



Reglamento General de Protección de Datos

¿Listos para la acción?





Contexto

El 25 de mayo de 2018, fecha de aplicación del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (en adelante RGPD), está a la vuelta de la esquina. Desde KPMG queremos hacer una recopilación de los principales puntos en los que centrar los esfuerzos para este cumplimiento, destacando las principales áreas en las que podemos aportar nuestro valor añadido y calidad.

Durante este último periodo, tanto a nivel local como internacional, hemos venido colaborando mediante nuestro equipo de expertos, con múltiples empresas de diferentes sectores en el soporte en la evaluación y asesoría en la adecuación a esta regulación.

Desde nuestra experiencia, entendemos que el trabajo en estos próximos meses se antoja crucial para poder garantizar un cumplimiento adecuado con el RGPD.



¿En qué te puede ayudar KPMG?

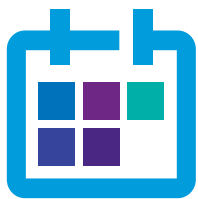
- Registro de las actividades de tratamiento.
- Análisis de riesgos que estas actividades de estos tratamientos pueden generar para los interesados.
- Ejecutar las evaluaciones de impacto en la protección de datos personales.
- Ofrecer soporte en la generación de procedimientos específicos.
- Modelo de gobierno de la privacidad, así como en la definición del rol del Delegado de Protección de Datos.
- Cumplimiento de requerimientos de seguridad de proveedores.
- Clasificación de la información y retención de la misma.
- Formación y concienciación.
- Framework de controles basados en estándares internacionales de seguridad y privacidad.
- Modelo de flujo de reporte de brechas de seguridad.
- Ciclo de monitorización continua de las medidas de seguridad.



¿En qué te puede ayudar KPMG? (cont.)

KPMG pone a su disposición un equipo compuesto por especialistas expertos en la asesoría y adecuación al Reglamento General de Protección de Datos para ayudarle a cumplir con todos los aspectos de aplicación. Especialmente, podemos trabajar en:

- Dar soporte en el **registro de las actividades de tratamiento** de datos de carácter personal en su compañía, generando un inventario único y de acuerdo a las especificaciones del Art.30 del RGPD.
- Realizar el **análisis de riesgos que estas actividades de estos tratamientos pueden generar para los interesados**. Con una metodología propia y ágil, basada en las recomendaciones del regulador, asesoramos a las compañías en la realización de este ejercicio de responsabilidad sobre dichos tratamientos.
- **Ejecutar las evaluaciones de impacto en la protección de datos personales**. Punto clave del cumplimiento y paso obligatorio para poder definir las medidas de seguridad concretas que la compañía debe establecer para mitigar los riesgos y garantizar un correcto cumplimiento y una adecuada protección de los datos personales. Para ello hemos desarrollado una metodología sencilla y acorde a las exigencias que ayuda a articular dichos análisis tanto en los tratamientos como en los sistemas y aplicaciones que sustentan los mismos.
- **Ofrecer soporte en la generación de procedimientos específicos**. El RGPD establece la necesidad de definir e implementar una serie de procedimientos específicos en la compañía orientados a garantizar aspectos como: La privacidad desde el diseño, la minimización del uso de datos de carácter personal, la articulación del derecho de Portabilidad, así como a identificar y notificar, en caso de que fuese necesario las **brechas de seguridad** que se pudieran producir sobre dichos datos.
- Asesorar en el **modelo de gobierno de la privacidad**, así como en la **definición del rol del Delegado de Protección de Datos**. El gobierno interno de la privacidad es un punto capital del cumplimiento del RGPD, esta responsabilidad proactiva tiene en la figura del Delegado de Protección de Datos a su principal adalid, pero debe ser vertebrada mediante una estructura adecuada de roles y responsabilidades, así como de unos mecanismos de reporting específicos y alineados con la estructura y cultura de la compañía.
- Revisar el **cumplimiento de requerimientos de seguridad de proveedores** a través de un modelo de gobierno de la seguridad, tanto a nivel de cumplimiento tecnológico, como del cumplimiento contractual. De esta forma se tendrán controlados a todos los encargados del tratamiento que disponga la compañía.
- Soporte al proceso de **clasificación de la información y retención de la misma**, cumpliendo de esta forma con el principio de conservación de los datos.
- Realizar un servicio de **formación y concienciación** tanto de privacidad como de seguridad que permita la prevención y alerta ante las amenazas de ciberseguridad.
- Proponiendo, de manera personalizada para nuestros clientes, un **framework de controles**, basado en los estándares internacionales de seguridad y de privacidad.
- Revisión de las posibles medidas técnicas y organizativas definidas por la compañía y propuesta de posibles mejoras (ciclo de **monitorización** continua)".



A partir del 25 de Mayo, ¿En qué debemos centrar los esfuerzos?

La fecha de cumplimiento no supone más que un punto y seguido, a partir del cual las compañías deben continuar su proceso de adaptación y cumplimiento, demostrando la debida diligencia y responsabilidad proactiva que exige esta normativa, para ello, y basándonos en la experiencia adquirida en los últimos meses en las colaboraciones que prestamos a nuestros principales clientes, nuestra oferta de servicios se orienta a:

- **Soporte experto del Delegado de Protección de Datos (en adelante DPD):**

- **de manera externa:**

- Resolviendo las consultas que tenga el DPD en el ejercicio de sus funciones.
 - Asistiendo en la metodología para la evaluación del impacto relativo a la protección de datos (Privacy Impact Assessments).
 - Elaborando una propuesta de actuaciones conforme al RGPD para tratar las incidencias que se detecten.
 - Apoyando en la formación y concienciación de su personal y le manteniéndoles informados de todas las novedades legales que les afecten.

- **de manera interna:** dotando a su Delegado de Protección de Datos de los perfiles expertos que pudiera necesitar para desplegar y operar la Oficina del Delegado de Protección de Datos.

- Asesoramiento en el **despliegue de las medidas organizativas y técnicas** necesarias para minimizar el riesgo de privacidad

- **KPMG como garante del cumplimiento.** Al

estar basado en un enfoque de gestión del riesgo, el cumplimiento del RGPD debe demostrarse mediante la proactividad de la compañía en garantizar dicho cumplimiento, para ello desde KPMG, y en base a nuestra experiencia, ofrecemos los servicios de tercera parte independiente a la hora de emitir un informe sobre las acciones llevadas a cabo por la compañía respecto a la adecuación, proponiendo como buena práctica la revisión de este proceso de manera anual.





Obligaciones del Delegado de Protección de Datos

- **Informar** a los responsables, a los encargados del tratamiento y a sus empleados, de las obligaciones contempladas en la legislación española y europea.
- **Supervisar** el cumplimiento de las obligaciones en materia de protección de datos y la política de protección de datos, incluyendo la asignación de responsabilidades, auditorías de cumplimiento, concienciación y formación del personal.
- **Asesorar** al responsable del tratamiento de datos en la evaluación del impacto relativo a la protección de datos, examen necesario cuando el tratamiento entrañe un alto riesgo para los derechos y libertades de las personas físicas.
- **Cooperar** con la Agencia Española de Protección de Datos (en adelante, AEPD) y ser su punto de contacto para las cuestiones relativas al tratamiento, incluyendo la consulta previa a la AEPD cuando el tratamiento implique el riesgo anteriormente descrito.



Informar



Supervisar



Asesorar



Cooperar



Riesgos

- El incumplimiento de estas obligaciones supone un riesgo de sanción que puede ascender a la mayor de estas dos cifras veinte millones de euros o el 4% de su cifra de negocio.



Beneficios

- Cumplirá con la normativa de la manera más beneficiosa posible para su negocio, teniendo en cuenta sus características particulares.
- Su personal se verá liberado de la carga burocrática y administrativa que conlleva la adaptación a esta normativa, pudiendo seguir centrándose en el negocio.

Contactos



Marc Martínez
Socio, IT Advisory
KPMG España

T: +34 606 43 36 47
E: marcmartinez@kpmg.es



Javier Aznar
Senior Manager, IT Advisory
KPMG España

T: +34 699 35 00 29
E: jaznar@kpmg.es



Juan Ignacio Rios
Manager, IT Advisory
KPMG España

T: +34 683 66 38 39
E: juanignaciorios@kpmg.es



Lorena Jurado
Manager, IT Advisory
KPMG España

T: +34 620 19 03 35
E: ljurado@kpmg.es

kpmg.es



© 2018 KPMG Asesores S.L., sociedad española de responsabilidad limitada y firma miembro de la red KPMG de firmas independientes afiliadas a KPMG International Cooperative ("KPMG International"), sociedad suiza. Todos los derechos reservados.

KPMG y el logotipo de KPMG son marcas registradas de KPMG International Cooperative ("KPMG International"), sociedad suiza.

La información aquí contenida es de carácter general y no va dirigida a facilitar los datos o circunstancias concretas de personas o entidades. Si bien procuramos que la información que ofrecemos sea exacta y actual, no podemos garantizar que siga siéndolo en el futuro o en el momento en que se tenga acceso a la misma. Por tal motivo, cualquier iniciativa que pueda tomarse utilizando tal información como referencia, debe ir precedida de una exhaustiva verificación de su realidad y exactitud, así como del pertinente asesoramiento profesional.