09/05/2018

DEPARTAMENTO SECRETARÍA

Protección de datos. Novedades importantes: RGDP

En mayo de 2016 se publicó el nuevo Reglamento General de Protección de Datos en Europa (RGPD)- Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

A partir del 25 de mayo de 2018, el nuevo RGPD europeo se aplicará en España.

El Gobierno realizó un nuevo proyecto de Ley de Protección de datos que fue enviado a las Cortes Generales, pero éste aún no ha sido aprobado, por lo que será de aplicación directa desde el 25 de mayo de este año el RGDP tanto ante los tribunales como ante la Agencia de Protección de datos (APD).

Las empresas españolas están obligadas a cumplir el RGPD, por lo que, surgen dudas en todas las empresas respecto a cómo se deben tratar los datos personales de clientes, trabajadores y proveedores que intentaremos aclarar.

Previamente, hemos de informar que contamos con los conocimientos y las herramientas necesarias para la elaboración de su política de seguridad y protocolo de actuación , así como para el cumplimiento de la nueva obligación legal.

Es recomendable que todas las empresas empiecen a familiarizarse con los conceptos, las nuevas exigencias y procedimientos **para evitar sanciones**. Por eso, en esta CIRCULAR INFORMATIVA explicamos las novedades más relevantes que se deben conocer para cumplir con el nuevo RGDP.

DATOS

El presente Reglamento se aplica exclusivamente al tratamiento de **datos personales (personas físicas)** en el contexto de las actividades de un establecimiento. La decisión de cumplir la norma debe estar basada siempre en el respeto por los derechos de nuestros clientes, contactos, empleados y demás personas físicas.

Se considera DATO PERSONAL toda información sobre una persona física identificada o identificable. Se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.

Aparte de los datos especialmente protegidos que ya preveía la LOPD, el RGDP incluye dos nuevas categorías especiales de datos:

- Datos genéticos: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionan una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica.

- Datos biométricos: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de esta persona (imágenes faciales, datos dactiloscópicos, etc.).

TRATAMIENTOS DE DATOS

Es cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.

Con la antigua LOPD, los datos que deben ser facilitados al interesado son los siguientes (art. 5 LOPD):

- Finalidad, destinatarios ficheros, obligación o no de la entrega y sus consecuencias, los derechos del interesado, la identidad del responsable.

A los anteriores indicados, con el RGPD se suman los siguientes (art. 13 RGPD):

- La base jurídica del tratamiento, el tiempo máximo que se mantendrán los datos, la identificación, si procede, del Delegado de Protección de datos, si habrá o no trasferencia internacional de datos, el derecho a presentar una reclamación y la existencia o no de decisiones automatizadas.

- En relación con los derechos conocidos por el acrónimo ARCO (Acceso, Rectificación, Consulta, Oposición), el RGPD los cambia y actualiza. Los nuevos ARCO, sobre los que hay que informar, ahora son los derechos siguientes: acceso, rectificación, supresión, limitación, portabilidad, y oposición.

  Este tratamiento de datos debe constar en un registro de actividades de tratamiento.

El RGPD suprime, a partir del 25 de mayo de 2018, la necesidad de crear formalmente los ficheros, inscribirlos y notificarlos a la Agencia Española de Protección de Datos.

ENCARGADOS DEL TRATAMIENTO. ANÁLISIS DEL RIESGO

Responsable del tratamiento. Es la persona física o jurídica, autoridad pública, servicio u otro organismo que, sólo o junto con otros, determine los fines y medios del tratamiento.

La responsabilidad última sobre el tratamiento sigue estando atribuida al responsable, que es quien determina la existencia del tratamiento y su finalidad.

El responsable deberá adoptar las medidas apropiadas, incluida la elección de encargados, de forma que garantice y esté en condiciones de demostrar que el tratamiento se realiza conforme al RGPD.

El responsable es quien asegura el cumplimiento de la normativa por parte del encargado de tratar los datos personales. La relación entre responsable y encargado debe formalizarse en un contrato o acto jurídico.

El responsable debe mantener un registro de actividades de tratamiento, determinar las medidas de seguridad y designar un delegado de protección de datos, cuando sea necesario.

Encargado del tratamiento. Es la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.

El contrato tiene que constar por escrito y deberá detallar las instrucciones del responsable al encargado en relación con las medidas de seguridad, el régimen de subcontratación, la confidencialidad y el destino de los datos tras finalizar la prestación del servicio.

Delegado de Protección de Datos (DPD). Esta figura no es obligatoria para todas las organizaciones: solo tendrán que contar con un delegado las empresas públicas, las que tengan un tratamiento a gran escala o las que recojan datos especialmente sensibles o relativos a condenas o infracciones penales.

EVALUACIÓN DE IMPACTO

Los responsables deban realizar el correspondiente análisis de riesgo y cuando sea probable que un tratamiento, especialmente si se utilizan las nuevas tecnologías, por su naturaleza, alcance, contexto o finalidades, suponga un riesgo alto para los derechos y libertades de las personas físicas, el responsable debe hacer una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales antes de iniciar el tratamiento.

El RGPD contiene una lista indicativa de tres supuestos en que se considera que los tratamientos conllevan un alto riesgo:

- Elaboración de perfiles sobre cuya base se tomen decisiones que produzcan efectos jurídicos sobre los interesados o que les afecten significativamente de modo similar.
- Tratamiento a gran escala de datos sensibles.
- Observación sistemática a gran escala de una zona de acceso público.

La diferencia entre la evaluación de impacto y el análisis de riesgo es que la primera se centra en medir el riesgo para los derechos y libertades de las personas físicas, en relación con la protección de datos; mientras que la segunda analiza las vulnerabilidades informáticas y potenciales brechas de seguridad lógica con el fin de seleccionar e implementar las mejores soluciones informáticas para impedir, bloquear o neutralizar los ataques.

REGISTRO DE ACTIVIDADES DE TRATAMIENTO

Los responsables y encargados del tratamiento tienen que llevar un registro de las actividades de tratamiento que lleven a cabo y documentarlo. Este registro debe contener, respecto de cada actividad, la información que establece el artículo 30 del RGPD.

Las organizaciones de 250 trabajadores o más deberán mantener un registro de operaciones de tratamiento en el que se contenga la información que establece el RGPD y recoja cuestiones como: Nombre y datos de contacto del responsable o corresponsable y del delegado de protección de datos si existiese, finalidades del tratamiento, descripción de categorías de interesados y categorías de datos personales tratados, transferencias internacionales de datos.

La aplicación de las medidas previstas por el RGPD debe adaptarse, por tanto, a las características de las organizaciones. Lo que puede ser adecuado para una organización que maneja datos de millones de interesados en tratamientos complejos que involucran información personal sensible o volúmenes importantes de datos sobre cada afectado no es necesario para una pequeña empresa que lleva a cabo un volumen limitado de tratamientos de datos no sensibles.

OBTENCIÓN DE LOS DATOS. EL CONSENTIMIENTO

El RGPD requiere que el interesado preste el consentimiento mediante una declaración inequívoca o una acción afirmativa clara.

A efectos del nuevo Reglamento las casillas ya marcadas, el consentimiento tácito o la inacción no constituirán un consentimiento válido.

¿Qué sucede con aquellos tratamientos que se realizan con base en el consentimiento por omisión?

Respecto a la obtención del consentimiento por omisión, no es compatible con el RGPD, ya que se basa en la inacción del interesado. El RGPD señala también que los tratamientos iniciados con anterioridad al inicio de su aplicación sobre la base del consentimiento seguirán siendo legítimos siempre que ese consentimiento se hubiera prestado del modo en que prevé el propio RGPD, es decir, mediante una manifestación o acción afirmativa.

Por tanto, los responsables que realizan tratamientos basados en ese consentimiento por omisión deberían evitar seguir obteniendo esta modalidad

de consentimiento y revisar esos tratamientos de forma que a partir de mayo de 2018 se hayan adecuado a las previsiones del RGPD.

Esa adaptación puede llevarse a cabo obteniendo un consentimiento de los interesados acorde con las disposiciones del RGPD o valorando si los tratamientos afectados pueden apoyarse en otra base legal como puede ser, entre otras, el interés legítimo del responsable o del cesionario de los datos que prevalezca sobre los derechos del interesado. En todo caso, y si se considera que cabe esta segunda opción, los interesados deben ser informados y podrán ejercitar los derechos que, como el de oposición, sean específicamente aplicables a la nueva base legal elegida.

El RGPD contempla algunas situaciones en que el consentimiento ha de ser explícito. Esta garantía adicional afecta a: Tratamiento de categorías especiales de datos, Adopción de decisiones automatizadas, Transferencias internacionales y datos de menores

En el ámbito de los servicios de la sociedad de la información, el consentimiento de los menores sólo será válido si tienen más de 16 años.

DERECHO DE INFORMACIÓN

La información es un derecho de las personas afectadas y es que es necesario informarlas, con los aspectos siguientes: los datos de contacto del delegado de protección de datos; la base jurídica del tratamiento; los intereses legítimos perseguidos en que se fundamente el tratamiento, en su caso; la intención de transferir los datos a un tercer país o a una organización internacional y la base para hacerlo, en su caso; el plazo durante el cual se conservarán los datos; el derecho a solicitar la portabilidad; el derecho a retirar en cualquier momento el consentimiento que se haya prestado; si la comunicación de datos es un requisito legal o contractual o un requisito necesario para suscribir un contrato; el derecho a presentar una reclamación ante una autoridad de control; la existencia de decisiones automatizadas, incluida la lógica aplicada y sus consecuencias.

El RGPD prevé que la información a los interesados se proporcione de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

Estas exigencias implican que debería evitarse acudir a fórmulas especialmente farragosas y que incorporan remisiones a los textos legales. Sería necesario que las cláusulas informativas expliquen el contenido de una forma clara y accesible para los interesados, con independencia de sus conocimientos en la materia.

El RGPD prevé que la información a los interesados se facilite por escrito, incluidos, cuando sea apropiado, los medios electrónicos.

La limitación de tratamiento supone que, a petición del interesado, no se aplicarán a sus datos personales las operaciones de tratamiento que en cada caso corresponderían. La limitación puede solicitarse cuando:

- El interesado ha ejercido los derechos de rectificación u oposición y mientras el responsable determina si procede atender a la solicitud

- El tratamiento es ilícito, lo que determinaría el borrado de los datos, pero el interesado se opone a ello

- Los datos ya no son necesarios para el tratamiento, lo que nuevamente determinaría su borrado, pero el interesado solicita la limitación porque los necesita para la formulación, el ejercicio o la defensa de reclamaciones.

DERECHO AL OLVIDO

El nuevo GDPR establece que cualquier persona tendrá derecho a que su información personal sea eliminada de los proveedores de servicios de Internet cuando lo desee, siempre y cuando quien posea esos datos no tenga razones legítimas para retenerlos.

Además obliga a los responsables de los datos que han difundido la información a terceros a comunicarles la obligación de suprimir cualquier enlace a los datos publicados, así como a eliminar cualquier copia o réplica de dichos datos.

PROACTIVIDAD Y CONTINUIDAD

El principio de «responsabilidad proactiva» exige la necesidad de que el responsable del tratamiento aplique medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento.

En términos prácticos, este principio requiere que las organizaciones analicen qué datos tratan, con qué finalidades lo hacen y qué tipo de operaciones de tratamiento llevan a cabo. A partir de este conocimiento deben determinar de forma explícita la forma en que aplicarán las medidas que el RGPD prevé, asegurándose de que esas medidas son las adecuadas para cumplir con el mismo y de que pueden demostrarlo ante los interesados y ante las autoridades de supervisión.

En síntesis, este principio exige una actitud consciente, diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales que lleven a cabo.

Todas las empresas, sin excepción, deben analizar las **vulnerabilidades informáticas** y potenciales brechas de seguridad lógica con el fin de seleccionar e **implementar las mejores soluciones informáticas para impedir, bloquear o neutralizar los ataques**.

Este análisis, así como la selección de las soluciones, debe realizarse teniendo en cuenta el estado de la técnica (art. 25 RGPD). Es decir, deben implementarse las medidas de seguridad avanzadas, nunca obsoletas, que sean capaces de impedir o bloquear los ataques informáticos actuales. Un ejemplo de incumplimiento sería el uso de sistemas de cifrado obsoletos.

El análisis de riesgo debe ser una actividad viva en la empresa. Debido a que la norma exige la **actualización constante de las medidas de seguridad** y al aumento de los delitos informáticos, la empresa debe establecer un sistema de vigilancia que haga revisiones periódicas y siempre que cambien circunstancias tecnológicas tanto en la empresa como en el sector informático.

El RGPD desplaza a las empresas la responsabilidad de identificar las medidas de seguridad que aplicarán en el tratamiento de datos que llevan a cabo y la actualización periódica de las medidas implementadas y el protocolo de actuación.

NOTIFICACIÓN DE VIOLACIONES DE SEGURIDAD DE LOS DATOS

La destrucción, pérdida o alteración accidental o ilícita de datos personales, o la comunicación o acceso no autorizados a dichos datos, deberá ser documentada y notificada a la autoridad competente. También deberá comunicarse a los interesados en caso de que entrañe un alto riesgo para sus derechos o libertades.

Esta es otra de las novedades más importantes se trata de una nueva obligación que el RGPD impone al responsable del tratamiento: notificar las violaciones de seguridad de los datos.

Es decir, el responsable del tratamiento de los datos deberá notificar a la autoridad competente (AEPD en España) cualquier brecha de seguridad que se haya producido en el plazo de 72 horas desde que ocurra.

Además, si la brecha implica un riesgo para los interesados, también se les deberá notificar a ellos.

SANCIONES

El RGDP (art. 83) establece tres supuestos de infracciones que conllevan una multa administrativa. Esta clasificación para entender mejor las sanciones sería:

- Infracciones LEVES: efectivas, proporcionadas y disuasorias, dejando a la Autoridad Administrativa su cuantificación.
- Infracciones GRAVES: 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 MUY GRAVES: 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.

Somos conscientes de la complejidad de la adaptación a esta nueva obligación legal, por ello queremos tranquilizarle e informar que contamos con los conocimientos y las herramientas necesarias para la elaboración de su política de seguridad y protocolo de actuación.

Durante este periodo debe invertirse para adaptar las medidas jurídicas, técnicas y organizativas de las empresas en la recogida de datos de sus usuarios y clientes, de modo que cuando llegue la fecha de la aplicación efectiva del Reglamento puedan garantizar su cumplimento, tanto a sus propios clientes como a las autoridades de supervisión nacionales y europeas.

El RGPD será aplicable a partir del 25 de mayo de 2018. Aún tienes tiempo para analizar y adecuar tu empresa. Si necesitas apoyo o asesoramiento, contacta con nosotros. Estamos a tu servicio.

GRUPO esem

Parque de Actividades Empresariales Asuaran
Edificio Asua, Planta Baja A. 48950 Erandio. Bizkaia
www.esem-empresas.net
CIF: B-95152252

secretaria@esem-empresas.net
Tel: 94 453 81 81 Fax: 94 494 15 73

laboral@esem-empresas.net
Tel: 94 453 81 82 Fax: 94 453 19 50

contabilidad@esem-empresas.net
Tel: 94 453 81 83 Fax: 94 453 82 78