APDTIC
Profesionales del derecho TIC

Impacto del RGPD en las Administraciones Públicas

¿Qué es el RGPD?

El Reglamento General de Protección de Datos (RGPD) es un reglamento europeo que tendrá efecto **a partir del 25 de mayo de 2018**, reemplazando la antigua normativa sobre protección de datos, e imponiendo unas normas que tienen entre sus objetivos fortalecer la privacidad de los ciudadanos y concienciar a las autoridades y organismos públicos que almacenan y tratan sus datos.

¿Cómo afecta esto a las Administraciones Públicas?

Las Administraciones Públicas **son los organismos responsables de los datos de los ciudadanos**, los cuales son utilizados para las múltiples actividades que son desarrolladas en el ámbito de sus funciones particulares (salud, educación, empleo, hacienda, y un largo etc).

Debido a la gran cantidad de información que almacenan las Administraciones Públicas, el RGPD ha puesto **especial foco en el sector público**, consciente de la necesidad de garantizar una protección de datos adecuada para todos los ciudadanos europeos.

El cambio de perspectiva que introduce el RGPD ha llevado a que la autoridad responsable en España, la Agencia Española de Protección de Datos (AEPD), esté fomentando el conocimiento de las implicaciones prácticas del RGPD, pues es imprescindible que los funcionarios sean conocedores de las obligaciones que esta normativa trae consigo.

¿Qué tienen que hacer las Administraciones Públicas para estar preparadas?

Aunque en algunos casos las Administraciones Públicas tendrán que cumplir las mismas exigencias que cualquier otro Responsable en el sector privado, existen algunas áreas donde el sector público deberá tener en cuenta ciertas particularidades

Aspectos más relevantes que afectan a las Administraciones Públicas

- La necesidad de **identificar con precisión las finalidades y la base jurídica de los tratamientos que realizan**(con exigencias adicionales en el caso de los datos especialmente protegidos)
- Ofrecer a los ciudadanos una **información más amplia** de la que actualmente se ofrece y hacerlo de forma concisa, transparente y con un lenguaje claro
- Recabar el **consentimiento** del ciudadano mediante una manifestación que muestre su voluntad o mediante una clara acción afirmativa
- Establecer **mecanismos visibles, accesibles y sencillos** para que los ciudadanos **puedan ejercer sus derechos** (incluidos los medios electrónicos)
- **Realizar análisis de riesgos** de todos los tratamientos de datos que lleven a cabo y revisar las medidas de Seguridad establecidas;
- Establecer un **registro de actividades**
- Designar a un **Delegado de Protección de Datos**

Obligación de designar un Delegado de Protección de Datos (DPO)

El RGPD impone como obligación que todas las Administraciones Públicas que asuma tratamientos de datos en calidad de Responsable o de Encargado del tratamiento, deberá designar a un DPO.

- Criterios para su designación (cualidades profesionales, conocimientos en derechos y práctica en materia de protección de datos) teniendo en cuenta las funciones que asume la organización pública
- En algunos casos, podrá nombrarse un único DPO para varias Administraciones Públicas, dependiendo de su tamaño y estructura organizativa
- Podrá ser **interno o subcontratado a una entidad privada**
- Se deberá establecer previamente los mecanismos para asegurar que los DPO designados reúnen los requisitos de cualificación y competencia requeridos.
- Su designación debe comunicarse a las autoridades de protección de datos.
- Se deberán establecer mecanismos para que los ciudadanos se puedan poner en contacto directamente con el DPO.

APDTIC
Profesionales del derecho TIC

Principales puntos que las Administraciones Públicas necesitan tener en cuenta con el RGPD

Informar correctamente a los ciudadanos

Las Administraciones Públicas deberán actualizar sus cláusulas informativas en todos sus procesos donde recojan datos personales como pueden ser las convocatorias de subvenciones o de pruebas selectivas, adaptándolas a las exigencias del RGPD.

Crear un registro de actividades de tratamiento

En sustitución de la obligación de inscripción de ficheros en la AEPD, las Administraciones Públicas deberán tener localizado internamente los tratamientos de datos que realiza, con la información que exige el RGPD, manteniéndolo actualizado y a disposición de la autoridad de protección de datos.

Verificar y adaptar los contratos con entidades externas

Las Administraciones Públicas tendrán que aplicar la obligación de diligencia debida en la elección de sus proveedores que asuman el papel de encargados de tratamiento, pues deben ofrecer garantías de que cumplen el RGPD y sus obligaciones deberán concretarse a través de actos jurídicos y contratos de encargo.

Análisis de riesgos y medidas de seguridad adecuadas

Las Administraciones Públicas deberán ampliar sus metodologías de análisis de riesgos (sobre todo orientadas a la seguridad de la información a través de las ISO) incluyendo los riesgos asociados al incumpliendo del RGPD. En función del análisis de riesgo específico sobre cada tratamiento, se deben estipular las medidas de seguridad adecuadas (siguiendo, a su vez, los criterios que marca el Esquema Nacional de Seguridad).

Mecanismos para identificar con rapidez las violaciones de seguridad de los datos

Es necesario que las Administraciones Públicas establezcan el mecanismo adecuado para localizar rápidamente cuando se produce una incidencia y en caso de ser necesario, notificarle a la AEPD.

Datos especialmente sensibles

Se deberá tener en cuenta que el tratamiento de estos datos sobre salud, ideología, religión o pertenencia étnica sean necesarios para satisfacer un interés público esencial, para fines de prevención, asistencia sanitaria, o para la gestión de los servicios de asistencia social.

Ajustar los instrumentos que se aplican cuando se realizan transferencias internacionales de datos de los ciudadanos

Habrá que actualizar los instrumentos al RGPD, donde se extienden las garantías para no requerir previamente la autorización de la autoridad de protección de datos.

Funciones de un DPO

Informar y asesorar a las Administraciones Públicas en cuestión y a los empleados públicos sobre el tratamiento de los datos y las obligaciones que establece el RGPD, asumiendo a su vez tareas como determinar si es necesario realizar una evaluación de impacto sobre un tratamiento que pueda suponer un alto riesgo; o como la de implantar programas de formación y sensibilización del personal.

La AEPD recuerda que estas modificaciones deberán estar listas para aplicarse, a más tardar, el 25 de mayo de 2018.

APDTIC
Profesionales del derecho TIC

Si desea obtener más información acerca de cómo podemos ayudarle, contacte con nuestro equipo de consultoría legal a través del mail: info@apdtic.com