# ADECUACIÓN DE PYMES Y PROFESIONALES AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS EN OCHO PASOS

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 pequeñas y medianas empresas, los profesionales y autónomos actúan como ***responsables y encargados de tratamiento*** de datos personales en el desarrollo de muchas de sus actividades. Consecuentemente, se van a ver afectadas por las previsiones del nuevo RGPD.

*Si bien la Agencia Vasca de Protección de Datos (AVPD)* ***actúa como "Autoridad de Control" únicamente respecto de los responsables de tratamientos del ámbito público vasco*** *(y sus encargados de tratamiento), se ofrecen estas directrices para responsables y encargados de tratamientos del sector privado con ánimo colaborador y siempre remitiendo al criterio de la Agencia Española de Protección de Datos (AEPD), que es la* ***Autoridad de Control competente*** para éstos. Para más información pueden dirigirse a la página web de la AEPD:

**http://www.agpd.es/**

y consultar allí tanto la información disponible en el "canal del responsable" como las diferentes guías y publicaciones disponibles. En particular, se recomienda la consulta de la "***Guía del Reglamento General de Protección de Datos para responsables de tratamiento***" elaborada por las tres Autoridades de Protección de Datos (AEPD, APDCAT y AVPD), disponible para su descarga en la URL:

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

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

así como la utilización de la herramienta "***Facilita_RGPD***" que la AEPD ha puesto a disposición en la URL:

**http://www.servicios.agpd.es/Facilita**

En resumen, el impacto del RGPD sobre pequeñas y medianas empresas y profesionales y autónomos puede resumirse en los siguientes ***ocho puntos***:

## 1 Determinar la necesidad de disponer de Delegado de Protección de Datos (DPD)

El RGPD prevé que, en determinados casos, deba existir una figura que es el ***Delegado de Protección de Datos*** (DPD). Sin embargo, no todas las empresas están obligadas a disponer del DPD, sino solamente aquellas cuyas actividades principales consistan en:

- operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una "*observación* ***habitual y sistemática*** *de interesados a* ***gran escala***", o
- tratamiento a ***gran escala*** de ***categorías especiales de datos*** personales, como son:
  - datos de origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas, o afiliación sindical
  - datos genéticos, biométricos, de salud o relativos a la vida u orientación sexual

Así como en los tratamientos llevados a cabo por autoridades y organismos públicos y en tratamientos relativos a condenas e infracciones penales.

En todos estos casos, los responsables o encargados de tratamiento afectados deberán designar un Delegado de Protección de Datos y notificarlo a la Autoridad de Control correspondiente, con la posición y las funciones que se indican en el RGPD.

***Si ninguno de los anteriores es su caso, no necesita designar Delegado de Protección de Datos.***

Para mayor información, puede consultar la información disponible en la página web de la aepd, en la URL:

**http://www.agpd.es/blog/que-es-un-delegado-de-proteccion-de-datos-ides-idPhp.php**

## 2 Mantener un Registro Interno de Actividades de Tratamiento

Una de las novedades destacables que, en la práctica, ha introducido el RGPD es la ***desaparición de la obligación de registrar los ficheros o tratamientos*** en las Autoridades de Control.

Sin embargo, establece la necesidad de llevar un ***Registro interno de Actividades de Tratamiento***, para todas las empresas que cumplan con ***alguno*** de los siguientes criterios:

- Que empleen a ***más de 250*** personas
- Que realicen tratamientos de forma ***no ocasional***
- Que realicen tratamientos ***que puedan entrañar riesgos*** para las los derechos y libertades de las personas
- Que realicen tratamientos de las ***categorías especiales de datos*** personales indicadas anteriormente

En resumen, en la práctica todos los responsables y encargados de tratamientos que realicen tratamientos de forma no ocasional (es decir, ***habitual o sistemáticamente***) debieran llevar, con carácter interno, dicho inventario o registro de tratamientos.

El RGPD establece un contenido mínimo de ese registro, tanto para responsables como para encargados de tratamiento. El registro podrá organizarse sobre la base de las informaciones ya proporcionadas en las notificaciones de los ficheros existentes. En este sentido, la AEPD ha anunciado una nueva funcionalidad que permitirá a los responsables de tratamientos descargarse desde su "Sede Electrónica" una copia de la actual inscripción de ficheros, en la URL:

**https://sedeagpd.gob.es/sede-electronica-web/vistas/formCopiaContenido/copiaContenido.jsf**

## 3 Revisar la legitimación de los tratamientos

El RGPD requiere identificar claramente cuáles son la finalidad y la base jurídica de los tratamientos que se llevan a cabo. En el caso de los responsables de tratamientos de naturaleza jurídica privada, la base jurídica suele ser alguna de las siguientes:

- ***Consentimiento*** del interesado
- Existencia de un ***contrato***, o precontrato, con el interesado
- Existencia de una ***obligación legal*** aplicable al responsable

(hay ***otros supuestos*** de legitimación que pueden consultarse en el artículo 6 del RGPD)

En el caso 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.

## 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 las URL:

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

**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:

- 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 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.
- 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 "***Directrices para la elaboración de contratos entre responsables y encargados del tratamiento***" elaborada por las tres Autoridades de Protección de Datos (AEPD, APDCAT y AVPD), disponible para su descarga en las URL:

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

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

## 7 Revisar las medidas de seguridad, incorporando un Análisis de Riesgos

Hasta ahora, las medidas de seguridad exigibles venían claramente enumeradas en el Reglamento de Desarrollo de la LOPD (RD-1720-2007), donde se establecían tres niveles de cumplimiento (*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."*

Es decir es necesario efectuar un ***análisis de riesgo*** para los derechos y libertades de los ciudadanos de todos 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 los resultados del análisis de riesgo.

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.

Existen diferentes metodologías para la realización de análisis de riesgos. Para una información general sobre el tema, se recomienda la consulta de la guía elaborada por el INCIBE (Instituto Nacional de Ciberseguridad) "***Gestión de riesgos. Una guía de aproximación para el empresario***", disponible para su descarga en la URL:

**https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf**

## 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*** 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.

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**