El Reglamento (UE) 2016/679 (RGPD) ha comenzado a aplicarse el 25 de mayo de 2018. Las empresas deben adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que el Reglamento establece. Es lo que se conoce como Responsabilidad Activa. ¿Estás aplicando estas medidas?

¿Que supone para las empresas?

El Reglamento supone un mayor compromiso de las organizaciones, debiendo estas de gestionar la protección de datos de forma distinta de la que se viene empleando hasta ahora. Las empresas como responsables del tratamiento, aplicaran medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario. La implantación de medidas dependerá de factores tales como el tipo de tratamiento, los costes de implantación de las medidas o el riesgo que el tratamiento presenta para los derechos y libertades de los titulares de los datos.

Es necesario que todas las empresas al tratar datos personales realicen un análisis de riesgo de sus tratamientos para poder determinar qué medidas han de aplicar y cómo hacerlo. Entre las medidas podemos enumerar las siguientes; *elaboración de registro de actividades de tratamiento, implantación de procedimientos para el ejercicio de los derechos de los titulares de los datos, establecimiento de medidas de seguridad concretas, planificación de la privacidad desde el diseño y por defecto, elaboración de la evaluación de impacto sobre protección de datos en ciertos casos o la existencia de un delegado de protección de datos.*

¿Qué implica la responsabilidad activa recogida en el Reglamento?

El Reglamento se basa en la prevención por parte de las organizaciones que tratan datos, por lo que entiende que actuar sólo cuando ya se ha producido una infracción es insuficiente como estrategia, dado que esa infracción puede causar daños a los interesados que pueden ser muy difíciles de compensar o reparar.

El Reglamento establece que el responsable del tratamiento deberá garantizar el cumplimiento de los principios relativos al tratamiento, así como, la figura responsable de demostrarlo. Por tanto, es fundamental definir adecuadamente las actividades de tratamiento y documentar los análisis realizados, así como, dejar trazabilidad de los mismos y de las conclusiones que los soportan para poder garantizar la responsabilidad proactiva.

¿Que deben de hacer las organizaciones?

- Planificación del tratamiento de los datos para facilitar la correcta determinación del estado de los sistemas de privacidad y un óptimo grado de cumplimiento del RGPD, alineado todo ello con el cumplimientos de los objetivos de la organización
- Formación e Información a todo el personal de la organización que traten datos personales.
- Nombramiento del Delegado de Protección de Datos (DPD), si fuese necesario.
- Elaboración de un Registro Interno de Actividades de Tratamiento, si fuese necesario.
- Revisión de la legitimación de los tratamientos. (consentimiento, contrato, obligación legal,...).
- Revisión de la información que se ofrece a los interesados y de los procedimientos de ejercicio de derechos.
- Revisión de los contratos con Encargados de Tratamiento.
- Revisión de las Medidas de seguridad, incorporando un Análisis de Riesgos.
- Determinación de la necesidad de realizar Evaluaciones de Impacto (EIPD).

¿Qué ocurre si no cumples?

La Agencia Española de Protección de datos garantiza la imposición de multas administrativas con arreglo al Reglamento para que en cada caso sean efectivas, proporcionadas y disuasorias.

Importes de las sanciones:

- Infracciones relacionadas con obligaciones del responsable y del encargado del tratamiento. *Multas administrativas de **10.000.000 EUR** como máximo o, tratándose de una empresa, de una cuantía equivalente al 2 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.*

- Infracciones relacionadas con los principios básicos para el tratamiento, condiciones para el consentimiento, derechos de los interesados, transferencias de datos personales a un destinatario en un tercer país o una organización internacional. *Multas administrativas de **20.000.000 EUR** como máximo o, tratándose de una empresa, de una cuantía equivalente al 4 % como máximo del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la de mayor cuantía.*

Estas multas administrativas se impondrán, en función de las circunstancias de cada caso individual.

¿Qué ofrece GAMA Consultoría y Formación?

Ponemos a vuestra disposición un Consultor especializado en la materia, con Certificado AENOR para implantar el RGPD en las empresas, que hará un estudio pormenorizado de vuestras necesidades y con base en la información que nos facilitéis os elaboramos una oferta sin compromiso.