Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

GUÍA EN 8 PASOS 1

ADECUACIÓN DE LAS ADMINISTRACIONES PÚBLICAS AL

Reglamento General de **Protección de Datos**

El Reglamento General de Protección de Datos (en adelante, RGPD) **de la Unión Europea** entró en vigor en mayo de 2016, si bien será **aplicable a partir del 25 de mayo de 2018**, fecha en la que todos los responsables y encargados de tratamiento habrán de haberse adecuado a sus previsiones.

Las Administraciones Públicas (AAPP) actúan como responsables y encargados de tratamientos de datos personales en el desarrollo de muchas de sus actividades. En consecuencia, se verán afectadas por las consecuencias del nuevo RGPD, tanto en los principios y obligaciones generales como en aquellas previsiones específicas que el RGPD contempla para el sector público.

A modo de resumen, la adecuación de las AAPP al RGPD sintetizarse en los siguientes ***ocho pasos***.

8 PASOS

1 ▶ Designar un Delegado de Protección de Datos (DPD)

2 ▶ Establecer el Registro Interno de Tratamientos

3 ▶ Revisar la legitimación de los tratamientos

4 ▶ Revisar la información que se ofrece a los interesados

5 ▶ Revisar los procedimientos de ejercicio de derechos

6 ▶ Revisar los contratos con Encargados de Tratamiento

7 ▶ Efectuar Análisis de Riesgos y revisar las medidas de seguridad

8 ▶ Determinar la necesidad de efectuar Evaluaciones de Impacto

Datuak Babesteko
Euskal Bulegoa
Agencia Vasca de
Protección de Datos

Beato Tomás de Zumárraga,
71–3ª planta.
01008 Vitoria-Gasteiz

Tel: 945 016 230
E-mail: avpd@avpd.eus
web: http://www.avpd.eus

Horario de atención al público:
Octubre-Mayo:
9:00-13:00 ; 15:00-16:00
Viernes: 9:00-14:00
Horario de verano:
Junio-Septiembre:
9:00-14:00

Edita: © Agencia Vasca de Protección de Datos.
Impresión: Gráficas Dosbi, S.L. –D.L.: VI 140-2018

1 Designar el DPD

El **Delegado de Protección de Datos** (DPD) es una figura prevista en el RGPD, que no existía en nuestra LOPD, pero que ya había sido implantada por otros países miembros de la UE.

Sus **funciones** principales son:

a) Informar y asesorar al responsable o al encargado del tratamiento.

b) Supervisar el cumplimiento del RGPD por el responsable o encargado, incluyendo:
- La asignación de responsabilidades
- La concienciación y formación del personal
- Las auditorías correspondientes

c) Asesorar acerca de las Evaluaciones de Impacto (EIPD) y supervisar su aplicación.

d) Cooperar y actuar como punto de contacto con la autoridad de control.

El RGPD prevé que todas las «*autoridades u organismos públicos*» habrán de designar un **Delegado de Protección de Datos**.

▶ También establece cuáles habrán de ser los criterios para su designación (cualidades profesionales y conocimientos en derecho y práctica de la protección de datos), su posición en la organización y sus funciones.

▶ Prevé, igualmente, que en el caso de las autoridades u organismos públicos puedan nombrarse un único DPD para varios de ellos, teniendo en cuenta su tamaño y estructura organizativa.

La designación del DPD debe comunicarse a las autoridades de protección de datos.

▶ Asimismo, se debe facilitar que los interesados puedan contactar con el DPD.

Se sugiere que la primera medida a adoptar de cara a la adecuación de las AAPP al RGPD sea la de regular la figura del Delegado de Protección de Datos.

▶ Para ello se debe:

▶ Identificar las unidades en que se habrá de integrar el DPD dentro de cada órgano u organismo.

▶ Su posición en la estructura administrativa y los mecanismos para asegurar que los DPD designados reúnen los requisitos de cualificación y competencia establecidos por el RGPD.

▶ Su configuración para asegurar su criterio independiente y en ausencia de conflicto de intereses.

2 Establecer el Registro Interno de Tratamientos

La actual exigencia de creación de los ficheros y tratamientos mediante una **disposición** general, **publicada** en un Diario Oficial, y su notificación a la Autoridad de Protección de Datos para su inscripción en el Registro de Ficheros, **desaparece con el RGPD**.

En cambio, el RGPD establece la necesidad de la **llevanza de un registro interno de actividades de tratamiento**, como instrumento primordial para demostrar el cumplimiento y facilitar la supervisión de los tratamientos.

▶ Debe llevarse tanto por Responsables como por Encargados de tratamiento.

▶ El RGPD establece el contenido mínimo de ese registro.

Deberá mantenerse actualizado y a disposición de las autoridades de protección de datos.

▶ Como medida de transparencia, las AAPP harán público su inventario de actividades de tratamiento, accesible por medios electrónicos.

3 Revisar la legitimación de los tratamientos

Las AAPP deberán identificar con precisión **las finalidades y la base jurídica de los tratamientos** que llevan a cabo. Esta obligación deriva de:

- La necesidad de cumplir con el principio de legalidad establecido en el RGPD.
- La información a proporcionar a los interesados (transparencia).
- Su constancia en el registro de actividades de tratamiento.

La identificación de finalidades y base jurídica tiene exigencias adicionales en los casos en que se traten datos de los considerados como objeto de **especial protección**, que incluyen, entre otros, los datos sobre ***salud***, ***ideología***, ***religión*** **o** ***pertenencia étnica***.

El tratamiento de estos datos está, con carácter general, prohibido, y sólo podrá llevarse a cabo si es aplicable alguna de las excepciones previstas en el art. 9.2 del RGPD.

▶ En el caso de la actividad de las AAPP será muy habitual que la base jurídica de los tratamientos sea el cumplimiento de una **tarea en interés público** o el **ejercicio de poderes públicos**.

Tanto el interés público como los poderes públicos que justifican el tratamiento deben estar establecidos en una norma de rango legal.

▶ En el caso de de que el tratamiento esté basado en el consentimiento, habrá de tenerse en cuenta que se han reforzado los requisitos para obtenerlo («*informado*, *libre*, *específico y otorgado mediante una clara acción afirmativa*»), lo cual **invalida los consentimientos «*tácitos*»**, es decir, basados en una inacción u omisión de acción por parte del interesado.

Cuando las AAPP efectúen **transferencias de datos a terceros países**, el RGPD amplía los mecanismos ya existentes (decisiones de adecuación, garantías adecuadas y normas corporativas vinculantes) con algunas previsiones específicas sin necesidad de autorización previa, como son la existencia de instrumentos **jurídicamente vinculantes y exigibles entre autoridades y organismos públicos**. Sin embargo, los meros **acuerdos administrativos** requerirán **autorización** de las Autoridades de Control.

4 Revisar la información que se ofrece a los interesados

La información que se ofrece a los interesados cuando se recogen sus datos (por ejemplo, en formularios web o papel, o de un tercero) **debe revisarse,** pues se ha reforzado la transparencia hacia el interesado, siendo la información a facilitar más amplia que la requerida hasta ahora.

Para mayor información, se recomienda la consulta de la «***Guía para el cumplimiento del deber de informar***» elaborada por las tres Autoridades de Protección de Datos (AEPD, APDCAT y AVPD), disponible para su descarga en la URL:

http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/modeloclausulainformativa-es.pdf

5 Revisar los procedimientos de ejercicio de derechos

El RGPD mantiene y amplía los tradicionales derechos de «*acceso, rectificación, cancelación y oposición*», debiendo los responsables y encargados de tratamientos tener en cuenta lo siguiente:

Se sugiere incorporar la supervisión del DPD cuando se vaya a resolver negativamente.

- establecer mecanismos ***visibles***, ***accesibles*** y ***sencillos***, incluidos los medios electrónicos, para el ejercicio de derechos.
- establecer procedimientos que permitan responder a los interesados **en los plazos previstos** por el RGPD.

6 Revisar los contratos con Encargados de Tratamiento

El RGPD también ha reforzado los requisitos respecto de la contratación de servicios con los encargados de tratamiento, como son:

- El RGPD establece que la relación entre responsables y encargados deberá formalizarse siempre mediante un ***contrato o un acto jurídico*** que vincule al encargado y, además:
- Establece una obligación de ***diligencia debida*** en la elección de los encargados de tratamiento por parte de los responsables, contratando únicamente encargados que estén en condiciones de cumplir con el RGPD.

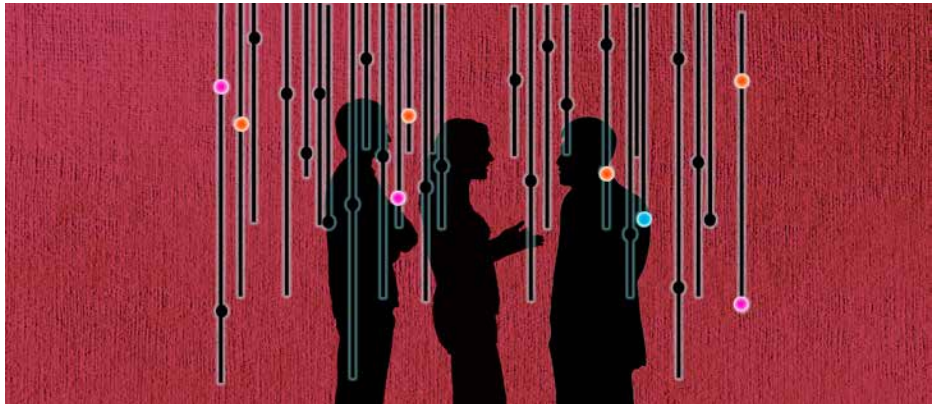
En el caso de las AAPP será frecuente que el encargo de tratamiento se establezca mediante ***actos jurídicos***, por ejemplo en la norma de creación de órganos encargados de la prestación de servicios informáticos.

Será necesario revisar y adecuar los contratos de encargo actualmente suscritos para contemplar el contenido mínimo que exige el RGPD.

Para mayor información, se recomienda la consulta de la guía «***Guía para el cumplimiento del deber de informar***» elaborada por las tres Autoridades de Protección de Datos (AEPD, APDCAT y AVPD), disponible para su descarga en la URL:

http://www.avpd.euskadi.eus/contenidos/informacion/20161118/es_def/adjuntos/directricescontratos-es.pdf

7 Efectuar Análisis de Riesgos y revisar las medidas de seguridad



Hasta ahora, las medidas de seguridad exigibles venían claramente enumeradas en el Reglamento de Desarrollo de la LOPD (RD-1720-2007), estableciéndose tres niveles de exigencia (*Básico, Medio y Alto*).

Sin embargo, el RGPD no establece cuáles han de ser las medidas de seguridad, sino que indica que:

> «*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, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo*».

Lo anterior significa que es necesario efectuar un ***análisis de riesgo*** para los derechos y libertades de los ciudadanos de los tratamientos de datos que se lleven a cabo, revisando las ***medidas de seguridad*** que actualmente se estén aplicando y, en su caso, completándolas a la luz de sus resultados.

▶ En el ámbito de las AAPP, las medidas de seguridad exigibles son las derivadas de la aplicación del Esquema Nacional de Seguridad, aprobado por Real Decreto 3/2010, de 8 de enero.

▶ La metodología para Análisis de Riesgos es "MAGERIT", publicada por el CCN-CERT.

▶ Adicionalmente, el RGPD introduce la necesidad de gestionar las violaciones de seguridad de los datos, notificando a la Autoridad de Control cuando tal violación constituya un riesgo para los derechos y libertades de los afectados.

8 Determinar la necesidad de efectuar Evaluaciones de Impacto

Finalmente, el RGPD también prevé la necesidad de efectuar una ***Evaluación de Impacto sobre la Protección de Datos*** (EIPD) con anterioridad a su puesta en marcha de nuevos tratamientos, siempre que puedan suponer un ***alto riesgo*** para los derechos y libertades de los interesados.

El RGPD determina algunos de los casos en que se presumirá que existe ese alto riesgo y prevé que las autoridades nacionales de protección de datos publiquen listas de otros tratamientos de alto riesgo.

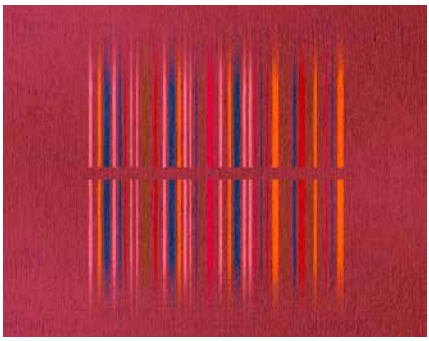
Las evaluaciones de Impacto sobre la privacidad consisten en:

a) una descripción sistemática de:
   - las operaciones de tratamiento previstas
   - los fines del tratamiento
   - cuando proceda, el interés legítimo perseguido por el responsable del tratamiento

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

c) una evaluación de los riesgos para los derechos y libertades de los interesados

d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales.



La metodología necesaria para llevar a cabo tales evaluaciones de impacto requiere una cierta especialización. La AEPD está trabajando actualmente en una guía que ayude a la realización de dichas Evaluaciones de Impacto. Mientras tanto, existe una «***Guía para una Evaluación de Impacto en la Protección de Datos Personales***», editada en 2014, disponible en la URL:

http://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf

El RGPD también prevé que se puedan efectuar ***EIPDs para proyectos de medidas legislativas***, o su desarrollo, que se refieran a tratamientos de datos. En tales casos, los tratamientos particulares derivados de tales medidas legislativas, que se legitimen en base a la consecución de fines de interés público, o vinculados al ***ejercicio de poderes*** públicos, no necesitarán llevar a cabo una nueva evaluación de impacto.