El nuevo Reglamento Europeo de Protección de Datos General Data Protection Regulation **(GDPR)** ya ha entrado en vigor.

El nuevo Reglamento Europeo de Protección de Datos (GDPR, en sus siglas en inglés),está en vigor desde el pasado 25 de mayo y será de aplicación obligatoria a partir del **25 de mayo de 2018.** La nueva normativa de la Unión Europea , pretende conseguir que todas las empresas y organizaciones que tratan datos de ciudadanos europeos, sean locales o internacionales, se atiendan a una única legislación en toda la UE, evitando así diferencias de criterios y regímenes sancionadores según el país en el que se realice el tratamiento.

¿Qué es el nuevo Reglamento Europeo de Protección de Datos?

El Reglamento General de Protección de Datos (Reglamento de la UE 2016/679) es el nuevo marco jurídico de la UE que rige el uso de los datos personales. Este texto deroga la actual Directiva 95/46/CE de protección de datos y sustituye a las leyes de protección de datos nacionales existente (En España, la Ley 15/1999 de Protección de Datos). El texto será aplicable en todos los estados de la Unión Europea de desde 25 de mayo de 2018.

Hasta entonces, las empresas pueden elegir si seguir con la normativa LOPD o adaptarse al GDPR la fecha límite es el 25 de mayo de 2018.

¿Qué quiere lograr esta nueva normativa de LOPD?

- Simplificar de las cargas administrativas de las empresas respecto a la transferencia internacional de datos.
- Proporcionar un marco legal único y claro en la UE a las empresas que procesan datos personales.
- Reforzar los derechos de los ciudadanos, para evitar los abusos por parte las empresas.
- Regular el acceso y uso de la información personal por que hacen las empresas.
- Aumento de las sanciones contra las empresas que incumplan la normativa.

¿Qué aspectos regula?

Ámbito territorial

Estarán sujetas al Reglamento las empresas establecidas fuera de la UE que realicen tratamientos de datos personales de ciudadanos residentes en la UE cuando les ofrezcan bienes o servicios, se pague o no por ello o controlen su comportamiento.

Consentimiento del interesado

El consentimiento para autorizar el tratamiento de datos debe ser libre, específico, informado, explícito e inequívoco. Será tan fácil retirar el consentimiento como darlo. El Responsable del tratamiento deberá poder demostrar que se ha obtenido el consentimiento del interesado.

No será necesario obtener el consentimiento cuando el tratamiento sea necesario para el cumplimiento de obligaciones legales a las que esté sujeto el Responsable.

Información al interesado

La información deberá estar unificada y facilitada por escrito o medios electrónicos pudiendo ser combinada con iconos formalizados. El deber de informar estará basado en la transparencia del tratamiento y en los derechos que asisten al interesado. Se añade la obligación de informar sobre el plazo de conservación de los datos y las posibles transferencias internacionales.

Derechos de los interesados

El derecho al olvido, como equilibrio entre el derecho a la información y el derecho a la supresión de los datos cuando ya no sean necesarios.

El derecho a la limitación del tratamiento, añadido a los existentes de oposición y supresión para restringir el tratamiento mientras sea necesario.

El derecho a la portabilidad de los datos de un Responsable del tratamiento a otro a petición del interesado.

El derecho a no ser objeto de una elaboración de perfiles basada únicamente en el tratamiento automatizado, cuando la decisión que pueda ser tomada a consecuencia de la misma pueda producir efectos jurídicos que puedan afectarle significativamente, y con derecho a reclamar al Responsable una intervención humana y a impugnar la decisión.

El derecho a reclamar ante la Autoridad de control.

Seudonimización

El Reglamento introduce el concepto de datos codificados para cuando los datos no puedan atribuirse a un interesado sin recurrir a información adicional, separada y sujeta a medidas de seguridad que garanticen el anonimato del mismo. Esta práctica pretende minimizar los riesgos del tratamiento.

Rendición de cuentas

Los Responsables del tratamiento deberán de ser capaces de demostrar el cumplimiento de todos los principios del tratamiento que impone el Reglamento: licitud, limitación de los fines, minimización de los datos, exactitud, limitación del plazo de conservación, efectividad, integridad y confidencialidad.

Medidas de seguridad

Implantar medidas, procedimientos y sistemas que garanticen la privacidad ajustados a las necesidades, tamaño, circunstancias, contexto y finalidades del tratamiento de datos. Ya no será necesario inventariar los equipos informáticos, el mobiliario y los soportes como precisaba el reglamento LOPD. Bastará con establecer una política de seguridad que garantice mediante unas prácticas de seguridad (identificación, autenticación, accesos, permisos, tratamiento, destrucción de documentos, copias de seguridad, etc.) que se correspondan adecuadamente a la protección de datos según los riesgos previstos. Existirán mecanismos de certificación homologados para demostrar que se cumple el Reglamento.

Protección de datos desde el diseño y por defecto

Las empresas deberán garantizar desde el diseño y por defecto la protección de datos en cualquier fase del tratamiento: obtención, acceso, intervención, transmisión, conservación y supresión. Deberán asegurar que el tratamiento se realice para fines específicos, aplicar técnicas de minimización de datos, posibilitar el ejercicio de los derechos de los interesados y que los datos no sean accesibles a un nº indeterminado de personas.

Evaluación de impacto

Las empresas deberán asumir la responsabilidad de evaluar el grado de riesgo que representa para las personas que sean objeto de tratamiento, debiendo realizar una evaluación de impacto cuando se prevea un alto riesgo para los derechos, libertades e intereses legítimos de las mismas. Cuando el tratamiento no presente riesgo, la carga para el cumplimiento se verá notablemente reducida. Las evaluaciones de impacto deberán tenerse en cuenta para nuevos procedimientos de tratamiento.

Registro de las actividades del tratamiento

Los Responsables y Encargados del tratamiento tendrán la obligación de llevar un registro de actividades cuando empleen a un mínimo de 250 personas, o el tratamiento pueda suponer un riesgo para los derechos y libertades del interesado, o se traten categorías especiales de datos o datos relativos a condenas y delitos penales. Este registro estará a disposición de la Autoridad de control.

Encargados del tratamiento

Los Encargados de tratamiento estarán sujetos a las mismas sanciones que los Responsables. Deberán suscribir un contrato de prestación de servicios por cuenta del Responsable siguiendo sus instrucciones, que deberán ser documentadas, incluyendo si fuera el caso las transferencias de datos a terceros países u organizaciones internacionales. Cuando el Encargado del tratamiento determine los fines y medios del tratamiento por su cuenta será considerado Responsable y estará sujeto a las normas aplicables como tal.

Corresponsables del tratamiento

Existe la nueva figura de Corresponsable del tratamiento para cuando entre varios Responsables o Encargados determinen los fines y los medios del tratamiento. En este caso se deberá formalizar un acuerdo donde se determine las funciones y responsabilidades de cada uno de ellos con respecto al tratamiento y a sus relaciones con los interesados. Con esta figura, muchos Encargados se van a convertir en Corresponsables del tratamiento.

Violación de datos

Se deberán notificar las incidencias a la Autoridad de control en 72 horas, documentando la naturaleza y el contexto de la violación y los posibles efectos de la misma. Podrá implicar el informar a las personas afectadas cuando sea probable que presente un alto riesgo para sus derechos y libertades o le sea exigido por la Autoridad de control.

Delegado de protección de datos

Nueva figura a cargo del Responsable encargada de informar y asesorar al Responsable o Encargado del tratamiento y al personal autorizado para tratar datos, de las obligaciones relativas a la protección de datos personales en tratamientos a gran escala o con un alto nivel de riesgo en protección de datos.

Sanciones

Las multas serán proporcionales a cada caso particular. Habrá un incremento de la cuantía sancionable que podrá llegar, en casos graves, al 4% de la facturación en todo el mundo.

¿Qué debemos hacer ahora para prepararnos para el GDPR

En la medida en que el nuevo Reglamento propone una nueva cultura de privacidad, es el momento de revisar los procedimientos que estamos usando actualmente:

- Si no cumplimos con la LOPD, **deberemos ponernos al día**, ya que la transición al GDPR será más fácil desde su cumplimiento. A partir de la entrada en vigor del nuevo Reglamento habrá 2 años para adaptarnos.

- **Regularizar las relaciones con los Encargados del tratamiento**: realizar un inventario de los mismos, revisar los contratos para establecer si existe corresponsabilidad y documentar las instrucciones del encargo para minimizar los riesgos.

- **Implementar medidas de seguridad desde el diseño y por defecto** en todos los procesos del tratamiento mediante procedimientos y sistemas que garanticen la protección de datos y el ejercicio de los derechos de los interesados.

- Realizar un **análisis de los riesgos que atañen al tratamiento y prevenir su impacto** para garantizar los derechos y las libertades de las personas que puedan ser afectadas, asumiendo que la protección de datos es mucho más que un cumplimiento formal y documental.

Barcelona, Septiembre 2016

APLISER

ASFCONSULTORES

Solicite más información de cómo adaptarse : info@apliser.com