications, together with the great amount of third party information in their possession make the fundamental rigth to data protection a right of massive relevance in these days.

The intention of this paper is to unite the most relevant points regarding updates and new duties includes on the Regulation and its application by Local entities with the purspose to comply with enough guaranties with the mentioned Regulations which are of mandatory compliance but an absolute necessity.

Palabras clave:

RGPD, Protección de Datos, Administración Local, Normativa

Índice

1. Introducción 1
1.1 Contexto y justificación del Trabajo 1
1.2 Objetivos del Trabajo 3
1.3 Enfoque y método seguido 4
1.4 Planificación del Trabajo 5
2. Contexto y justificación del Reglamento Europeo de Protección de Datos 6
3. Principios de Protección de Datos 8
4. Derecho de información: el principio de transparencia 14
5 Derechos de los interesados 19
6. Legitimación para el tratamiento de datos: supuestos 25
7. Registro de Actividades del Tratamiento de los datos personales 30
8. Medidas de seguridad 34
9. Análisis de riesgos de protección de datos 38
10. Evaluaciones de impacto 48
11. Notificación de brechas de seguridad 59
12. La figura del Delegados de Protección de Datos (DPO) 62
13. Contratos de encargo de tratamiento 67
14. Transferencias internacionales de datos personales 70
15. Régimen sancionador en las Administraciones Locales 74
16. Conclusiones 76
17. Definiciones 78
18. Anexos 81
19. Bibliografía 86

1. Introducción

1.1 Contexto y justificación del Trabajo

Uno de los derechos más relevantes en las sociedades actuales y de plena actualidad es el derecho fundamental a la protección de datos, dado que el uso de las tecnologías de la información y de las comunicaciones condiciona de manera importante el ejercicio de los derechos fundamentales y muy especialmente el referido a la Protección de Datos.

El avance de las tecnologías de la información y de las comunicaciones en la administración supeditada, inicialmente a la Ley 11/2007 de acceso electrónico y actualmente a la ley 39/2015 del Procedimiento Administrativo Común de las Administraciones Públicas, unido a la gran cantidad de información de terceras personas en su poder, hacen del derecho fundamental a la protección de datos, un derecho de enorme relevancia en la actualidad.

Las Administraciones públicas españolas establecen varias obligaciones en torno a la Administración electrónica que propician una mayor eficacia, innovación y modernización.

El nuevo 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 éstos, por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos), que es aplicable desde mayo de 2018, supone un fuerte impulso por armonizar la distinta legislación y garantizar el máximo nivel de protección**.**

En todo caso, las disposiciones contenidas en el Reglamento son directamente aplicables en cada uno de los Estados Miembros, sin necesidad de trasposición y obliga a las empresas privadas e instituciones públicas a afrontar un importante proceso de readaptación normativa.

Es por tanto, que las Administraciones locales deberán realizar modificaciones para poder llevar a buen puerto el uso de los tratamientos de datos teniendo en cuenta la nueva normativa, de exigente cumplimiento pero de absoluta necesidad.

1.2 Objetivos del Trabajo

En este trabajo se pretende realizar una serie de recomendaciones que detalle cómo debemos actuar los profesionales que trabajamos en las instituciones locales en materia de protección de datos y podamos conocer el nuevo marco legislativo para adaptarnos y adecuarnos a ella, teniendo en cuenta el Reglamento Europeo de Protección de Datos y su aplicación.

Se pretende recoger los puntos más relevantes del mismo en su aplicación en las administraciones locales con el fin de prestar un mejor servicio al ciudadano e interpretar de forma práctica y homogénea las obligaciones derivadas del mismo.

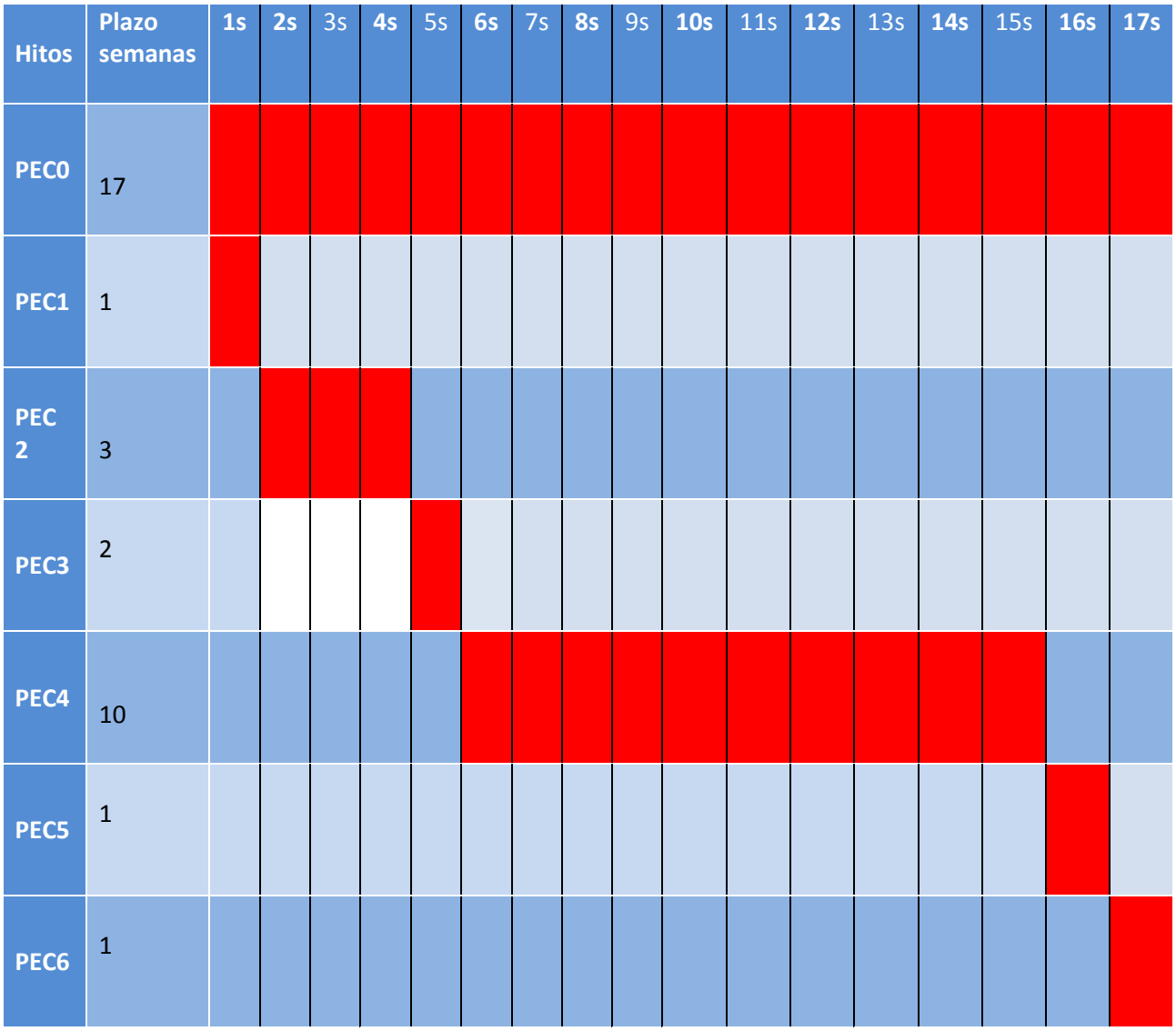
El objetivo de este trabajo por tanto, es la creación de una serie de pautas para ayudar a la comprender un documento tan complejo como es el Reglamento Europeo de Protección de datos, a facilitar a las Administraciones Locales a interpretar de forma práctica y homogénea las obligaciones derivadas del nuevo Reglamento Europeo de Protección de Datos, donde se pueden encontrar las claves necesarias para el cumplimiento normativo.

Este documento permitirá que cada Administración local sea capaz de elaborar su propia hoja de ruta hacia la consecución del objetivo de cumplir con suficientes garantías el Reglamento Europeo de Protección de Datos.

1.3 Enfoque y método seguido

El método y la estrategia se han centrado en la búsqueda de bibliografía y legislación en relación a la protección de datos y las administraciones públicas. El enfoque de este proyecto es principalmente teórico y se finaliza con la elaboración de una hoja de ruta con los puntos mas destacados a tener en cuenta para la adecuación y medidas a adoptar, por parte de las administraciones locales al Reglamento Europeo de Protección de Datos. En esta guía sobre el itinerario para la adecuación al Reglamento europeo de Protección de Datos, se habrá conseguido el objetivo principal si con la elaboración del mismo, ayudamos a saber cómo hemos de trabajar en la adecuación y medidas a adoptar dentro de nuestra organización, para asegurar la información y los datos dentro de las infraestructuras necesarias y que no se quede en una mera declaración de intenciones.

1.4 Planificación del Trabajo



Inicio **28/02/2018**

PEC0 Búsqueda de información, documentación

PEC1 Propuesta, Índice Provisional, Calendario de trabajo

PEC2 Capítulos: 1. Contexto y Justificación; 2 Objetivos; Enfoque y Método; 4 Planificación

PEC3 Bibliografía terminada y correctamente citada

PEC4 Resto de capítulos

PEC5 Memoria finalizada

PEC6 Video presentación

Final **08/06/2018**

2. Contexto y justificación del Reglamento Europeo de Protección de Datos

La rápida evolución tecnológica y la globalización han planteado nuevos retos para la protección de los datos personales. La magnitud de la recogida y del intercambio de datos personales está aumentando de manera significativa.

La masiva utilización de la tecnología está permitiendo que se utilicen datos personales en una escala sin precedentes.

La economía, la forma de relacionarnos se ha transformado gracias a uso de la tecnología, redes sociales, internet, la banca etc., cada día se difunden un volumen cada vez mayor de información personal a escala mundial y todo esto ha modificado nuestros hábitos de vida.

La tecnología ha transformado, por tanto, tanto la economía como la vida social, y se ha de facilitar aún más la libre circulación de datos personales dentro de la Unión y la transferencia a terceros países y organizaciones internacionales, garantizando al mismo tiempo un elevado nivel de protección de los datos personales.

Estos avances tecnológicos, así como la globalización, han planteado nuevos retos para la protección de los datos personales por lo que es necesario un nuevo marco normativo más sólido y coherente para el momento en el que nos encontramos por lo que se han planteado nuevos retos en cuanto a la protección de datos que permita generar la confianza que en el control de los datos personales.

Por lo que hay que reforzar la seguridad jurídica y práctica para las personas físicas, los operadores económicos y las autoridades públicas, que supone un mayor compromiso de las organizaciones, públicas o privadas, con la protección de datos. Para ello, el nivel de protección de los derechos y libertades de las personas físicas por lo que se refiere al tratamiento de dichos datos debe ser equivalente en todos los Estados miembro.

Por lo que el objetivo principal que se pretende **unificar la normativa de protección de datos de la Unión Europea** para garantizar un nivel equivalente de protección de las personas físicas en la UE y la libre circulación de datos personales en la Unión Europea.

Este nuevo reglamento aprobado y en vigor desde el 24 de mayo de 2016 será de aplicación directa en todos los estados miembro, el 25 de mayo de 2018, y con su aplicación, se pretende fundamentalmente, devolver a los ciudadanos el control de sus datos personales y garantizar unos elevados estándares de protección, confianza y seguridad jurídica uniformes en toda la UE.

En este contexto, se explica el nuevo reglamento de Protección de Datos, en adelante RGPD.

3. Principios de Protección de Datos

Los principios del tratamiento constituyen el fundamento del sistema europeo de protección de datos.

En el artículo 5 del RGPD, quedan señalados los principios relativos al tratamiento siendo esto:

Principio de licitud, transparencia y lealtad

Un primer principio es el de "licitud, transparencia y lealtad", que consiste en que los datos deben ser tratados de manera lícita, leal y transparente para el interesado.

Por lo que los datos personales deben ser tratados de manera licita. La licitud en el tratamiento se relaciona con la necesidad de que el responsable del tratamiento se base en alguna de las bases jurídicas que establece el Reglamento para el tratamiento de los datos personales.

El principio reconoce que el derecho a la protección de datos implica que los datos solo pueden ser tratados conforme a lo estipulado en el artículo 6 del presente Reglamento que señala lo siguiente:

<<…a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos; 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 al responsable del tratamiento; 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 al responsable del tratamiento; f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades

fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño…>>

Al mismo tiempo, el principio incluye el que los datos sean tratados de forma leal para con el interesado o que se le proporcione la información necesaria para que entienda el objeto y fines del tratamiento, y pueda, en su caso, decidir sobre él.

Este aspecto del principio de "licitud, lealtad y transparencia" viene condicionado por las disposiciones del RGPD que determinan qué información debe proporcionarse al interesado, en qué forma y en qué momento, así como en las que regulan los procedimientos de respuesta a las solicitudes de ejercicio de derechos.

Principio de limitación de la finalidad.

El segundo de los principios que se enumera en el RGPD es el de "limitación de la finalidad".

Por tanto, obliga a que los datos sean tratados con una o varias finalidades determinadas, explícitas y legítimas. La finalidad del tratamiento ha de estar claramente definida.

Además prohíbe que los datos recogidos con unos fines determinados, explícitos y legítimos sean tratados posteriormente de una manera incompatible con esos fines. Por lo que no es posible es tratar los datos recogidos para una finalidad con fines que no sean compatibles con ella.

Por lo que, tal y como señala el considerando 59 del RGPD, el tratamiento de datos personales con fines distintos de aquellos para los que hayan sido recogidos inicialmente solo debe permitirse cuando sea compatible con los fines de su recogida inicial.

Se considera compatible si el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos

conferidos al responsable del tratamiento, siempre y cuando estén determinados por el Derecho de la Unión o de los Estados miembros.

El responsable del tratamiento, tras haber cumplido todos los requisitos para la licitud del tratamiento inicial, y para determinar si el fin del tratamiento ulterior es compatible con el fin de la recogida inicial de los datos personales, debe tener en cuenta:

- cualquier relación entre estos fines y los fines del tratamiento ulterior previsto,
- el contexto en el que se recogieron los datos, en particular las expectativas razonables del interesado basadas en su relación con el responsable en cuanto a su uso posterior,
- la naturaleza de los datos personales,
- las consecuencias para los interesados del tratamiento ulterior previsto
- la existencia de garantías adecuadas tanto en la operación de tratamiento original como en la operación de tratamiento ulterior prevista.

Principio de minimización de datos

El principio de minimización de datos nos dice que sólo serán tratados los datos adecuados, pertinentes y no excesivos en relación con los fines para los que son tratados. Por lo que, si los fines del tratamiento pueden cumplirse tratando datos anónimos. Si no es posible, verificar si pueden excluirse determinados datos.

Principio de exactitud

Los datos, según el “principio de exactitud”, deben ser exactos y, si fuera preciso, actualizados, debiendo adoptarse todas las medidas razonables para que se rectifiquen o supriman los datos inexactos en relación a los fines que se persiguen.

Este principio también actúa durante la recogida de datos por parte del encargado o responsable del tratamiento, por lo que se deben establecer

mecanismos que la información recogida no contiene errores y si los tiene se corrijan.

Principio de limitación del plazo de conservación artículo 5.1.e del RGPD

El principio de “limitación del plazo de conservación” puede describirse como limitación temporal en el tratamiento de datos, ya que la conservación de esos datos debe limitarse en el tiempo del fin del mismo. Una vez que ese fin ha finalizado, los datos deben ser borrados.

No obstante, hay casos en que es posible mantener los datos por más tiempo del necesario para la consecución de la finalidad inicial. El RGPD menciona excepciones que se encuentran recogidas en el artículo 17.3 del Reglamento como pueda ser tratamiento con fines archivísticos en interés público, investigación científica e histórica y fines estadísticos. Además es posible que los datos sean conservados para el cumplimiento de una obligación legal del responsable, o para que el responsable pueda ejercer acciones legales.

Principio de integridad y confidencialidad, artículo 5.1.f del RGPD

El último principio es el de integridad y confidencialidad. Básicamente, obliga a quienes tratan datos la obligación de actuar proactivamente con el objetivo de proteger los datos que manejan frente a cualquier riesgo que amenace su seguridad y 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 apropiadas.

Por lo que, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

Responsabilidad Proactiva

Además en el mismo artículo punto 2 nos señala que el responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo, este concepto novedoso es la Responsabilidad proactiva.

Fuera del listado de principios que se recogen en el artículo 5 del RGPD se encuentra un principio denominado de "responsabilidad proactiva", expresión que pretende traducir el término inglés "accountability".

Este principio se describe no en el propio artículo 5, sino en el artículo 24, según el cual *"teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento*".

Por lo que, la responsabilidad por la forma en que se traten los datos es responsabilidad del responsable del tratamiento de datos, ya que es el que decide que se inicie un tratamiento, su finalidad, los datos que van a ser tratados y cuáles son las actividades de tratamiento que se van a realizar y por tanto se deberá ocupar de que se lleve a cabo el tratamiento adecuado y encargarse de las responsabilidades en caso de que ello no suceda.

Para la implementación del principio de responsabilidad proactiva tenemos que tener en cuenta dos principios señalados en el considerando 78 del RGPD: el principio de protección de datos desde el diseño y protección de datos por defecto

El principio de protección de datos desde el diseño obliga a los responsables del tratamiento a tener en cuenta desde el inicio, al desarrollar, diseñar, seleccionar y usar aplicaciones, servicios y productos que están basados en el tratamiento de datos personales o que tratan datos personales, a que se tenga en cuenta el derecho a la protección de datos.

El principio de protección de datos por defecto obliga al responsable del tratamiento a adoptar políticas internas y aplicar medidas de seguridad como puedan ser, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad.

Además, El RGPD no se limita a situar la responsabilidad sobre un responsable pasivo, ya que se debe adoptar un enfoque proactivo, exigiendo que el responsable adopte medidas preventivas dirigidas a reducir los riesgos de incumplimiento y, además, que esté en condiciones de demostrar que ha implantado esas medidas de seguridad adecuadas y que las mismas son las adecuadas para lograr la finalidad perseguida.

4. Derecho de información: el principio de transparencia

Los responsables y encargados de tratamiento en las Administraciones Locales deberán facilitar a los interesados toda la información que precisen en relación con el tratamiento de sus datos personales.

Dicha información y tal como señala el RGPD debe ser concisa, fácilmente accesible y fácil de entender por parte del interesado, además de que se debe utilizar un lenguaje claro y sencillo.

El Considerando 58 del RGPD indica:

*«El principio de transparencia exige que toda información dirigida al público o al interesado sea **concisa, fácilmente accesible y fácil de entender**, y que se utilice un **lenguaje claro y sencillo**, y, además, en su caso, **se visualice**. Esta información podría facilitarse en forma electrónica, por ejemplo, cuando esté dirigida al público, mediante un sitio web. (…)».*

Es decir, para que cumplir adecuadamente con el deber de información se deben cumplir los siguientes requisitos:

- Lenguaje claro y sencillo.
- Información concisa, fácilmente accesible y fácil de entender.

En cuanto al derecho de información y teniendo en cuenta lo señalado en el artículo 12.1 del RGPD:

<<.. El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información indicada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida

<u>específicamente a un niño.</u> La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos…>>

Con la aplicación del RGPD, se incrementa la información que habrá de facilitarse al interesado cuando los datos se recaben de este, que la que anteriormente con la LOPD había que suministrar al interesado.

Teniendo en cuenta lo definido en sus artículos 13 y 14, el RGPD nos indica la información que deberá facilitarse a los interesados, distinguiendo dos supuestos:

- Cuando los datos personales se obtienen del interesado.
- Cuando los datos no se han obtenido del propio interesado.

Es decir, el RGPD obliga al Responsable del Tratamiento a proporcionar una mayor información a los interesados, o cuando se soliciten los datos o bien *«dentro de un plazo razonable»* (cuando los datos no se obtienen del propio interesado).

Asimismo, debemos destacar que el propio RGPD en su artículo 14.3 indica **que debemos entender por un plazo razonable**:

- Dentro del mes siguiente a la obtención de los datos.
- En el momento de la primera comunicación con el interesado.

Además hay que tener en cuenta que no siempre hay que informar al interesado ya que no será necesario informar cuando los datos personales se hayan obtenido del interesado en aquellos supuestos en los que el interesado ya disponga de la información. Y en los supuestos en que los datos no procedan del interesado no resulta preciso informar cuando se de alguno de los siguientes supuestos:

- El interesado ya disponga de la información.

- La comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado.
- La obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o por el Derecho nacional.
- Cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional.

Teniendo en cuenta el modelo establecido por la Agencia Española de Protección de Datos, en su «Guía para el cumplimiento del deber de informar» , cuya función es orientar acerca de las mejores prácticas para dar cumplimiento a la obligación de informar a los interesados, en virtud del principio de transparencia, los procedimientos, modelos o formularios diseñados de conformidad con la LOPD deberán ser revisados y adaptados por los Responsables de Tratamientos con anterioridad a la fecha de plena aplicación del RGPD y se recomienda adoptar un **modelo de información por capas o por niveles**.

Los procedimientos, modelos o formularios de recogida de información pueden ser muy variados, las formas más habituales de recogida de datos pueden ser:

- Formularios en papel,
- Entrevista telefónica
- Navegación o formularios Web,
- Registro de aplicaciones móviles
- Datos de actividad personal

Por otra parte, las comunicaciones al interesado sobre datos ya disponibles, o tratamientos adicionales, pueden hacerse llegar, entre otros, por medio de:

- Correo postal
- Mensajería electrónica
- Notificaciones electrónicas

El modelo de información por capas consiste en lo siguiente:

Primera Capa: Presentación de la información básica de forma resumida. Esta información básica se puede presentar en forma de tabla de forma que se garantice que esta información quede dentro del «campo de visión» del interesado y la misma debe quedar claramente identificada con un título como *«información básica sobre protección de datos»*.

Responsable	*Se debe incluir el nombre del Responsable del tratamiento de datos.*
Finalidad	*Se debe informar de la finalidad del tratamiento de los datos; en el supuesto de que dicho tratamiento tenga varias finalidades se deberá informar de la principal.*
Legitimación	*Debe hacer referencia a la base jurídica que ofrece licitud al tratamiento de datos, de entre las indicadas en el artículo 6 del RGPD. En el supuesto de administraciones locales lo más habitual será que la base jurídica sea:* *el cumplimiento de una misión realizada en interés público* *el consentimiento del interesado* *en el ejercicio de poderes públicos.*
Destinatarios	*Debe incluir la referencia a los terceros a los que esté previsto comunicar los datos. Asimismo, en el supuesto de que no se prevea comunicar los datos se deberá hacer constar expresamente con una mención como la siguiente «No se cederán los datos a terceros, salvo obligación legal».*
Derechos	*Se puede hacer una breve alusión a los derechos así como una referencia a la información adicional, donde se encontrará el resto de información.*
Información adicional	*Aquí se deberá indicar donde se puede acceder a la información adicional de la segunda capa.*

Segunda Capa: En esta capa se deben completar todos los detalles de la información resumida así como añadir toda la información adicional exigible conforme al RGPD. Debe tenerse en cuenta en esta capa que se debe incluir toda la información.

Para cumplir con estos aspectos, la AEPD establece las siguientes recomendaciones:

- Exposición bien estructurada, en base a «preguntas y respuestas».
- Debe buscar un equilibrio entre concisión y precisión, evitando explicaciones innecesarias o detalles confusos.

- Se debe evitar el abuso de las citas legales, los términos ambiguos o con escaso sentido para los destinatarios.

Por lo que se tiene que presentar una información básica en un primer nivel o primera capa, de forma resumida, en el mismo momento y en el mismo medio en que se recojan los datos y remitir a la información adicional en un segundo nivel o segunda capa, donde se presentarán con más detalle el resto de las informaciones, en el medio más adecuado para su presentación y comprensión.

En el anexo B se ofrece un ejemplo de cómo podría ser un modelo de información por capas o niveles.

5. Derechos de los interesados

Otra de las novedades que presenta el RPGD es cuanto a los derechos de los ciudadanos, ya que además de los derechos descritos en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de carácter personal, que recoge una serie de derechos fundamentales de los ciudadanos, derechos conocidos como derechos ARCO (A-acceso, R-rectificación, C-cancelación y O-oposición), aparecen un nuevo catalogo de derechos para dar más protección a los interesados en materia de protección de datos, y además se modifica el procedimiento para ejercitar los mismos.

Derecho de Acceso

El derecho de acceso viene regulado en al artículo 15 del RGPD y se recoge en los considerandos 63 y 64, como un derecho del interesado a obtener, del responsable del tratamiento, en este caso, la administración local, si se están tratando o no sus datos personales.

Por tanto, el interesado conocerá si sus datos de carácter personal están siendo tratados por la Administración Local responsable del tratamiento, así como los fines, el origen, el destinatario, el plazo o si se han comunicado o se van a comunicar a un tercero.

Si se ejercita este derecho por parte del interesado/afectado, se debe responder a tal derecho, por medio de una copia de los datos personales objeto de tratamiento del mismo y de forma gratuita

Por lo que, según la información contenida en el artículo 15 del RGPD, el interesado puede acceder a los mismos y a la siguiente información:

- Finalidad del tratamiento
- Categoría de los datos personales que se tratan
- Destinatarios o categorías de destinatarios a los que se les comunicará estos datos
- Plazo previsto de conservación o, si no es posible, los criterios para su determinación

- Derecho a solicitar del responsable del tratamiento la rectificación o supresión de datos personales o la restricción del tratamiento de los datos personales relativos al interesado o a oponerse al tratamiento de dichos datos.
- Existencia del derecho a presentar una reclamación ante la autoridad de control.
- Cuando los datos personales no se hayan obtenido del interesado, se le facilitará cualquier información disponible sobre su origen.
- En el caso de las decisiones basadas en un tratamiento automatizado que comprenda la elaboración de perfiles, información sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento la importancia y las consecuencias previstas de dicho tratamiento.
- Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías apropiadas.

Derecho de Rectificación

El derecho de rectificación, viene regulado en el Artículo 16 del RGPD, y es el derecho que tiene el interesado a solicitar del responsable del tratamiento la rectificación o modificación de sus datos cuando sean inexactos.

Asimismo, si se ejercita este derecho por parte del interesado/afectado, se prevé que el solicitante acompañe, cuando sea preciso, la documentación justificativa de la inexactitud o carácter incompleto de los datos objeto de tratamiento y la administración local, responsable del tratamiento, debe responder a tal derecho, de forma gratuita.

Derecho de Supresión o Derecho al Olvido

El derecho a la supresión o derecho al olvido, regulado en el artículo 17 del RGPD, también conocido como derecho de cancelación es el derecho que tiene el interesado a obtener la supresión de los datos personales que le

conciernen cuando concurra alguna de las circunstancias previstas en el artículo 17 del RGPD, entre las que se encuentran:

- Cuando los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo.
- Cuando el interesado retire el consentimiento en que se basa el tratamiento y este no se base en otro fundamento jurídico.
- Cuando el interesado se oponga al tratamiento y no prevalezcan otros motivos legítimos para el tratamiento.
- Cuando los datos personales hayan sido tratados ilícitamente.
- Cuando los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.
- Cuando los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información dirigidos a menores.

Por lo que las Entidades Locales han de facilitar a los ciudadanos la posibilidad de solicitar, la supresión de sus datos personales cuando, éstos ya no sean necesarios para la finalidad con la que fueron recogidos, cuando se haya retirado el consentimiento o cuando estos se hayan recogido de forma ilícita.

Ahora bien, existen excepciones para el ejercicio de este derecho**:**

- Cuando sea necesario para ejercer el derecho a la libertad de expresión e información;
- Para el cumplimiento de una obligación legal o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable
- Con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos,
- Para la formulación, el ejercicio o la defensa de reclamaciones.

Derecho a la limitación del tratamiento

El derecho a la limitación del tratamiento de los datos personales es otro de los nuevos derechos que recoge el RGPD en su artículo 18, y supone la

limitación del tratamiento de los datos en determinadas circunstancias por parte el responsable del tratamiento para los fines del tratamiento.

Los supuestos en los que el interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos son:

- Cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar los mismos.
- Cuando el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso.
- Cuando el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones.
- Cuando el interesado se haya opuesto al tratamiento ejercitando su derecho de oposición, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.

Derecho de Portabilidad

Como se señala el artículo 20.1 del RGPD

> << *El interesado tendrá derecho a recibir los datos personales que le incumban, 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 al que se los hubiera facilitado*.>>

Por tanto, el derecho a la portabilidad de los datos implica que el interesado que haya proporcionado sus datos a un responsable que los esté tratando de modo automatizado podrá solicitar recuperar esos datos en un formato que le permita su traslado a otro responsable. Cuando ello sea técnicamente posible, el responsable deberá trasferir los datos directamente al nuevo responsable designado por el interesado. Como requisitos de aplicación de este derecho se destacan los siguientes: deben ser tratamientos automatizados (no papel), y la legitimación del tratamiento se basará únicamente en la ejecución de un contrato o en el consentimiento.

Derecho de oposición

Se trata del derecho del interesado a oponerse al tratamiento de sus datos, a que datos personales que le conciernan sean objeto de un tratamiento, incluyendo la elaboración de perfiles, que se basen en la necesidad de la ejecución de contratos en los que el interesado es parte o que resulte necesario para la satisfacción de intereses legítimos perseguidos.

Este derecho está regulado en el artículo 21 del RGPD y en los Considerandos (69) y (70).

Ante dicho ejercicio del derecho de oposición el responsable del tratamiento dejará de tratar los datos personales.

Las Administraciones Locales deberán por tanto, facilitar a los interesados el ejercicio de sus derechos, por medio de la presentación de solicitud por medios electrónicos, si se realiza el tratamiento por este medio o bien en papel, si así lo deseara.

Cabe destacar que el artículo 23 del RGPD establece una serie de limitaciones de cumplimiento de estos derechos que tiene el interesado en cuanto al tratamiento de sus datos personales. Estos supuestos son los siguientes:

- la seguridad del Estado, la defensa y la seguridad pública
- la prevención, investigación, detección o enjuiciamiento de infracciones penales o la ejecución de sanciones penales, incluida la protección frente a amenazas a la seguridad pública y su prevención
- otros objetivos importantes de interés público general de la Unión o de un Estado miembro, en particular un interés económico o financiero importante de la Unión o de un Estado miembro, inclusive en los ámbitos fiscal, presupuestario y monetario, la sanidad pública y la seguridad social
- una función de supervisión, inspección o reglamentación vinculada, incluso ocasionalmente, con el ejercicio de la autoridad pública en los casos contemplados en la protección del interesado o de los derechos y libertades de otros
- la ejecución de demandas civiles.

Una vez ejercitado por el interesado alguno de estos derechos, y teniendo en cuenta el considerando 59 y el articulo 12.3 y 12.4 del presente Reglamento, la Administración Local, en su caso, el delegado de Protección de datos debe facilitar al interesado información sobre su solicitud en el plazo de un mes, aunque es prorrogable a dos meses si se tiene en cuenta el número de solicitudes y la complejidad de las mismas, por lo que habrá que informar al interesado de esa prórroga indicando los motivos.

Asimismo, en el supuesto de que la administración decida no atender dicha solicitud, a más tardar, transcurrido 1 mes, informará de las razones de su no actuación y que puede presentar una reclamación ante la autoridad de control.

Toda actuación en el ejercicio de los derechos del interesado tendrá carácter gratuito, excepto aquellos casos en los que la solicitud sea infundada o excesiva.

En estos casos, el responsable del tratamiento podrá:

- Cobrar un canon razonable en función de los costes administrativos afrontados para facilitar la información o la comunicación o realizar la actuación solicitada.
- Negarse a actuar respecto de la solicitud.

6. Legitimación para el tratamiento de datos: supuestos

En el artículo 6 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal nos señala, como norma general, para la legitimización el tratamiento de datos se utilizara el consentimiento inequívoco del afectado y cuenta con varias excepciones entre ellas, el utilizado en las administraciones locales que no será necesario el consentimiento para el ejercicio de sus funciones o en el ámbito de sus competencias, además y como señala el artículo 11 de la citada ley en la comunicación de datos, el consentimiento no será preciso cuando la cesión está autorizada en una ley.

Con la aplicación del RGPD esta legitimación en el tratamiento de datos cambia notablemente en las AAPP, como queda señalado en el artículo 6 del RGPD donde se observan los siguientes supuestos para la legitimación del tratamiento de datos:

<<a. *el interesado dio su* ***consentimiento*** *para el tratamiento de sus datos personales para uno o varios fines específicos;*
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 al responsable del tratamiento;*
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 al responsable del tratamiento;*
f. *el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.*

*Lo dispuesto en la letra **f)** no será de aplicación al tratamiento realizado por las autoridades públicas en el ejercicio de sus funciones…>>*

Por lo que, en el RGPD, se parte de que no será la legitimación de datos el consentimiento y una serie de excepciones sino más bien habrá diferentes supuestos que serán los que legitimen el tratamiento de datos.
Además, teniendo en cuenta el Considerando 40 del RGPD:

<<..Para que el tratamiento sea lícito, los datos personales deben ser tratados con el consentimiento del interesado o sobre alguna otra base legítima establecida conforme a Derecho…>>

Consentimiento
En el RGPD está definido de la siguiente forma:
<<Toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen;>>

Y además, teniendo en cuenta lo contemplado en el Considerando 32 del RGPD:
<<.. *El consentimiento debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal. …>> <<… Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos. Si el consentimiento del interesado se ha de dar a raíz de una solicitud por medios electrónicos, la solicitud ha de ser clara, concisa y no perturbar innecesariamente el uso del servicio para el que se presta…>*

Por lo que, aunque no será prácticamente utilizado en las Administraciones locales, ya que los tratamientos de datos en estas entidades estará sustentado en una normativa legal, se utilizara en algunos supuestos como por ejemplo, en la suscripción a la revista municipal, en la suscripción a noticias push de una

app municipal, con la nueva definición de consentimiento dada por el RGPD las Administraciones Locales se deben revisar la solicitudes de consentimiento para cumplan con los requisitos del Reglamento. Habrá que tener en cuenta lo siguiente:

• Acto afirmativo claro. No es válido el consentimiento tácito ni los checks premarcados.
• No debe existir desequilibrio. No se puede considerar que el consentimiento se haya dado libremente en aquellos supuestos en los que existe un desequilibrio claro entre el interesado y el responsable del tratamiento.
• No general. En el supuesto de que el tratamiento de los datos tenga varias finalidades se debe otorgar el consentimiento para cada una de las finalidades de forma independiente; es decir, no son válidos los consentimientos generales.
• Documentado. Se deben mantener registros adecuados para ser capaz de demostrar el consentimiento para el tratamiento de los datos personales.

La Administración puede seguir utilizando consentimiento preexistente siempre y cuando la forma en que se dio el consentimiento se ajuste a las condiciones del RGPD. En este sentido, el considerando 171 del RGPD nos indica lo siguiente:

<<…La Directiva 95/46/CE debe ser derogada por el presente Reglamento. Todo tratamiento ya iniciado en la fecha de aplicación del presente Reglamento debe ajustarse al presente Reglamento en el plazo de dos años a partir de la fecha de su entrada en vigor. Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento, a fin de que el responsable pueda continuar dicho tratamiento tras la fecha de aplicación del presente Reglamento…>>

Consentimiento de menores

En el caso del consentimiento de los menores de edad en el RGPD se considera que sólo se considerará lícito si el menor fuera mayor de 13 años o si, siendo menor de esa edad, el consentimiento es prestado por los titulares de la patria potestad o la tutela. (Artículo 8 del RGPD)

En el caso del consentimiento prestado por menores el responsable está obligado a realizar esfuerzos razonables para verificar que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño.

El artículo 7.1 indica que cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales. Por lo que es recomendable que en las Administraciones locales se tenga un registro de cómo y cuándo se ha otorgado el consentimiento, donde se recojan, en los supuestos que sea necesario, como mínimo, los siguientes datos:

- Identificación del interesado: El nombre del interesado y su identificador (NIF).
- Fecha y hora: Almacenar una copia del documento de otorgamiento del consentimiento fechado.
- Contenido: Copia de los documentos o de la captura de datos en los que se incluye la declaración de consentimiento junto con cualquier política de privacidad independiente.
- Forma de consentimiento: Copia del formulario de consentimiento o captura de los datos.
- Retirada del consentimiento. En el supuesto de que el interesado haya retirado su consentimiento constancia de este hecho y del momento.

El consentimiento no es la única base legal que habilita al tratamiento de datos personales, además, en las administraciones locales, ya que ésta no será la habitual, ya que en el artículo 6 del RGPD señala los siguientes supuestos indicados inicialmente que legitiman los tratamientos de datos personales.

Normalmente se tendrá en cuenta una base legal que habilite el tratamiento de datos, siendo las más habituales **el de interés público o el ejercicio de poderes públicos o el cumplimiento de una obligación legal**, se tiene que tener en cuenta que dicha normativa reguladora en las Administraciones Locales ya que estas desarrollan los supuestos establecidos en la ley, por ejemplo, Ley de bases de Régimen Local, Ley de subvenciones, Ordenanzas fiscales, ordenanzas reguladoras, etc.

Por lo tanto, los responsables del tratamiento de datos deben documentar e identificar la base legal sobre la que se desarrollan sus tratamientos, pudiendo ser por consentimiento, por relación contractual, por obligación legal del responsable, por ser necesario para proteger intereses vitales del interesado, por ser necesaria para el cumplimiento de una misión realizada en interés público o en ejercicios de poderes públicos o por ser necesario para la satisfacción de intereses legítimos perseguidos por el responsable o por un tercero.

Asimismo, debemos tener en cuenta que en los supuestos en los que se acuda a una base legal y donde se va a fundamentar el tratamiento de los datos en las Administraciones Locales es obligatorio suministrar información sobre las circunstancias del tratamiento de forma concisa, transparente y de fácil acceso, además de con un lenguaje claro y sencillo, teniendo en cuenta lo previsto en el RGPD sobre el Principio de Transparencia.

7. Registro de Actividades del Tratamiento de los datos personales

Una de las obligaciones de los responsables de los ficheros, en las administraciones Públicas era la inscripción a la Agencia Española de Protección de Datos de los ficheros que empleaban en su actividad y que contuvieran datos de carácter personal, informando, como señala al artículo 26 de la LOPD, sobre el responsable del fichero, los fines del tratamiento, una descripción de las categorías de interesados y de las categorías de datos personales, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar además, si tuviesen lugar, las transferencias de datos que se prevean a países fuera del Espacio Económico Europeo.

Con la aplicación del RGPD, esta obligación desaparece, por lo que ya no será necesario realizar la inscripción de los ficheros en el Registro General de Protección de datos de la AEPD, y se establece la obligación de tener, por parte de los responsables y encargados del tratamiento de datos, de un Registro de actividades de tratamiento.

Teniendo en cuenta el Considerando 82 del RGPD, que señala que el responsable o el encargado del tratamiento debe mantener registros de las actividades de tratamiento bajo su responsabilidad, esto, nos indica, en relación con el registro, que se trata de un instrumento para el cumplimiento con el RGPD, debiendo reflejar cualquier actividad de los tratamientos de los datos y cooperando con la Autoridad de Control, poniéndolos a su disposición si fuese requerido al efecto.

Teniendo en cuenta el artículo 30.1 del RGPD

<<…*Cada responsable y, en su caso, su representante llevará un registro de las actividades de tratamiento efectuadas bajo su responsabilidad*".

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
Las finalidades del tratamiento
Descripción de las categorías de interesados y de las categorías de datos personales
Descripción de las de las categorías de los interesados y de los datos personales.
Las categorías de los destinatarios.
Las transferencias de datos a un tercer país u organización internacional.
Los plazos para la supresión de las categorías de datos.
Una descripción general de las medidas de seguridad utilizadas por el responsable.

Adicionalmente indica que <<…*cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable*…>>

Los Responsables y encargados de los ficheros tendrán que inventariar todos los tratamientos que se estén llevando en la Administración Local, y que el cual deberá contener como señala el artículo 30 del RGPD:

Asimismo, los **encargados** deberán llevar un registro de todas las categorías de actividades de tratamiento que contenga:

El nombre y los datos de contacto de encargado, responsable y del delegado de protección de datos.
Las categorías de tratamientos efectuados por cada responsable.
Las transferencias de datos personales a un tercer país u organización internacional.
Una descripción general de las medidas técnicas y organizativas de seguridad, en caso que sea posible.

Dichos registros constarán por escrito, inclusive en formato electrónico, además el responsable o el encargado del tratamiento pondrán el registro a disposición de la autoridad de control que lo solicite.

En la "Guía del Reglamento General de Protección de Datos para responsables de tratamiento" publicada, por la Agencia española de Protección de datos en su web http://wwww.agpd.es nos guía para organizar el registro de actividades de tratamiento de datos teniendo en cuenta lo siguiente:

- Partir de los ficheros que actualmente tienen notificados los responsables en el Registro General de Protección de Datos.

- En torno a operaciones de tratamiento concretas vinculadas a una finalidad básica común de todas ellas.

- Con arreglo a otros criterios distintos.

La obligación de mantener el registro exigirá a las administraciones locales a llevar a cabo un proceso de revisión de los tratamientos y de los datos por lo que será necesario inventariar todos los tratamientos que esté realizando la entidad pública.

A efectos de facilitar a los responsables la constitución de estos registros, la AEPD permitirá que con antelación suficiente a la fecha de aplicación del RGPD, los responsables puedan obtener de forma automatizada toda la

información acerca de sus propios ficheros o tratamientos notificados al Registro General.

Para identificar y describir los tratamientos de datos que se llevan a cabo en la administración local para poder realizar el Registro de actividades de tratamiento tendremos que:

Identificar al responsable del tratamiento, en su caso al corresponsable y al delegado de protección de datos.
Identificar a los encargados
Identificar las categorías de datos personales tratados,
Identificar los datos que conllevan un mayor riesgo por ser datos sensibles,
Identificar las finalidades del tratamiento
Aunque no se exige por el artículo 30 del Reglamento, se incluirá la base jurídica del tratamiento.
Especificar los destinatarios de las posibles cesiones de datos, si las hubiera
Determinar si se producen transferencias internacionales de datos
Tiempo de conservación
Medidas de seguridad existentes o se vayan a implementar para garantizar un nivel de seguridad adecuado al riesgo que presente el tratamiento de los datos

En el anexo A podemos ver como podría ser un registro de actividades con dos tratamientos de datos.

8. Medidas de seguridad

En la LOPD, en su artículo 80 nos señalaba que las medidas de seguridad que se exigían a los a los ficheros y tratamientos de datos personales se clasifican en tres niveles : BÁSICO, MEDIO y ALTO, dependiendo de la información que se trataba, a partir del 25 de mayo de 2018, con la aplicación del nuevo Reglamento de Protección de Datos, estas medidas dejan de tener validez, ya que las medidas de seguridad no se van a clasificar en estos niveles, sino que se va a contemplar otro tipo de actuaciones.

Teniendo el artículo 4 punto f) sobre los principios relativos al tratamiento, del RGPD que nos señala que los datos serán:

<<*…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 apropiadas («integridad y confidencialidad»)…*>>

Se parte de la base que en las Administraciones locales, por tanto, y teniendo en cuenta el volumen de datos personales que trata y almacena tendrá que realizar una protección exhaustiva de los datos donde se realiza el tratamiento, realizar una análisis de riesgos, además de revisar las medidas de seguridad con el fin de garantizar el cumplimiento de lo dispuesto en el RGPD.

Por tanto y teniendo en cuenta el artículo 32 del RGPD sobre seguridad de los datos personales , el responsable y los encargados del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que incluya, entre otros:

a) la seudonimización y el cifrado de datos personales;
b) la capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento;

c) la capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico;
d) un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

Además en su punto 2 nos señala que deberemos revisar las políticas de seguridad teniendo en cuenta los riesgos que pueden presentar dicho tratamiento de datos, teniendo en cuanta lo que podría ocurrir como consecuencia de 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.
Por lo que el responsable y el encargado del tratamiento tomarán medidas para garantizar que cualquier empleado público que tenga acceso a datos personales solo pueda tratar dichos datos siguiendo instrucciones del responsable.
En las Administraciones Públicas, las medidas de seguridad exigibles son las de la aplicación del Esquema Nacional de Seguridad (ENS). La finalidad del Esquema Nacional de Seguridad es la creación de las condiciones necesarias de confianza en el uso de los medios electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita a los ciudadanos y a las Administraciones locales, el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
Según su Artículo 4 de Real Decreto 3/2010 Esquema Nacional de Seguridad, los principios básicos del Esquema Nacional de Seguridad son:
a) Seguridad integral.
La seguridad es un proceso completo constituido por todos los elementos técnicos, humanos, materiales y organizativos, relacionados con el sistema de información y habrá que concienciar a todas las personas que intervienen en el proceso y a sus responsables jerárquicos,
b) Gestión de riesgos
El análisis y gestión de riesgos será imprescindible en la gestión de la seguridad y deberá mantenerse permanentemente actualizado, además

permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

c) Prevención, reacción y recuperación.

Para conseguir que las amenazas sobre el sistema no se materialicen, se debe realizar un ejercicio de prevención, detección y corrección, además, Las medidas de prevención deben eliminar o, al menos reducir, la posibilidad de que las amenazas lleguen a materializarse con perjuicio para el sistema. Y debe permitir la restauración de la información y los servicios, de forma que se pueda hacer frente a las situaciones en las que un incidente de seguridad inhabilite los medios habituales.

d) Líneas de defensa.

La protección de los sistemas debe ser una protección por de forma que, cuando una de las capas falle, permita minimizar los tiempos para una reacción adecuada frente a los incidentes que no han podido reducir la probabilidad de que el sistema sea comprometido totalmente. Además éstas deben ser de carácter organizativas, físicas y lógicas.

e) Reevaluación periódica.

Las medidas de seguridad se reevaluarán y actualizarán periódicamente, para adecuar su eficacia a la constante evolución de los riesgos y sistemas de protección.

f) Función diferenciada.

La responsabilidad de la seguridad de los sistemas de información estará diferenciada de la responsabilidad sobre la prestación de los servicios existiendo el responsable de la información, el responsable del servicio y el responsable de la seguridad.

Las administraciones locales deben contar ya con un documento de seguridad, aprobado en sesión plenaria de esa entidad local, donde se establecen la política de seguridad promovida por esa administración. En éste, deben quedar plenamente establecidos los principios básicos y los siguientes requisitos mínimos:

a) Organización e implantación del proceso de seguridad.
b) Análisis y gestión de los riesgos.
c) Gestión de personal.
d) Profesionalidad.
e) Autorización y control de los accesos.
f) Protección de las instalaciones.
g) Adquisición de productos.
h) Seguridad por defecto.
i) Integridad y actualización del sistema.
j) Protección de la información almacenada y en tránsito.
k) Prevención ante otros sistemas de información interconectados.
l) Registro de actividad.
m) Incidentes de seguridad.
n) Continuidad de la actividad.
o) Mejora continua del proceso de seguridad.

En el caso de las Administraciones Locales, tanto el Esquema Nacional de Seguridad como el RGPD establecen la obligación de realizar análisis de riesgos para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicable.

La Federación Española de municipios junto con el CCN-CERT han publicado unos documentos teniendo en cuenta la dimensión municipal que pueden servir de guías para la adecuación del ENS en las entidades locales. Dichas guías son las siguientes:

- Guía estratégica en seguridad para Entes Locales
- Guía para entidades locales de menos de 20000 habitantes

Estas guías las podemos encontrar en la web de Centro Criptológico Nacional, https://www.ccn-cert.cni.es/documentos-publicos/ens/.

9. Análisis de riesgos de protección de datos

Como se ha comentado anteriormente, en el caso de las Administraciones Locales, tanto el Esquema Nacional de Seguridad como el RGPD establecen la obligación de realizar análisis de riesgos, y en el caso del RGPD, para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicable.

El enfoque de la LOPD anterior y el Reglamento de desarrollo de la misma se basaban en un modelo de cumplimiento formal, en el cual nos decían que medidas debíamos aplicar en función de la tipología de los datos tratados. Sin embargo, el enfoque del RGPD se basa en evaluar para cada actividad de tratamiento la probabilidad y la gravedad del riesgo para los derechos y libertades del interesado, teniendo en cuenta la naturaleza, el contexto y los fines del tratamiento. El resultado del mismo determinará si las actividades de tratamiento suponen un riesgo, así como si el riesgo es alto, en cuyo caso deberá realizarse una EIPD.
El Considerando 75 del RGPD nos señala una vulneración grave de los derechos y las libertades fundamentales en los siguientes casos:

- El tratamiento pueda dar lugar a problemas de discriminación, usurpación de identidad o fraude, pérdidas financieras, daño para la reputación, pérdida de confidencialidad de datos sujetos al secreto profesional, reversión no autorizada de la seudonimización o cualquier otro perjuicio económico o social significativo.
- En los casos que se prive a los interesados de sus derechos y libertades o se les impida ejercer el control sobre sus datos personales.
- En los que los datos personales tratados revelen el origen étnico o racial, las opiniones políticas, la religión o creencias filosóficas, la militancia en sindicatos y el tratamiento de datos genéticos, datos relativos a la salud o datos sobre la vida sexual, o las condenas e infracciones penales o medidas de seguridad conexas.

- En los que se evalúen aspectos personales, en particular el análisis o la predicción de aspectos referidos al rendimiento en el trabajo, situación económica, salud, preferencias o intereses personales, fiabilidad o comportamiento, situación o movimientos, con el fin de crear o utilizar perfiles personales.
- Que se traten datos personales de personas vulnerables, en particular niños.
- Que el tratamiento implique una gran cantidad de datos personales y afecte a un gran número de interesados.

Dado lo señalado en el artículo 25 del RGPD, el responsable del tratamiento, teniendo en cuenta los riesgos de puede entrañar el tratamiento para los derechos y libertades de las personas físicas, debe aplicar, desde el diseño como en el propio tratamiento las medidas técnicas y organizativas apropiadas para cumplir con los requisitos del RGPD y proteger los derechos de los interesados. Además debe garantizar que solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

Para la realización de un análisis de riesgos, y una vez conocido una descripción del tratamiento, tendremos que identificar los riesgos o potenciales escenarios de riesgos a los que nos enfrentamos que podrían repercutir negativamente a los derechos y libertades de los terceros con respecto al tratamiento de datos que se realice, por lo que, las decisiones que tengan relación con el tratamiento de los datos de carácter personal, y no sólo las vinculadas a la seguridad de los tratamientos, se deben sustentar en la gestión de los riesgos.

Por lo que, se trata de una obligación mas con respecto al responsable del tratamiento que debe llevar a cabo para seleccionar y adoptar las medidas de carácter técnico y organizativo más adecuadas para garantizar que el tratamiento se hace según lo que prevé el RGPD y demostrar que el tratamiento es conforme al RGPD (principio de responsabilidad proactiva).

Además, gestionar los riesgos implica evaluarlos (articulo 35.7.c RGPD) y tratarlos (articulo 35.7.d del RGPD).

Por lo que hay que hacer una estimación, de la manera más objetiva posible, del nivel o de la zona de riesgo, en que se sitúan las operaciones de tratamiento o el tratamiento en su conjunto.
Por lo que hay que hacer una estimación, de la manera más objetiva posible, del nivel o de la zona de riesgo, en que se sitúan las operaciones de tratamiento o el tratamiento en su conjunto.

En cualquier análisis de riesgos hay que tener en cuenta tres aspectos básicos:

- Activos: Aquello que pretendemos proteger
- Amenaza: Aquello de lo que pretendemos protegernos
- Impacto: Lo que pretendemos evitar

La gestión del riesgo permite determinar, de forma objetiva donde se sitúan las operaciones de tratamiento o el tratamiento en su conjunto y cuál es su zona de riesgo y cómo podemos mitigar ese riesgo, realizando un tratamiento del mismo.
Las fases por tanto, para la realización de una gestión de riesgos en un tratamiento o conjunto de tratamientos de datos serán:

- Evaluación de riesgos
- Tratamiento de riesgos

A su vez, la evaluación de los riesgos debe ser sistemática y se estructura en tres etapas:

- Identificación de los riesgos
- Análisis de los riesgos
- Valoración de los riesgos

El punto de partida es que cualquier tratamiento de datos de carácter personal implica potencialmente algún tipo de riesgo, será el riesgo inherente al tratamiento, que existe solo por el hecho de llevarlo a cabo.

Lo que persigue el proceso de gestión de riesgos es mantenerlo en unos niveles aceptables.

El resultado de la primera evaluación de riesgos nos indica el nivel de riesgo inicial, que debe ser objeto de reducción, para aumentar el control que podemos ejercer sobre el riesgo que generan las operaciones de tratamiento.

Este tratamiento de los riesgos se debe encaminar a seleccionar medidas de carácter técnico y organizativo para reducir la probabilidad y el impacto de las operaciones de tratamiento.

Estas nuevas medidas tienen que reducir el nivel de riesgo de las operaciones de tratamiento. Para verificarlo, debemos volver a analizar y valorar los riesgos, teniendo en cuenta las nuevas medidas previstas.

De este segundo proceso de análisis y valoración nos da como resultado un riesgo, dicho riesgo que, en principio no se puede reducir más, y que se debe aceptar, es el conocido como riesgo residual.

Las etapas de cualquier evaluación de riesgos son por tanto: identificación, análisis y valoración de riesgos

Trataremos los riesgos desde la perspectiva de cada proceso clave o tratamiento que hemos identificado.

Identificación del riesgo

Se debe identificar los riesgos potenciales que implican un daño o perjuicio para las personas afectadas por el tratamiento de los datos, ya sea porque suponen un daño o perjuicio material directo, porque vulneran principios o derechos y libertades o porque el responsable del tratamiento incumple alguna obligación.

Por lo que habrá que evaluar los riesgos teniendo en cuenta las operaciones de tratamiento concretas que se esté evaluando de acuerdo con su contexto y que afecte a: principios, derechos, obligaciones, otros derechos y libertades, y daños y perjuicios directos.

Análisis del riesgo

El objetivo del análisis de riesgos es determinar la probabilidad de que se produzcan amenazas o situaciones no deseadas, así como su impacto.

Por lo que el riesgo se cuantifica de la siguiente manera:

Riesgo = impacto x probabilidad

Por lo que el riesgo es el resultado de multiplicar el impacto que tendría una amenaza por la probabilidad de que esta amenaza llegue a materializarse.

Así pues, el análisis del riesgo concreta las medidas que van a definir para esos procesos claves definidos al inicio o bien para el tratamiento de datos en su conjunto. Con esto se tiene que conseguir, reducir el riesgo potencial o bien reducir el impacto del mismo, si se llegase a producir, o la probabilidad de que esto ocurra.

Dichas medidas podrán ser preventivas, siendo estas definidas para reducir la probabilidad o bien reactivas o de recuperación, definidas para reducir el impacto

Por lo que se podrá conocer el nivel del riesgo inicial del tratamiento de datos que estamos evaluando y poder reducir los riegos del tratamiento.

Valoración del riesgo

Una vez identificadas todas las medidas previstas y definidas inicialmente, se debe valorar su probabilidad y su impacto.
Esto nos proporciona información del nivel de riesgo inicial y nos permite elaborar un primer mapa de riesgos del tratamiento que conecte la probabilidad y el impacto.
Para hacerlo, podemos utilizar cualquier escala de valores que nos permita ubicar de la forma más precisa posible el nivel de riesgo en que se sitúa el tratamiento que estamos evaluando.
Pueden ser valores entre el 1 y el 5 u otra forma cuantitativa.

Probabilidad	
Descripción	**Nivel**
Muy Probable	*5*
Probable	*4*
Posible	*3*
Poco Probable	*2*
Muy raro	*1*

Impacto	
Descripción	**Nivel**
Muy alto	*5*
Alto	*4*
Medio	*3*
Bajo	*2*
Muy Bajo	*1*

Los valores superiores de cada variable de riesgo (probabilidad e impacto) señalan altos niveles de riesgo, que indican que estamos muy cerca de que se produzca la situación de riesgo y que las potenciales consecuencias son bastante graves. Por lo tanto, habrá que realizar una estimación de la probabilidad y del impacto.

Estimación de la probabilidad

En cuanto a la probabilidad, utilizamos principalmente dos criterios de carácter general: por un lado, se debe tener en cuenta de qué manera las medidas previstas pueden reducir la probabilidad y por el otro, se debe considerar hasta qué punto el potencial escenario de riesgo se ha producido en otros tratamientos anteriormente.

La valoración del nivel de riesgo implica un cierto grado de subjetividad. Por lo que tendremos que realizar estimación del riesgo teniendo en cuenta criterios generales que ayuden a valorar el riesgo, y teniendo en cuenta además la eficacia de las medidas previstas. Por lo que:

- Una situación de riesgo es muy rara que se produzca cuando se han previsto varias medidas en forma de “línea de defensa”, es decir, que si falla una siempre hay otra que continúa impidiendo los escenarios no deseados.
- Una situación de riesgo es poco probable que se produzca cuando se han previsto varias medidas en forma de “línea de defensa”, es decir que si falla una hay otra que puede impedir el hecho no deseado, pero no en todos los casos.
- Una situación de riesgo es posible que se produzca cuando las medidas para reducir la probabilidad no están previstas en forma de “línea de

defensa", es decir que si falla una el resto no puede impedir el hecho no deseado.

– Una situación de riesgo probable que se produzca cuando se ha previsto una única medida para reducir su probabilidad y se conoce algún caso en que se ha producido el hecho no deseado.

– Una situación de riesgo es muy probable que se produzca cuando no se ha previsto ninguna medida para reducir su probabilidad y se conocen varios casos en que se ha producido el hecho no deseado.

Estimación del impacto

En cuanto al impacto, utilizaremos criterios relacionados con las características del impacto que puede tener el potencial escenario de riesgo que estamos valorando.

Se pueden tener en cuenta otros criterios específicos de las operaciones de tratamiento, así como la eficacia de las medidas previstas

– Situación de riesgo muy bajo se produce cuando las consecuencias se centran en deficiencias formales leves, relacionadas con las obligaciones materiales del responsable del tratamiento que se pueden corregir con medidas de fácil implantación.

– Situación de riesgo bajo se produce cuando las consecuencias se centran en deficiencias materiales leves, y que se pueden corregir con medidas de fácil implantación.

– Situación de riesgo resulta medio se produce cuando las consecuencias son difíciles de reparar. Dichas consecuencias se pueden corregir implantando medidas o mejorando la eficacia de las medidas implantadas.

– Situación de riesgo alto se produce cuando las consecuencias pueden corregir implantando nuevas medidas o mejorando las existentes, siendo esto complicado para el responsable del tratamiento.

– Una situación de riesgo es muy alto se produce cuando las consecuencias requieren unos esfuerzos desproporcionados del responsable del tratamiento, ya que es prácticamente imposible implantar medidas.

A partir de este punto, ya definidos la estimación de la probabilidad y del impacto, podernos combinarlos en una tabla para calcular el riesgo, teniendo en cuenta las escalas cualitativas del impacto, la probabilidad y el riesgo:

Escala							
Impacto			**Probabilidad**			**Riesgo**	
Muy alto	5	MA	Prácticamente seguro	5	MA	Critico	MA
Alto	4	A	Probable	4	A	Importante	A
Medio	3	M	Posible	3	M	Apreciable	M
Bajo	2	B	Poco Probable	2	B	Bajo	B
Muy Bajo	1	MB	Muy raro	1	MB	Despreciable	MB

RIESGO			**Probabilidad**				
			MB	**B**	**M**	**A**	**MA**
			1	**2**	**3**	**4**	**5**
Impacto	**MA**	**5**	A	MA	MA	MA	MA
	A	**4**	M	A	A	MA	MA
	M	**3**	B	M	M	A	A
	B	**2**	MB	B	B	M	M
	MB	**1**	MB	MB	MB	B	B

Este mapa de riesgos inicial es una representación visual o gráfica del nivel de riesgo en que se sitúa inicialmente el conjunto del tratamiento o un proceso clave concreto.

Para determinar si los riesgos que presentan las operaciones de tratamiento son Critico, Importante, Apreciable, Bajo o Despreciable, los niveles de riesgo se tienen que convertir a una segunda escala.

- Los riesgos valorados con un nivel igual a A o MA se deben considerar riesgos Importantes y críticos y, por lo tanto se deben aplicar medidas para reducir este nivel de riesgo, puesto que las operaciones de tratamiento estarían situadas en un nivel alto de riesgo.
- Cuando el nivel es igual a M el riesgo es apreciable, pero se tiene que procurar que sean eficaces las medidas previstas. Por lo tanto, conviene tratar estos riesgos para procurar bajarlos de nivel.

• Cuando el nivel se sitúa a B o MB el riesgo es bajo o despreciable, puesto que los datos se están tratando en unas condiciones de riesgos razonablemente controlados.

Si el resultado de la valoración de los riesgos es un riesgo MA (riesgo crítico), se deben diseñar medidas para situar estas operaciones de tratamiento en una zona de riesgo tolerable o aceptable.

Se tienen que seleccionar medidas nuevas o modificar y mejorar las previstas, y posteriormente volver a hacer el análisis y la valoración de los riesgos, para analizar si los riesgos han sido modificados y no podemos considerar que están en zonas de riesgo critico.

En el caso de las administraciones locales, para poder realizar un análisis de riesgos, de manera sencilla y visual, el Centro Criptológico Nacional en colaboración con la Agencia Española de Protección de Datos han puesto a disposición la herramienta PILAR que permite evaluar de forma sistemática y objetiva los posibles riesgos en materia de protección de datos y de seguridad de la información, de hecho ya en su versión 7.1.7 (19.2.2018), ya se tiene en cuenta la normativa sobre protección de datos.

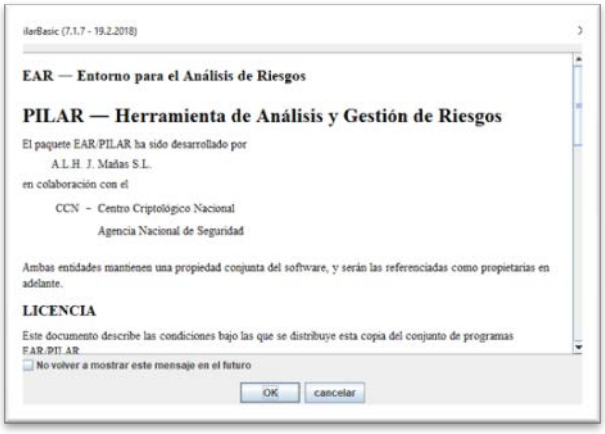


Figura 1. Herramienta Pilar

Pilar, actúa teniendo en cuenta la metodología MAGERIT, metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica y que se utiliza en las administraciones publicas.

Este esquema de trabajo, requiere una evaluación periódica y continua ya que se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), tal y como nos señala en RGPD, este análisis de riesgos se enmarca en el principio de Responsabilidad Proactiva, ya que obliga al responsable del tratamiento a adoptar políticas internas y aplicar medidas de seguridad como puedan ser, entre otras, en reducir al máximo el tratamiento de datos personales, seudonimizar lo antes posible los datos personales, dar transparencia a las funciones y el tratamiento de datos personales, permitiendo a los interesados supervisar el tratamiento de datos y al responsable del tratamiento crear y mejorar elementos de seguridad, y esto se consigue, con el obligado cumplimiento de la realización de aun análisis de riesgos del los tratamientos de datos personales sobre los derechos y libertades de las personas y tomando las medidas de seguridad apropiadas.

10. Evaluaciones de impacto

El artículo 35.1 del RGPD nos señala:

<<…1. Cuando 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 libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares...>>

Con lo expuesto, podemos señalar que las evaluaciones de impacto se deben enmarcar dentro del principio de protección de datos desde el diseño y por defecto (articulo 25.1 RGPD), ya que estas tienes que realizarse antes de iniciar una operación de tratamiento de datos personales.

Las EIPD son instrumentos importantes para la rendición de cuentas, ya que ayudan a los responsables no solo a cumplir los requisitos del RGPD, sino también a demostrar que se han tomado medidas adecuadas para garantizar el cumplimiento del Reglamento. En otras palabras, una EIPD es un proceso utilizado para reforzar y demostrar el cumplimiento. Por lo que se están enmarcadas dentro del principio de responsabilidad proactiva, ya que facilita no solo cumplir con el Reglamento sino poder demostrarlo.

Por lo que las EIPD permiten determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel aceptable o residual.

Habrá que realizar, de manera obligatoria, una evaluación de impacto en los siguientes supuesto que nos señala el RGPD:

a) evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles,

b) tratamiento a gran escala de las categorías especiales de datos, es decir: *«el origen étnico o racial, las opiniones políticas, las convicciones religiosas o*

filosóficas, o la afiliación sindical, y el tratamiento de datos genéticos, datos biométricos dirigidos a identificar de manera unívoca a una persona física, datos relativos a la salud o datos relativos a la vida sexual o las orientación sexuales de una persona física», así como los datos relativos a condenas e infracciones penales (descritos en el artículo 10 del Reglamento).

c) observación sistemática a gran escala de una zona de acceso público.

Aunque, en estos casos son obligatorias, pueden existir otros tratamientos, que no estén en estos supuestos que también requieran una, por los riesgos altos que presentan, una evaluación de impacto.

Además, en el caso que el responsable considere que no es necesario la realización de una evaluación de impacto en un tratamiento de datos, deberá justificarlo y documentarlo, incluyendo la opinión del delegado d Protección de datos.

Hay que tener en cuenta que una vez realizado dicha evaluación de impacto, esta implica un riego alto que no puede ser mitigado o controlado por las medidas de seguridad propuestas por el responsable del tratamiento, se tiene que consultar a la autoridad de control, AGPD, que es lo que hay que hacer, antes de iniciar dicho tratamiento.

El artículo 36.1 del RGPD, sobre consulta previa nos señala:

<<…1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo…>>

Por lo que, el responsable del tratamiento, si ha realizado la evaluación de impacto, y esta arroja un resultado de riesgo alto, y además no ha sido capaz de mitigar ese riesgo, con las medidas de seguridad pertinentes, debe realizar una consulta previa a la autoridad de control, la AGPD, y ésta, en un plazo de 8 semanas deberá contestar por escrito, o bien se puede ampliar este plazo a 6 semanas debida a la complejidad de la misma. La autoridad de control, puede entre tanto, limitar o prohibir dicho tratamiento al responsable del tratamiento.

Por último, el RGPD igualmente establece que las autoridades de control deberán establecer y publicar, una lista de los tipos de operaciones de tratamiento que estarán sujetos a la exigencia de llevar a cabo una evaluación de impacto relativa a la protección de datos.

En los casos en que no esté claro si se requiere una evaluación de impacto, se recomienda que esta se lleve a cabo, ya que en cualquier caso, la evaluación de impacto es una herramienta útil para ayudar a los responsables de tratamientos a cumplir con la legislación de protección de datos.

Dicho todo esto, y tal como señala el artículo 35.7 del RGPD, la evaluación deberá incluir como mínimo:

a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento,

b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;

c) una análisis de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.

En"La Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)", publicada por la APDCAT en su web en su página 22, nos muestra un flujograma o fases para realizar una evaluación de impacto, donde cada fase tiene una serie de actividades a realizar y a partir de aquí se van a desarrollar:

Antes de realizar cada una de las fases de una evaluación de impacto, haya que tener en cuenta unos prerrequisitos como puedan ser la identificación de los diferentes roles o actores que tiene que proporcionar información del tipo organizativo, funcional y tecnológico, así como del análisis de riesgos y medidas de seguridad y validar las propuestas del al EIPD.

Estos actores intervinientes pueden ser, el responsable del tratamiento, los encargados de tratamientos, los responsables de seguridad o departamento de tecnologías de la información, delegado de protección de datos, etc.

Una vez tengamos esto definido se iniciara el proceso de evaluación de impacto.

Las fases por tanto, para la realización de una evaluación de impacto en la protección de datos personales serán:

- **Análisis previo: obligación de una EIPD**
- **Descripción sistemática del tratamiento**
- **Gestión del Riesgo**
- **Informe de evaluación de impacto**
- **Supervisión de la implantación**
- **Revisión del tratamiento de la EIPD**

Análisis previo: obligación del tratamiento

Lo primero que tenemos que tener en cuenta en esta fase, ya que, o bien vamos a realizar una nueva actividad, o bien hemos realizado cambios sustanciales en un tratamiento que ya estábamos realizando y presuponemos que requiere una evaluación de impacto por el riego alto al que nos enfrentamos, son los datos a tratar, y a operaciones se hará con ellos. Por lo tanto:

- Tipos de datos (datos personales, datos de categorías especiales)
- Volumen. de datos aproximado o diferentes tipos de datos
- Operaciones de tratamiento de esos datos (recogida, almacenamiento, anonimizacion, consulta, modificación, supresión, etc., tecnologías asociadas)

Como carácter general, no se debe realizar una evaluación de impacto cuando no suponga un riesgo alto para los derechos y libertades de las personas físicas, si en este punto se considera esto deberemos documentarlo.

Se puede considerar, con carácter general que se puede incurrir en una vulneración grave de los derechos y libertades de las personas físicas y por tanto tener un riego alto, deberemos realizar hasta tres niveles de análisis

Primer nivel de análisis:

Habrá que verificar si el tratamiento está incluido en las listas previstas del artículo 35.4 y 35.5 del RGPD. Si no se encuentra en ella, no será necesaria la realización de dicha evaluación de impacto.

Si se encuentra en esa lista, deberemos pasar a un segundo nivel de análisis

Segundo nivel de análisis:

Habrá que verificar si el tratamiento está incluido en las listas previstas del artículo 35.3 del RGPD. Si el tratamiento no encaja, tendremos que realizar un tercer análisis.

Tercer nivel:

El tercer nivel es más general, se basa en el artículo 35.1 del RGPD y se debe verificar lo siguiente:

- Naturaleza del tratamiento:
- Alcance del mismo

- Contexto del tratamiento
- Finalidades

Una vez analizada toda esta información, ya estaríamos en disposición si el tratamiento requiere una EIPD o no y se documentara en un informe. En el caso que se requiera la evaluación de impacto, pasaríamos a la siguiente fase.

Descripción sistemática de las operaciones de tratamiento.

Tal como señala el artículo 35.7 del RGPD, La evaluación deberá incluir, entre otros:

<<…a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento…>>

La descripción sistemática de las operaciones de tratamiento describe la descripción del tratamiento con detalle y el conjunto de elementos que forman parte del sistema para poder realizar las operaciones relacionadas con ese tratamiento. Para realizarlo, se tiene en cuenta los siguientes:

- Descripción funcional del tratamiento que se está evaluando
- Detalle de elementos más importantes del sistema teniendo en cuenta los datos personales

Descripción funcional del tratamiento que se está evaluando

Para hacer una descripción del tratamiento que se está evaluando tendremos que tener en cuenta el ciclo de vida de la información, dividiendo en 4 etapas:

- Etapa 1 -> Entrada (Origen de la recogida de datos, formularios, extracción de datos, etc. y la forma de recoger esos datos (propio interesado, tercero, dispositivo, etc.)
- Etapa 2 -> Almacenamiento (operaciones y tecnologías que permiten la conservación de los datos, y la forma de almacenarla, sistemas propios, de terceros, etc.)
- Etapa 3 -> Acceso (funciones y permisos de diferentes usuarios a los datos)
- Etapa 4 -> Supresión (tiempo de conservación de los datos y procedimientos de supresión, bloqueo y destrucción)

Detalle de elementos más importantes del sistema teniendo en cuenta los datos personales

Se realizara una descripción del sistema por capas, teniendo en cuenta estas 5 capas:

- Capa 1 -> Procesos clave
- Capa 2 -> Modelo de datos
- Capa 3 -> Intervinientes
- Capa 4 ->Flujos de información
- Capa 5 -> Tecnologías

Capa 1 -> Procesos clave

Habrá que describir los procesos claves del que tenemos que evaluar, teniendo en cuenta que un proceso clave está formado por un conjunto de operaciones de tratamiento de datos personales, que se aplican a un conjunto de datos (entrada) y transforman la información o resultado (salida de proceso). Para que resulte más simple se puede utilizar como modelo lo propuesto por la guía "la Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)", publicada por la APDCAT en su web en su página 46, e utilizar dicha tabla para identificar los procesos:

Identificación del proceso	[nombre del proceso]		Código [si resulta útil]
Entrada(*) (clases de datos)	[A]	[B]	
Mecanismo de recogida	Origen datos	Almacenamiento datos	Función principal
Operaciones de tratamiento	[por ejemplo: formulario web]	[por ejemplo: persona interesada]	[por ejemplo: base de datos en proveedor externo (nube)]	[por ejemplo: recogida de datos básicos de identificación para darse de alta en el servicio]
Resultado principal del proceso	[por ejemplo: incorporación de los datos básicos en el sistema, creación y entrega del mecanismo de acreditación y verificación de los medios de contacto (correo electrónico, teléfono, etc.)]		

(*) Recordatorio (de la plantilla de recogida de información sobre los datos y operaciones de tratamiento)

Clase A. Datos de carácter personal facilitados directamente por las personas afectadas

Clase B. Datos de carácter personal facilitados por terceros

Clase C. Datos de carácter personal ya disponibles anteriormente

Clase D. Datos de carácter personal capturados

Clase I. Datos de carácter personal calculados

Clase Z. Datos que inicialmente no se consideran de carácter personal

Capa 2 -> Modelo de datos

Aquí se identificara los datos personales relacionados con cada uno de los procesos que han sido definidos en la capa 1 procesos clave.

Por lo que se elaborara una lista y se indicara atributos de los datos como pueda ser si es una categoría especial de dato o si se puede prescindir de ese dato. Para que resulte más simple se puede utilizar como modelo lo propuesto por la guía “la Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)”, publicada por la APDCAT en su web en su página 47, e utilizar dicha tabla

Identificación proceso	[nombre del proceso]	Código [si se utiliza]	
		Crítico [valoración]*	
Datos	Descripción	Especial	Prescindible
[Identificador]	[Código único de identificación de la persona en el sistema]	☐	☐
[Nombre]	[Nombre]	☐	☐
[Apellidos]	[Apellidos]	☐	☐
[Usuario]	[Código usuario]	☐	☐
[Contraseña]	[Contraseña elegida por el usuario]	☐	☐
[Correo electrónico]	[Dirección de correo electrónico]	☐	☐
[Dirección IP]	[Dirección IP desde la cual se ha hecho el alta]	☐	☐
etc.	...	☐	☐

:

Capa 3 -> Intervinientes

Cada uno de los intervinientes que están implicados en el tratamiento de esos datos, como puedan ser el responsable del tratamiento, los encargados, empresas proveedores de soluciones de terceros, etc., además estos deben tener claramente definidas sus funciones y sus rol dentro del sistema.

La ISO/IEC 29134 clasifica la parte intervinientes en cuatro grupos: personas afectadas, responsable del tratamiento, encargado del tratamiento y terceras partes; esta clasificación se puede utilizar para concretar la función o rol principal.

Para que resulte más simple se puede utilizar como modelo lo propuesto por la guía “la Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)”, publicada por la APDCAT en su web en su página 48, e utilizar dicha tabla

	Procesos			
Intervinientes	[código proceso]	[código proceso]	[código proceso]	etc.
[...]	x	x	x	□
	Función o rol principal: [...]			
[...]	x	□	□	□
	Función o rol principal: [...]			

Capa 4 ->Flujos de información

Se describirá los movimientos de información, de forma que dispongamos de un mapa claro de quien tiene acceso a datos personales y en qué momento.

Para que resulte más simple se puede utilizar como modelo lo propuesto por la guía “la Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)”, publicada por la APDCAT en su web en su página 49, e utilizar dicha tabla

Proceso	[alta usuario]		Código		[código]
Operaciones (*)	**Entrada**	**Almacenamiento**	**Acceso**	**Supresión**[38]	
Intervinientes origen					Intervinientes destino
[usuario]	x	□	□	□	[proveedor alojamiento aplicación] [responsable del tratamiento]
[proveedor alojamiento aplicación]	x	x	□	□	[responsable del tratamiento]
[responsable del tratamiento]	x	x	x	x	n/a
etc.	□	□	□	□	etc.

Capa 5 -> Tecnologías

En esta capa, se identificara las tecnologías más relevantes que estarán presentes en el tratamiento de datos de carácter personal, de manera conceptual, por lo que habrá que realizar un inventario de las tecnologías que intervienen y su vinculación con los proceso.

Por último, para la realización de la descripción del tratamiento, se tendría que añadir las finalidades del tratamiento y la evaluación de la proporcionalidad de las operaciones de tratamiento.

Se debe determinar si se cumple el requisito de necesidad, tanto en relación a la actividad del responsable del tratamiento como en relación a la finalidad del mismo tratamiento.

Gestión del Riesgo (ver Capitulo análisis de riesgos)

Si el resultado de la valoración de los riesgos es un riesgo inaceptable (riesgo alto), se deben implantar medidas para situar estas operaciones de tratamiento en una zona de riesgo tolerable o aceptable.

Habrá que seleccionar medidas nuevas o modificar y mejorar las previstas, y posteriormente volver a hacer el análisis y la valoración de los potenciales escenarios de riesgos, para verificar si los riesgos se han modificado y si ya podemos considerar que no están en zonas de riesgo alto.

Hay que recordar, que si no se puede reducir el nivel de riesgo, y éste se mantiene alto, se tiene que hacer una consulta previa a la autoridad de protección de datos.

Informe de evaluación de impacto

El informe final de la evaluación de impacto es la base para implantar las medidas que servirán para mitigar los riesgos del tratamiento.

El documento final que recoge la evaluación de impacto tiene que transmitir con claridad que se ha tenido en cuenta el contenido mínimo que exige el artículo 35.7 del RGPD.

Debe ser un documento con la evaluación del el impacto de las operaciones de tratamiento y las conclusiones y recomendaciones para minimizar los riesgos inherentes al tratamiento.

Supervisión de la implantación y Revisión del tratamiento de la EIPD

Una vez que tenemos el informe final de la evaluación de impacto siendo esta la base para implantar las medidas encaminadas a mitigar los riesgos del tratamiento y se ha supervisado que las medidas se han implantado tal como ha sido definido en la EIPD, ya se puede iniciar el tratamiento en cuestión.

Por lo que habrá que revisar si las previsiones de impacto iniciales continúan siendo válidas, o si ha habido cambios sustanciales que afectan a las operaciones de tratamiento y ser objeto de especial monitorización por parte del responsable del tratamiento, y de especial supervisión por parte de delegado de protección de datos .

Por lo tanto, se debe supervisar tanto desde el diseño final como en su implantación.

En cuanto al Delegado de Protección, éste debe ofrecer el asesoramiento que se le pida sobre la evaluación de impacto relativa a la protección de datos, y supervisar su aplicación.

En cuanto a las revisiones, se tienen que prever dos tipos de revisiones: ordinarias y extraordinarias.

Para las ordinarias, la periodicidad adecuada es cada dos o tres años, en todo caso se trata de una decisión que debe tomar el responsable del tratamiento a la vista de las particularidades y riesgo que potencialmente implica.

Las revisiones extraordinarias se tienen que hacer cuando las operaciones de tratamiento se modifican sustancialmente, porque se introducen nuevas tecnologías, nuevas finalidades, nuevos datos, nuevos afectados, etc. En este caso, es conveniente hacer una evaluación de impacto más completa, para actualizar la evaluación inicial de acuerdo con los cambios relevantes que se han producido en las condiciones del tratamiento.

Nota:

Para que resulte más simple todo el proceso de la realización de la evaluación de impacto se puede utilizar como modelo lo propuesto por la guía “la Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0)”, publicada por la APDCAT en su parte 3, donde se proponen unos modelos para su realización.

11. Notificación de brechas de seguridad

En la definición dada en el artículo 4 del RGPD señala que una violación de la seguridad de los datos personales es:

<<… toda violación de la 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…>>

El RGPD, por lo tanto, presenta otra nueva obligación para el responsable y el encargado del tratamiento las organizaciones, la aplicación de medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, en el caso que haya una violación, es de obligado cumplimiento notificar a la autoridad de control (AGPD), de cualquier fuga de datos personal que pueda ocasionar un riesgo para los derechos y las libertades de los individuos.

Cuando ese riesgo se considere alto, la notificación también debe ampliarse a los interesados de los datos afectados.

Las notificaciones se deben realizar “sin dilación indebida” y donde sea factible en el plazo de 72 horas desde la aparición del evento.

Tal y como señala el artículo 33.1 del mismo texto legal:

<<…En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación. ..>

Además, el obligación del encargado del tratamiento el notificar “sin dilación indebida” al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.

Dicha notificación, deberá contener como mínimo:
a) Una descripción de la naturaleza de la violación de la seguridad de los datos personales, y cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
b) El nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
c) Una descripción de las posibles consecuencias de la violación de la seguridad de los datos personales;

Además se deberá realizar una descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner solución a esa violación de la seguridad de los datos personales, y cuando sea posible las medidas adoptadas para mitigar los posibles efectos negativos.

En el caso que no se tuviese toda esa información, esta será facilitada de manera gradual y sin dilación además, el responsable del tratamiento documentará toda violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control que se está cumpliendo de lo dispuesto en el presente artículo.
Por lo que, estamos ante la **obligación de notificar a las organizaciones pertinentes de cualquier fuga de datos que pueda ocasionar un riesgo para los derechos y las libertades de los individuos.**
Por lo que, el responsable del tratamiento debe llevar a cabo un registro en el cual se recojan el lugar, día y hora de detección de la violación de seguridad, así como también los sistemas, datos y equipos que se han visto afectados.
En las administraciones locales el **responsable del tratamiento** será este el encargado de notificar la violación de seguridad, previa consulta con el Delegado de Protección de Datos.

En cuanto a la comunicación al interesado de las violaciones de seguridad, en el artículo 34 del RGPD se señala que:

<<…1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.

2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).

3. La comunicación al interesado a que se refiere el apartado 1 no será necesaria si se cumple alguna de las condiciones siguientes:

a) el responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas apropiadas y estas medidas se han aplicado a los datos personales afectados por la violación de la seguridad de los datos personales, en particular aquellas que hagan ininteligibles los datos personales para cualquier persona que no esté autorizada a acceder a ellos, como el cifrado;

b) el responsable del tratamiento ha tomado medidas ulteriores que garanticen que ya no exista la probabilidad de que se concretice el alto riesgo para los derechos y libertades del interesado a que se refiere el apartado 1;

c) suponga un esfuerzo desproporcionado. En este caso, se optará en su lugar por una comunicación pública o una medida semejante por la que se informe de manera igualmente efectiva a los interesados.

4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3….>>

12. La figura del Delegados de Protección de Datos (DPO)

El Reglamento General de Protección de Datos (RGPD) obliga que los responsables y encargados de tratamiento deberán designar un Delegado de Protección de Datos (DPO) en el supuesto que se trate de una administración pública.

Por lo que, las administraciones publicas deberán nombrar a un Delegado de Protección de Datos de manera obligatoria. Esta designación del DPO en el ámbito público deberá haberse producido con antelación a la fecha de aplicación del RGPD, 25 de mayo de 2018.

Además, el articulo 37 nos señala como debe ser la designación del Delegado de Protección de Datos, de aquí en adelante, DPO.

<<… *1.El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:*

a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;…>>

Además en sus apartados 3, 5, 6 y 7:

<<*…3.Cuando el responsable o el encargado del tratamiento sea una autoridad u organismo público, se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.*

5.El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.

6. El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control…>

En este sentido, las Administraciones Locales, actúan como responsables y encargadas de los tratamientos de datos personales en ejercicio de sus funciones, por lo que será obligatorio contar con esta figura tal y como estima el artículo 37 del RGPD.

En el caso de las administraciones Públicas se podrán tener en cuenta varios supuestos:

- Se podrá designar un único delegado de protección de datos para varias de estas autoridades u organismos, teniendo en cuenta su estructura organizativa y tamaño.
- Podrá formar parte de la plantilla interna de la Administración Local a tiempo completo o parcial o incluso desempeñar sus funciones en el marco de un contrato de servicios.
- Y se permite que se contraten externamente las funciones de Delegado de Protección de Datos, considerando esta opción la más ventajosa para los municipios pequeños puesto que podrán beneficiarse de los servicios que, en su caso, ofrezcan la diputación provincial, cabildos o la comunidad autónoma, así como contratar servicios de entidades privadas especializadas.

Este Delegado será designado atendiendo a sus cualidades profesionales, a sus conocimientos especializados del derecho (pero no siendo necesario que sea Licenciado en derecho) así como con conocimientos en Nuevas Tecnologías y en Protección de datos.

El método de evaluación se basará tanto en la valoración del conocimiento y experiencia, como en el desarrollo profesional continuo. La provisión de los puestos de trabajo requerirá la selección de empleados públicos que reúnan tales requisitos.

La Agencia Española de Protección de Datos cuenta con un sistema de certificación de Delegado de Protección de Datos en el cual el candidato deberá justificar la experiencia profesional en materia de protección de datos, así como superar una prueba de evaluación teórica mediante la realización de un examen, aunque esto no es obligatorio.

Una vez designado el Delegado de Protección de Datos en esa entidad local, los responsables del tratamiento deben publicar sus datos de contactos y comunicarlos a la autoridad de control, en este caso, la AGPD.

Posición del DPD: funciones, obligaciones e independencia.

Teniendo en cuenta lo señalado en el artículo 38 del RGPD, el responsable y el encargado del tratamiento garantizarán la participación adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.
De esta forma, es fundamental que el DPO participe desde la etapa más temprana posible en las cuestiones relativas a la protección de datos, para así evitar cualquier riesgo o vulneración de los mismos.
Asimismo, el responsable y/o el encargado del tratamiento deberán facilitar al DPO los recursos necesarios para el ejercicio de sus funciones. De esta forma **el DPO tiene derecho** a contar con los siguientes aspectos:

- Actuar como punto de contacto para la Agencia de Protección de Datos y los interesados.
- Supervisar respuestas a requerimientos de la Agencia de Protección de Datos.
- Diseñar e implantar medidas de información a los afectados por los tratamientos de datos.
- Mantenimiento y gestión de los Registros de Actividades de Tratamiento.
- Cualesquiera otras relacionadas con las anteriores.
- Derecho a que sea comunicada su designación a todo el personal de la Administración Pública para garantizar que su existencia y función se conozca dentro de la misma.

- Apoyo activo a su labor por parte de la alta dirección.
- Contar con tiempo suficiente para el cumplimiento de sus funciones.
- Disponer del apoyo adecuado en relación a los recursos financieros, infraestructuras y personal, en su caso.
- Acceder a otros servicios dentro de la organización, para que de esta forma puedan recibir apoyo, aportaciones o información de estos otros servicios cuando fuere necesario para el ejercicio de sus funciones.
- Derecho a una formación continua, con el fin de mantener actualizados sus conocimientos en el ámbito de la protección de datos.

En lo relativo a las **obligaciones del Delegado de Protección de Datos** cabe destacar las siguientes:

- Deberá rendir cuentas directamente al más alto nivel jerárquico del responsable o encargado del tratamiento.
- Está obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones.
- Deberá atender cualquier cuestión de los interesados, ya que los mismos podrán ponerse en contacto con él en relación al tratamiento de sus datos personales.
- El DPO no puede ocupar un puesto dentro de la organización pueda que incurrir en un conflicto de intereses en el ejercicio de sus funciones, por ejemplo, no puede ser el secretario de la entidad así como no puede ser el responsable de informática de esa entidad ya que esto podría provocar un conflicto de intereses.

Sin embargo, tal y como indica el propio artículo 39 del RGPD, estas funciones son las mínimas que el DPO tiene que tener atribuidas para poder ser considerado como tal, sin perjuicio de que cada responsable o encargado pueda atribuirle **otras funciones,** como pueden ser:

- Identificación de las bases jurídicas del tratamiento.
- Prestar atención a los riesgos asociados a las operaciones de tratamiento.
- Asegurar la existencia y mantenimiento de documentación obligatoria.

- Supervisar la gestión de las quiebras de seguridad en el tratamiento de datos.
- Actuar como punto de contacto para la Agencia de Protección de Datos y los interesados.
- Supervisar respuestas a requerimientos de la Agencia de Protección de Datos.
- Diseñar e implantar medidas de información a los afectados por los tratamientos de datos.
- Mantenimiento y gestión de los Registros de Actividades de Tratamiento.
- Cualesquiera otras relacionadas con las anteriores.

Además, el Delegado de Protección de Datos debe desempeñar sus funciones y cometidos de una manera independiente, y así como a no recibir ninguna instrucción durante el desempeño de funciones y está obligado a mantener el secreto o la confidencialidad en el desarrollo de las mismas.

Hay que destacar que el DPO no es personalmente responsable del incumplimiento del Reglamento, sino que es el responsable o encargado del tratamiento quien debe garantizar el cumplimiento del mismo.

13. Contratos de encargo de tratamiento

El articulo 28.1 nos define otra de las novedades que nos ofrece el RGPD que es que el responsable del tratamiento debe recurrir a encargados que ofrezcan suficientes garantías respecto a la aplicación de medidas técnicas y organizativas que cumplan los requisitos del presente Reglamento, incluida la seguridad del tratamiento y garantice la protección de los derechos del interesado.

La relación entre el responsable y el encargado puede basarse en un contrato individual o en cláusulas contractuales tipo que vincule al encargado respecto del responsable y establezca como mínimo:

- el objeto,
- la duración,
- la naturaleza y la finalidad del tratamiento,
- el tipo de datos personales y categorías de interesados,
- y las obligaciones y derechos del responsable.

Dicho contrato o acto jurídico estipulará lo siguiente referente al encargado:

a) Instrucciones del responsable:

Tratará los datos personales únicamente siguiendo instrucciones del responsable. Se identificara de manera clara cuales son los tratamientos de datos a realizar, de acuerdo al tipo de servicio prestado y a la forma de prestarlo.

Se incluirá las instrucciones con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento.

b) Confidencialidad:

   El encargado 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) Medidas de seguridad:

El encargado tomará todas las medidas necesarias de conformidad con el artículo 32; por lo que el encargado y el responsable establecerán las medidas técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo existente.

d) Subcontratación:

El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable del tratamiento.

Además, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.

Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se hará mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, sujeto a las mismas condiciones y a la misma forma que el encargado del tratamiento, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento.

Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.

e) Derechos de los interesados

El encargado asistirá al responsable, 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) colaboración en el cumplimiento de las obligaciones de los responsables

Ayudará al responsable a garantizar el cumplimiento de las obligaciones relativas a la aplicación de las medidas de seguridad, notificación de

violaciones de datos, comunicación de violaciones de datos a los interesados, realización de evaluaciones de impacto y consultas previas.

g) destino de datos al finalizar el contrato

Según decisión del responsable, el encargado 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) Colaboración con el responsable para demostrar cumplimiento

Pondrá a disposición del responsable 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. El encargado informará inmediatamente al responsable si, una instrucción infringe el presente Reglamento u otras disposiciones en materia de protección de datos de la Unión o de los Estados miembros.

En la guía publicada por al AGPD, “Directrices para la elaboración de contratos entre responsables y encargados del tratamiento” en su Anexo 1 se muestra un ejemplo de clausulas contractuales para supuestos en el que el encargado del tratamiento trate los datos en sus locales y exclusivamente con sus sistemas, como carácter orientativo.

Los contratos de Encargado de tratamiento anteriores a la aplicación del RGPD deberán ser revisados y modificarse de acuerdo al RGPD.

14. Transferencias internacionales de datos personales

El RGPD mantiene el modelo de transferencias internacionales ya establecidos en la Directiva 95/46 y en la LOPD, pero amplía el catálogo de instrumentos para ofrecer garantías suficientes que solo requerirán de autorización previa de las autoridades de protección de datos en muy pocos supuestos.

Dado que en las administraciones locales se realizan transferencias internacionales de datos debido, sobre todo, al aumento de servicios "en la nube", al no garantizarse de manera adecuada el nivel de protección de datos de los derechos fundamentales, se debe tener en cuenta los supuestos presentados por el nuevo Reglamento a la hora de realizar dichas transferencias.

Como novedad en el RGPD, es que tanto el responsable del tratamiento como el encargado pueden realizar transferencias internacionales eliminando la restricción que existía en la LOPD que solo podía ser el responsable del tratamiento.

Además, se amplía el catalogo de instrumentos para ofrecer las garantías adecuadas y, por tanto, proteger los derechos de los afectados como consecuencia de la transferencia de datos.

Con la aplicación del RGPD, las transferencias se pueden realizar sin necesidad de autorización previa, salvo que las garantías se aporten a través de un contrato ad hoc o de un acuerdo administrativo entre autoridades públicas, ni de notificación a la autoridad de control, excepto unos supuestos concretos.

En el RGPD se establece los siguientes tipos para las transferencias internacionales:

- Transferencias internacionales de datos basadas en una decisión de adecuación (artículo 45 RGPD).

- Transferencias mediante garantías adecuadas (artículo 46 RGPD)
- “Binding corporate rules” (artículo 47 RGPD)
- Y añade excepciones (articulo 49 RGPD)

Transferencias internacionales basadas en una decisión de adecuación

El artículo 45.1 del RGPD señala:

<<…*Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica*…>>

Por lo que ya no será necesario notificar la transferencia a la AGPD.

A continuación se enumera la lista de países con nivel adecuado de protección, que se encuentra publicado en la página web de la Agencia de Protección de Datos.

Hasta la fecha, han sido considerados que una protección adecuada:

- Andorra
- Argentina
- Canadá (Sector privado)
- Suiza
- Islas Feroe
- Guernsey
- Israel
- Isla de Man
- Jersey
- Nueva Zelanda
- Uruguay

La Comisión, revisara periódicamente, al menos cada 4 años que garantizan un nivel de protección adecuado a tenor de lo dispuesto en el apartado 2 del presente artículo. Además, si tras dicha revisión, ya no se no garantiza un nivel

de protección adecuado, se derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión anteriormente tomada.

Transferencias internacionales mediante garantías adecuadas

El responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional ofreciendo garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.

Según los requisitos para aportar dichas garantías, pueden distinguirse entre las que requieren y las que no requieren de autorización de una autoridad de control.

Requisitos que deben tener las transferencias internacionales que no requieren autorización por parte de la AEPD (art. 46.2 RGPD):

- instrumentos jurídicamente vinculantes entre autoridades públicas;

- Normas corporativas vinculantes;
- cláusulas tipo adoptadas por la Comisión;
- cláusulas tipo adoptadas por una autoridad de control y aprobadas por la Comisión
- un código de conducta
- un mecanismo de certificación

Requisitos que deben tener las transferencias internacionales que requieren autorización de una autoridad de control (art. 46.3 RGPD):

a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional,

b) acuerdos administrativos entre autoridades públicas.

Además, se tendrá en cuenta que las autorizaciones otorgadas por un Estado miembro o una autoridad de control de conformidad seguirán siendo válidas hasta que hayan sido modificadas, sustituidas o derogadas, por dicha autoridad de control.

Normas corporativas vinculantes o "*Binding corporate rules*"

El artículo 47 RGPD establece que la autoridad de control aprobará normas corporativas de carácter vinculante a las que se podrán unir los grupos de empresas, permitiendo salvaguardar la transferencia de datos. Las normas corporativas vinculantes son las que se dan dentro de un grupo empresarial o una unión de empresas dedicadas a una actividad económica conjunta para la realización de transferencias internacionales que estén situadas en países donde no exista una garantía adecuada.

Excepciones para situaciones específicas

El RGPD en su artículo 49, también contempla unos supuestos para realizar transferencias internacionales sin cumplir ninguna de los tres puntos anteriores:

1. consentimiento explícito e informado del de los riesgos
2. sea necesaria para la ejecución de un contrato o precontrato entre el interesado y el responsable;
3. sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable y un tercero;
4. sea necesaria por razones importantes de interés público;
5. sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;
6. sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté incapacitado para dar su consentimiento;
7. se realice desde un registro público que tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o persona con interés legítimo.

15. Régimen sancionador en las Administraciones Locales

El Reglamento General de Protección de Datos presenta un nuevo régimen sancionador establecido en el articulo 83 *«Condiciones generales para la imposición de multas administrativas*» en su punto 7 y en el artículo 84 denominado «*Sanciones*».

<<… *Sin perjuicio de los poderes correctivos de las autoridades de control en virtud del artículo 58, apartado 2, cada Estado miembro podrá establecer normas sobre si se puede, y en qué medida, imponer multas administrativas a autoridades y organismos públicos establecidos en dicho Estado miembro*…>>

De aquí se desprende que dependerá de la normativa de cada Estado Miembro, para determinar si a las Administraciones Locales se le pueden imponer dichas multas administrativas.

Asimismo, el artículo 84 del RGPD, regulador de las Sanciones determina dos aspectos:

- Los Estados Miembros establecerán las normas en materia de otras sanciones aplicables a las infracciones del RGPD y se adoptarán todas las medidas necesarias para garantizar su observancia.
- Cada Estado notificará a la Comisión, antes del 25 de mayo de 2018, las disposiciones legislativas que se adopten según las citadas sanciones, así como cualquier modificación posterior que le sea aplicable.

Además, en el Proyecto de Ley Orgánica de Protección de Datos, aún en tramitación parlamentaria, en su artículo 77.1.c señala:

<<…1. El régimen establecido en este artículo será de aplicación a los tratamientos de los que sean responsables o encargados:

c) La Administración General del Estado, las Administraciones de las comunidades autónomas y las entidades que integran la Administración Local…>>

Por tanto, visto lo dispuesto en el RGPD y en el Proyecto de ley de Protección de datos en relación al régimen sancionador y con respecto a las Administraciones Públicas, las Administraciones Locales al ser responsables del tratamiento de datos estarán sometidas al RGPD pudiendo incurrir en la comisión de infracciones.

Es decir, se prevé por tanto que la autoridad de protección de datos podrá realizar sanciones, en los casos que procedan, a las entidades locales con apercibimiento, indicando las medidas a adoptar para el cese o corrección de la conducta.

16. Conclusiones

El Reglamento europeo de protección de datos, ya se encuentra en vigor desde el 25 de mayo, supone un fuerte impulso por armonizar la distinta legislación y garantizar el máximo nivel de protección ya que, obliga a las empresas privadas e instituciones públicas a afrontar un importante proceso de readaptación normativa.

Nos encontramos con una nueva regulación en cuanto a la protección de datos, con muchas obligaciones para los responsables de los tratamientos en las administraciones locales, dado que se da un enfoque muy proactivo con las novedades que en este reglamento se presentan.

Esta normativa, que entró en vigor en mayo del 2016, y dando un plazo de adaptación de las empresas y organizaciones, de dos años hasta su entrada en aplicación, ya está aquí, pero desgraciadamente, como norma general, y dada su complejidad y dificultad, hay pocas entidades que se encuentren en disposición de decir que ya están adaptadas al nuevo Reglamento.

Con la aplicación del RGPD, se introducen novedades como pueda ser, el principio de la responsabilidad proactiva obligando al responsable del tratamiento de datos a adoptar un enfoque proactivo el principio de responsabilidad activa, la Privacidad desde el Diseño y por Defecto, el contenido del derecho de información en la recogida de datos que debe facilitarse a los afectados ya se que deberá facilitar a los interesados toda la información que precisen en relación con el tratamiento de sus datos personales de una manera ser concisa, fácilmente accesible y fácil de entender.

Por otro lado, aparece la figura del Delegado de Protección de datos es novedosa en España, se trata de una figura de gran importancia práctica ya que supone la garantía del cumplimiento de la normativa de protección de

datos en las Administraciones Públicas, las cuales tienen obligación de contar con esta figura.

Otras de las novedades ya no será necesario realizar la inscripción de los ficheros ya se establece la obligación de tener, por parte de los responsables y encargados del tratamiento de datos, de un Registro de actividades de tratamiento.

Además, en lo referente a seguridad, en cuanto a las medidas de seguridad, el responsable y los encargados del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. En el caso de las Administraciones Locales, tanto el Esquema Nacional de Seguridad como el RGPD establecen la obligación de realizar análisis de riesgos, y en el caso del RGPD, para determinar el posible impacto de los tratamientos de datos sobre los derechos y libertades de las personas y las medidas de seguridad aplicable, las notificaciones de quiebras de seguridad que puedan afectar a los datos personales y las Evaluaciones de impacto en la protección de datos.

Por lo que, se requerirá mucho esfuerzo y mucha concienciación por parte de las administraciones locales, para la consecución de este Reglamento.

17. Definiciones

Tal y como señala el artículo 4 del RGPD:

Datos personales:

Toda información sobre una persona física identificada o identificable; se considerará persona física identificable toda persona cuya identidad pueda determinarse, mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona;

Tratamiento:

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

Elaboración de perfiles:

Cualquier tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, como pueda ser analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.

Seudonimización:

el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.

Fichero:

Conjunto de datos personales, estructurado o no, accesibles con arreglo a criterios determinados, ya sea centralizado, descentralizado o repartido de forma funcional o geográfica.

Responsable del tratamiento o responsable:

Toda persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento, es decir, quien decide que el tratamiento se lleve a cabo y la forma en que se desarrollará

Encargado del tratamiento o encargado:

Toda persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento

Destinatario:

La persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero.

No se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento

Tercero:

Toda persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

Violación de la seguridad de los datos personales:

Cualquier brecha de la 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

Datos genéticos:

Se trata de los datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona

Datos biométricos:

Se trata de los datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos

Datos relativos a la salud:

Se trata de los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud;

Representante:

Toda persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento

Autoridad de control:

La autoridad pública independiente establecida por un Estado miembro con arreglo a lo dispuesto en el artículo 51, en este caso, la Agencia española de Protección de Datos, en adelante, AGPD.

18. Anexos

Anexo A. Registro de actividades de tratamiento
Estará compuesto de dos partes:

a) Fichero identificación de tratamientos
b) Fichero por actividad pormenorizado

Fichero identificación de tratamientos

Identificación del tratamiento				Intervinientes	Fin del tratamiento	Transferencias Internaciones	Datos Sensibles	Legitimación del tratamiento
Nombre de la actividad	N° / REF	Fecha de creación	Fecha Actualización	Responsable de tratamiento	Fin Principal			

Fichero por actividad pormenorizado

FICHA DE REGISTRO							
DESCRIPCIÓN DEL TRATAMIENTO							
Nombre							
N° / REF							
Fecha de Creación							
Fecha de Actualización							
INTERVINIENTES							
Actores	Nombre	Dirección	CP	Población	País	e-mail	Teléfono
Responsable del tratamiento							
DPO							
FINES DEL TRATAMIENTO							
Fin Principal							
Otro fin							
SEGURIDAD SEGÚN EL ESQUEMA NACIONAL DE SEGURIDAD							
Medidas Técnicas							
Medidas organizativas							
CATEGORIAS DE DATOS PERSONALES							

	DESCRIPCION	PLAZO DE SUPRESIÓN

CATEGORIAS ESPECIALES DE DATOS	
DESCRIPCIÓN	**PLAZO PREVISTOS DE SUPRESIÓN**

INTERESADOS	
Categoría de los interesados	**Descripción**
Interesado	
Colectivo	

DESTINATARIOS		
Destinatarios	**Descripción**	**Tipos de destinatarios**

ENCARGADOS DE TRATAMIENTO		
Encargados	**Descripción**	**Enlace documento**

LEGITIMACION DEL TRATAMIENTO		
Consentimiento/Base legal	**Base jurídica del tratamiento**	**Enlace documento**

TRANSFERENCIAS DE DATOS				
SI/NO	**Destinatario**	**País**	**Tipo de garantías**	**Enlace documento**

Anexo B. ejemplo formulario - modelo de información por capas

MODELO DE INSTANCIA GENERAL

SR. ALCALDE-PRESIDENTE DEL AYUNTAMIENTO DE……
Don/Doña:……
mayor de edad, con domicilio, a efectos de notificación en calle……
número……..., localidad:……..
Provincia:……con email:……
provisto de Documento Nacional de Identidad número……..

Ante V.S. comparece y

Expone y solicita:
……
……
……
……
……
……
……
……
……
……
……..
……..
Teniendo esta por presentada y previos los trámites correspondientes, se conceda lo solicitado.

En ……, a …… de……de 20…

Firmado

"Antes de firmar la solicitud, debe leer la información básica sobre protección de datos que se presenta en al pie y mas ampliada en la cara posterior de este formulario"

INFORMACIÓN BASICA SOBRE PROTECCIÓN DE DATOS	
RESPONSABLE	
FINALIDAD	
LEGITIMACIÓN	
DESTINATARIOS	
DERECHOS	
INFORMACION ADICIONAL	

PAGINA POSTERIOR

INFORMACIÓN AMPLIADA SOBRE PROTECCION DE DATOS

RESPONSABLE	
IDENTIDAD	
DIRECCION POSTAL	
TELEFONO	
E-MAIL	
DELEGADO DE PROTECCIÓN DE DATOS	
CONTACTO	Nota: poner únicamente el e-mail del DPO

¿CON QUÉ FIN TRATAMOS SUS DATOS?
¿POR CUANTO TIEMPO LOS CONSERVAMOS?

¿CUAL ES LA LEGITIMACION PARA EL TRATAMIENTO DE DATOS?

¿A QUE DESTINATARIOS SE COMUNICARAN LOS DATOS?

¿CUÁLES SON SUS DERECHOS? / ¿CÓMO PUEDE EJERCERLOS?
· Cualquier persona tiene derecho a obtener confirmación sobre si estamos tratando datos personales que les conciernan, o no. · Las personas interesadas tienen derecho a si acceder a sus datos personales, así como a solicitar la rectificación de los datos inexactos o, en su caso, solicitar su supresión cuando, entre otros motivos, los datos ya no sean necesarios para los fines que fueron recogidos. · En determinadas circunstancias, los interesados podrán solicitar la limitación del tratamiento de sus datos, en cuyo caso únicamente los conservaremos para el ejercicio o la defensa de reclamaciones. · En determinadas circunstancias y por motivos relacionados con su situación particular, los interesados podrán oponerse al tratamiento de sus datos a través del formulario que se encuentra en su sede electrónica https://www.xxx.es/ o bien a través de escrito dirigido al Ayuntamiento de xxx, calle x, y.
VÍAS DE RECLAMACIÓN
Si considera que sus derechos no han sido atendidos adecuadamente, tiene derecho a presentar una reclamación ante la Autoridad de Control en materia de Protección de Datos competente, la Agencia Española de Protección de Datos, especialmente cuando no haya obtenido satisfacción en el ejercicio de sus derechos, a través del formulario que se encuentra en su sede electrónica https://sedeagpd.gob.es/sede-electronica-web/ o bien a través de escrito dirigido a la Agencia Española de Protección de Datos C/ Jorge Juan, 6, 28001-Madrid.

Anexo C. Procedimiento interno de notificación de violaciones de seguridad

Todos los empleados de esta corporación, ante la evidencia de una violación de seguridad en los datos tratados o una fuga de datos, deben comunicar de manera inmediata a su superior jerárquico, y este a su vez al Responsable de Informática de este Ayuntamiento los siguientes datos:

Fecha y hora	
Departamento	
Fichero afectado	
Tipo de violación: ☐ Lectura (solo ha habido lectura, ningún atacante tiene datos) ☐ Copia (los datos aun están en el sistema) ☐ Alteración (los datos aun existen pero ha habido alteración) ☐ Borrado (los datos no están en el sistema, pero el atacante tampoco) ☐ Eliminación(los datos no existen en el sistema, los tiene un atacante)	
Sujeto en la violación: *[escoge una o varias opciones]* ☐ Un Pc ☐ Un portátil/móvil ☐ Documento en papel ☐ Fichero/os o parte de un fichero ☐ Una copia de datos ☐ la red	
Descripción del suceso:	

19. Bibliografía

Agencia Catalana de Protección de Datos. 2018. Guía sobre la evaluación de impacto relativa a la protección de datos en el RGPD (2.0) [online] [consulta 22/05/18]
http://apdcat.gencat.cat/web/.content/03-documentacio/Reglament_general_de_proteccio_de_dades/documents/GUIA-EVALUACION-DE-IMPACTO-CAST-2.0.pdf
Agencia española de Protección de datos. 2018 Adaptación al RGPD - Administraciones Públicas (infografía) [online] [consulta 09/03/18]
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/infografias/Adaptacion_RGPD_AAPP.pdf
Agencia española de Protección de datos. 2018. Delegado de protección de datos en las Administraciones Públicas [online] [consulta 11/04/18]
http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Funciones_DPD_en_AAPP.pdf
Agencia española de Protección de datos. 2018 Directrices sobre los delegados de protección de datos [online] [consulta 16/04/18]
http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Traduc_oficial_ult_version/wp243rev01_es.pdf
Agencia española de Protección de datos. 2018 Esquema de certificación de delegados de protección de datos de la agencia española de protección de datos [online] [consulta 12/04/18]
https://www.agpd.es/portalwebAGPD/temas/certificacion/common/pdf/ESQUEMA_AEPD_DPD.pdf**El**
Agencia española de Protección de datos. 2018 Protección de datos en el mundo [online] [consulta 22/04/18]
http://www.agpd.es/portalwebAGPD/internacional/Proteccion_datos_mundo/index-ides-idphp.php
Agencia española de Protección de datos. 2018. Códigos de Conducta [online] [consulta 05/05/18]
https://www.agpd.es/portalwebAGPD/jornadas/8_sesion_anual/common/JPH__CODIGOS_CONDUCTA_-_CERTIFICACIONES_-_TRANSFERENCIAS_INTERNACIONALES_8SAA.pdf
Agencia española de Protección de datos. 2018. De la inscripción de ficheros al registro de actividades [online] [consulta 22/03/18]
http://www.agpd.es/blog/de-la-inscripcion-de-ficheros-al-registro-de-actividades-ides-idPhp.php
Agencia española de Protección de datos. 2018. Directrices sobre notificación de las violaciones de seguridad de los datos personales de acuerdo con el Reglamento 679/2016 (EN) [online] [consulta 10/05/18]
http://www.agpd.es/portalwebAGPD/canaldocumentacion/docu_grupo_trabajo/wp29/common/Versiones_ingles/20171013_wp250_enpdf.pdf
Agencia española de Protección de datos. 2018. Guía para el cumplimiento del deber de informar [online] [consulta 17/04/18]
https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf
Agencia española de Protección de datos. 2018. Guía Protección Datos Administración Local [online] [consulta 06/05/18]
http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_Proteccion_Datos_Administracion_Local.pdf
Agencia española de Protección de datos. 2018. Orientaciones y garantías en los procedimientos de anonimización de datos personales [online] [consulta 21/04/18]

https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2016/Orientaciones_y_garantias_Anonimizacion.pdf

Agencia española de Protección de datos. 2018. Elaborar el registro de actividades de tratamiento [online] [consulta 01/03/18]

http://www.agpd.es/blog/elaborar-el-registro-de-actividades-de-tratamiento-ides-idPhp.php

Agencia española de Protección de datos. El enfoque de riesgos en el Reglamento de Protección de Datos [online] [consulta 27/05/18]

https://www.agpd.es/blog/el-enfoque-de-riesgos-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php

Agencia española de Protección de datos. Guía práctica de Análisis de riesgos [online] [consulta 25/05/18]

www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/AnalisisDeRiesgosRGPD.pdf

Agencia española de Protección de datos.2018. Guía práctica de Evaluaciones de impacto [online] [consulta 24/05/18]

www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

Agencia española de Protección de datos. Importancia de la información por capas en el Reglamento General de Protección de Datos [online] [consulta 12/04/18]

http://www.agpd.es/blog/la-importancia-de-la-informacion-por-capas-en-el-reglamento-general-de-proteccion-de-datos-ides-idPhp.php

Agencia española de Protección de datos. Modelo de cláusulas para contratos de encargados de tratamiento [online] [consulta 15/05/18]

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/Clausulas_contratos_encargado_tratamiento.pdf

Agencia española de Protección de datos.2018 Delegado de Protección de Datos [online] [consulta 04/04/18]

https://www.agpd.es/portalwebAGPD/temas/certificacion/index-ides-idphp.php

Agencia francesa de Protección de Datos. 2018. Le registre du responsable de traitement [online] [consulta 03/03/18]

https://www.cnil.fr/fr/RGDP-le-registre-des-activites-de-traitement

Agencia vasca de Protección de Datos. Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del Reglamento (UE) 2016/679 (WP248rev01) ***(Adoptadas el 4 de abril de 2017. Revisadas por última vez y adoptadas el 4 de octubre de 2017)*** **[online] [consulta 22/05/18]**

http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/wp248%20rev.01_es.pdf

Boletín Oficial del Estado. 2016. Reglamento General de Protección de Datos. 2016 [online] [consultado el 01/05/18]

https://www.boe.es/doue/2016/119/L00001-00088.pdf

Boletín Oficial del Estado. Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica [online] [consulta 01/05/18]

https://www.boe.es/diario_boe/txt.php?id=BOE-A-2010-1330

Centro Criptológico Nacional. Acceso Electrónico de los Ciudadanos a los Servicios Públicos [online] [29/04/18]

https://www.ccn-

cert.cni.es/publico/ens/Acceso_Electronico_de_los_ciudadanos_a_los_servicios_publicos.pdf
Centro Criptológico Nacional. Ear/Pilar [online] [consulta 21/05/18]
https://www.ccn-cert.cni.es/herramientas-ciberseguridad/ear-pilar.html
Centro Criptológico Nacional. ENS [online] [consulta 17/05/18]
https://www.ccn-cert.cni.es/publico/ens/ens/index.html#!1001
Centro Criptológico Nacional. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método0 [online] [consulta 20/05/18]
https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html
Centro Criptológico Nacional. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro II - Catálogo de Elementos [online] [consulta 20/05/18]
https://www.ccn-cert.cni.es/documentos-publicos/1791-magerit-libro-ii-catalogo/file.html
Centro Criptológico Nacional. MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro III - Guía de Técnicas [online] [consulta 21/05/18]
https://www.ccn-cert.cni.es/documentos-publicos/1793-magerit-libro-iii-tecnicas/file.html
Congreso de los Diputados. Proyecto de Ley Orgánica de Protección de Datos de Carácter Personal [online] [consulta 20/05/18]
http://www.congreso.es/public_oficiales/L12/CONG/BOCG/A/BOCG-12-A-13-1.PDF
Federación española de Municipios y Provincias. Pilar-Protección de datos [online] [consulta 01/05/18]
http://femp.femp.es/files/566-2239-archivo/herramienta%20pilar.pdf
Federación española de Municipios y Provincias .FEMP-ENS - Tomo 2 - Guía para entidades locales de menos de 2000 habitantes [online] [consulta 12/05/18]
https://www.ccn-cert.cni.es/documentos-publicos/ens/2452-femp-ens-tomo-2-guia-para-entidades-locales-de-menos-de-2000-habitantes.html
Federación española de Municipios y Provincias. FEMP-ENS - Tomo 1 - Guía estratégica en seguridad para entidades locales [online] [consulta 13/05/18]
https://www.ccn-cert.cni.es/documentos-publicos/ens/2449-femp-ens-tomo-1-guia-estrategica-en-seguridad-para-entidades-locales/file.html
Instituto Nacional de Administración Pública. 2018(videos). Adaptación al RGPD en las Administraciones Públicas. INAP – AEPD [online] [consulta 11/03/18]
https://www.inap.es/mediateca?p_p_id=contentviewerservice_WAR_alfresco_packportlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=columna-1&p_p_col_pos=1&p_p_col_count=2&_contentviewerservice_WAR_alfresco_packportlet_nodeName=JORNADA_PROTECCION_DATOS_04042018_2985487.gcl&_contentviewerservice_WAR_alfresco_packportlet_struts_action=/contentviewer/view&contentType=notice
Instituto Nacional de Administración Pública. 2018(video). Curso Proceso para la adaptación al RGPD en las Administraciones Pública [online][consulta 11/03/18]
https://www.inap.es/mediateca?p_p_id=contentviewerservice_WAR_alfresco_packportlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=columna-1&p_p_col_pos=1&p_p_col_count=2&_contentviewerservice_WAR_alfresco_packportlet_nodeName=Curso_proteccion_datos_2946347.gcl&_contentviewerservice_WAR_alfresco_packportlet_struts_action=/contentviewer/view&contentType=notice

Instituto Nacional de Administración Pública. 2017. El Reglamento General De Protección De Datos. (No Publicado) Módulo 1: Marco general para el tratamiento de datos personales [online] [consulta 02/03/18]

Instituto Nacional de Administración Pública. 2017. El Reglamento General De Protección De Datos. (No Publicado) Módulo 2.Los derechos de los ciudadanos en el RGPD cuando las Administraciones Públicas traten sus datos personales [online] [consulta 02/03/18]

Instituto Nacional de Administración Pública. 2017. El Reglamento General De Protección De Datos. (No Publicado) Módulo 3.Las Administraciones públicas como responsables en el RGPD. Relaciones con sus encargados de tratamientos [online] [consulta 02/03/18]

Instituto Nacional de Administración Pública. 2017. El Reglamento General De Protección De Datos. (No Publicado) Módulo 4. Otras medidas de responsabilidad activa: Delegado de Protección de Datos. Códigos Tipo. Certificaciones. Transferencias internacionales de datos [online] [consulta 03/03/18]

Instituto Nacional de Administración Pública. 2017. El Reglamento General De Protección De Datos. (No Publicado) Módulo 5.Las autoridades de supervisión. El Comité Europeo de Protección de Datos. El régimen sancionador en el RGPD [online] [consulta 11/04/18]

Instituto Nacional de Administración Pública. 2018(videos). Novedades en materia de protección de datos (vídeo) – AEPD – INAP [online][consulta 11/03/18]
https://www.inap.es/mediateca?p_p_id=contentviewerservice_WAR_alfresco_packportlet&p_p_lifecycle=0&p_p_state=maximized&p_p_mode=view&p_p_col_id=columna-1&p_p_col_pos=1&p_p_col_count=2&_contentviewerservice_WAR_alfresco_packportlet_struts_action=/contentviewer/view&_contentviewerservice_WAR_alfresco_packportlet_nodeName=JORNADA_NOVEDADES_PROTECCION_DATOS_2753529.gcl&contentType=notice

Ministerio de la Presidencia y para las administraciones territoriales. Anteproyecto de Ley Orgánica de Protección de Datos de Carácter Personal [online] [consulta 06/04/18]
http://servicios.mpr.es/seacyp/search_def_asp.aspx?crypt=xh%8A%8Aw%98%85d%A2%B0%8DNs%90%8C%8An%87%A2%7F%8B%99tt%84sm%A3%91