CINC | ASESORÍA

SE ACERCA LA FINALIZACIÓN DEL PLAZO PARA ADAPTARSE AL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)

A partir del próximo 25 de mayo de 2018 entra en vigor el nuevo Reglamento Europeo General de Protección de Datos (RGPD), relativo al tratamiento de datos personales y a la libre circulación de éstos. Esta normativa será de aplicación obligatoria a partir de esa fecha e impone a las empresas numerosos deberes en relación a la privacidad.

Además, también queda pendiente la aprobación de la nueva Ley Orgánica de Protección de Datos, que se encuentra actualmente fase de tramitación parlamentaria y que muy probablemente no estará llesta para el próximo 25 de mayo, fecha de aplicación del RGPD. En cualquier caso, esto no supone ningún tipo de ventaja o inconveniente, ya que el Reglamento europeo será plenamente exigible de todas formas.

¿En qué consiste el RGPD?

El RGPD es un tipo de norma que tiene aplicación directa en todos los estados de la UE y, por tanto, no precisa de ningún tipo de mecanismo de transposición específico. Esto significa que no hace falta que exista ninguna ley española para que el Reglamento europeo resulte obligatorio, sino que es exigible como si fuera una ley nacional.

Mi empresa aún no se ha adaptado al RGPD: ¿por dónde empiezo?

Es importante establecer un mapa de ruta para cumplir con el nuevo Reglamento, ya que hay numerosas decisiones jurídicas relevantes a tener en cuenta.

El primer paso que todas las empresas deberían llevar a cabo es identificar y analizar las áreas de riesgo y documentar los tratamientos de datos personales que se llevan a cabo, a través de un inventario de todas las actividades de tratamiento que realiza la compañía. De esta forma será más sencillo clasificar los datos de acuerdo con: su naturaleza, finalidad, categoría, origen, si son susceptibles de ser compartidos, etc.

¿Cúales son las obligaciones derivadas del RGPD deberán asumir las empresas y a qué riesgos se enfrentan en caso de incumplimiento?

Son muchas las obligaciones que tanto las empresas, autónomos y organismos públicos y privados que traten datos de carácter personal deben conocer y el tiempo es escaso, por lo que es necesario adoptar rápidamente las decisiones necesarias para llegar a ese plazo en situación de cumplimiento.

El riesgo de no hacerlo es el de posibles sanciones: las multas pueden llegar hasta los 20 millones de euros o el 4% de la facturación anual global del infractor. La autoridad de control puede actuar de oficio o por denuncia de los interesados.

En cuanto a los cambios y obligaciones que afectan a las empresas, podemos destacar entre otros los siguientes:

• Delegado de Protección de Datos (DPD/DPO). El Reglamento obliga a quienes realicen ciertos tratamientos, a nombrar un DPO, que podrá ser externo o interno. Un DPO deberá ser una persona experta en Protección de Datos y en métodos y técnicas de Seguridad de la información.

• Exigencia de la realización de una evaluación de impacto relativa a la protección de datos para ciertos tratamientos.

• Violaciones de la seguridad de los datos personales. Obligatoriedad de comunicarlas en un plazo de 72 horas a la Agencia Española de Protección de Datos, y en casos graves, a los propios afectados.

• Se elimina el consentimiento tácito (por silencio), lo que obligará a las empresas a recabar un nuevo consentimiento para poder mantener todos aquellos datos que en el pasado se obtuvieron tácitamente o buscarles otra cobertura legal.

• Se amplían las obligaciones de información a los afectados, lo que obligará ponerles al día en dicha información a los ya existentes.

• Se amplía el contenido mínimo en los contratos de acceso a datos por parte de terceros, por lo que deberán de establecerse de nuevo los contratos con los encargados de tratamiento, dado que los actuales no cumplen con el RGPD.

• El RGPD no establece diferenciación entre datos personales y datos 'profesionales' (datos de contacto de personas físicas que prestan sus servicios en una persona jurídica y empresarios individuales) como estableció el vigente Reglamento, lo que obligará a las empresas a tener que realizar acciones informativas a esta categoría de datos.

1.- CONSENTIMIENTO EXPRESO

Se establece la obligación de las empresas de obtener un consentimiento expreso, inequívoco y verificable, y no tácito de la información que se obtenga de sus clientes. Se considera consentimiento tácito cuando, después de haber recibido la información correspondiente, el usuario no dice que no (ejemplo: "si no me contestas antes de 30 días, entonces te enviaré información comercial de terceros").

Por tanto, el consentimiento tácito se considera válido, siempre y cuando no nos encontremos ante datos especialmente protegidos.

Atención: A partir de la entrada en vigor del nuevo RGPD, no se podrá seguir obteniendo el consentimiento de los afectados por omisión. Será necesario revisar todos los tratamientos anteriores, para adecuarlos a las previsiones de la nueva normativa.

Puede ser inequívoco y otorgarse de forma implícita cuando se deduzca de una acción del interesado (por ejemplo, cuando el interesado continúa navegando por una web y acepta así el que se utilicen cookies para monitorizar su navegación).

2.- TRANSPARENCIA EN LA INFORMACIÓN

Será necesario que las empresas detallen explícitamente y con un lenguaje comprensible los datos e información personal requerida al usuario o cliente y solo se podrá tratar los datos en caso que tengan un interés legítimo.

El deber de informar a los afectados sobre el uso y las finalidades del tratamiento de datos, sufre una importante modificación con el nuevo RGPD, pues se amplía considerablemente la información que se les debe suministrar, incluyendo aspectos no contemplados hasta la fecha como:

• Base jurídica del tratamiento

- Intención de realizar transferencias internacionales
- Datos del Delegado de Protección de Datos (si lo hubiere)
- El plazo o los criterios de conservación de la información,
- La existencia de decisiones automatizadas o elaboración de perfiles,
- El derecho a presentar una reclamación ante las Autoridades de Control

Atención. Los procedimientos, modelos o formularios diseñados de conformidad con la LOPD, deberán ser revisados y adaptados al nuevo RGPD, tanto para adaptarlos al nuevo contenido del deber de informar, como para ajustar su forma a los requisitos de precisión y claridad que exige la nueva normativa.

3.- SEGURIDAD

Las empresas están obligadas a informar cuando hayan sufrido una brecha de seguridad a las autoridades de control y, dependiendo de la gravedad, a los afectados. Aunque es un asunto necesario hoy en día, el reglamento establece la necesidad de dejar plasmada una estrategia en materia de seguridad.

En la nueva normativa, las medidas de seguridad no aparecen tan detalladas, sino que cada organización deberá contar con un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

Además, la tipología de los datos no será la única variable a tomar en consideración a la hora de determinar las medidas técnicas y organizativas aplicables sino que, por el contrario, el nuevo RGDP tiene en cuenta:

- El coste de la técnica
- Los costes de aplicación
- La naturaleza, el alcance, el contexto y los fines del tratamiento
- Los riesgos para los derechos y libertades

Atención. El esquema de medidas de seguridad previsto en el Reglamento de Desarrollo de la LOPD no seguirá siendo válido de forma automática. Es necesario determinar, caso por caso, las medidas aplicables, bajo un enfoque de riesgo, basado en el principio de la seguridad desde el diseño y por defecto.

4.- ENCARGADOS DE TRATAMIENTO

También la figura de los encargados de tratamiento sufre importantes cambios en la nueva regulación. En síntesis, estos cambios se pueden resumir en tres puntos:

1) El nuevo RGPD establece obligaciones expresamente dirigidas a los encargados de tratamiento, como:

- Mantener un registro de actividades de tratamiento.
- Determinar las medidas de seguridad aplicables a los tratamientos que realizan.
- Designar a un Delegado de Protección de Datos en los casos previstos por el RGPD.

2) Se acentúa el deber de diligencia en la elección del encargado del tratamiento, de manera que los responsables habrán de elegir únicamente encargados que ofrezcan garantías suficientes para aplicar medidas técnicas y organizativas apropiadas.

3) Se modifica el contenido mínimo que debe incluir el contrato con el encargado del tratamiento, incluyendo aspectos como:

• Objeto, duración, naturaleza y la finalidad del tratamientos
• Tipo de datos personales y categorías de interesados
• Obligación del encargado de tratar los datos personales únicamente siguiendo instrucciones documentadas del responsable
• Condiciones para que el responsable pueda dar su autorización previa, específica o general, a las subcontrataciones
• Asistencia al responsable, siempre que sea posible, en la atención al ejercicio de derechos de los interesados...

Atención. Se deben revisar todos los contratos de encargo de tratamiento firmados con anterioridad, para verificar si cumplen las nuevas exigencias del RGPD.

5.- DERECHOS DEL CIUDADANO

El nuevo RGPD incluye nuevos derechos como el derecho a la portabilidad y el derecho al olvido, el derecho a no ser objeto de decisiones individualizadas y el derecho a la limitación del tratamiento.

- EL DERECHO DE ACCESO: Es el derecho a conocer qué datos de carácter personal tuyos están siendo tratados por parte del responsable, la finalidad de este tratamiento, el origen de los citados datos y si se han comunicado o se van comunicar a un tercero.

Atención: Según la LOPD, el responsable del tratamiento debía facilitarse todos los datos de base del afectado, pero no copias o documentos. Sin embargo, el nuevo RGPD reconoce expresamente el derecho de los afectados a obtener gratuitamente una copia de los datos personales objeto de tratamiento.

Si es posible, el responsable del tratamiento debe estar facultado para facilitar acceso remoto a un sistema seguro que ofrezca al interesado un acceso directo a sus datos personales.

- EL DERECHO DE RECTIFICACION: Consiste en la posibilidad de modificar aquellos datos que sean inexactos o incompleto

Atención: Además de rectificar los datos inexactos, se incluye el derecho a que se completen los datos personales incompletos, inclusive mediante una declaración adicional.

- EL DERECHO DE CANCELACIÓN: Permite la cancelación de datos personales que sean inadecuados o excesivos.

Atención: Los interesados tienen derecho a que sus datos personales se supriman y dejen de tratarse:

- si ya no son necesarios para los fines para los que fueron recogidos o tratados de otro modo,
- si los interesados han retirado su consentimiento para el tratamiento o se oponen al tratamiento de datos personales que les conciernen,
- si el tratamiento de sus datos personales incumple de otro modo el RGPD

- El DERECHO DE OPOSICION: Mediante el ejercicio de este derecho el interesado puede oponerse al tratamiento de sus datos personales en los siguientes supuestos:

- Cuando no siendo necesario su consentimiento para el tratamiento, exista un motivo legítimo y fundado referente a su concreta situación personal (salvo que una Ley establezca lo contrario).

- Cuando estemos ante tratamientos de datos personales cuya finalidad sea la realización de actividades de publicidad y prospección comercial
- Cuando el tratamiento tenga como fin la adopción de una decisión referida a su persona, basada únicamente en un tratamiento automatizado de sus datos personales

- DERECHO AL OLVIDO: Es una manifestación de los derechos de cancelación u oposición en el entorno online. El responsable del tratamiento que haya hecho públicos datos personales, está obligado a indicar a los responsables del tratamiento que estén tratando tales datos personales, que supriman todo enlace a ellos, o las copias o réplicas de los mismos.

Atención: El derecho al olvido tiene algunas limitaciones como la libertad de expresión y el derecho a la información, el interés público en el ámbito de la salud, la investigación así como la defensa de reclamaciones.

- DERECHO A LA PORTABILIDAD DE LOS DATOS: Es una forma avanzada del derecho de acceso por el cual la copia que se proporciona al interesado debe ofrecerse en un formato estructurado, de uso común y lectura mecánica. Implica que los datos personales del interesado se transmiten directamente de un responsable a otro, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.

- DERECHO A NO SER OBJETO DE DECISIONES INDIVIDUALIZADAS. El interesado debe tener derecho a no ser objeto de una decisión, que puede incluir una medida, que evalúe aspectos personales relativos a él, y que se base únicamente en el tratamiento automatizado y produzca efectos jurídicos en él o le afecte significativamente de modo similar.

- DERECHO A LA LIMITACION DEL TRATAMIENTO: Solicitar al responsable que suspenda el tratamiento de datos cuando:

- Se impugne la exactitud de los datos, mientras se verifica dicha exactitud por el responsable.

- El interesado ha ejercitado su derecho de oposición al tratamiento de datos, mientras se verifica si los motivos legítimos del responsable prevalecen sobre el interesado.

- el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;

- el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones

6- REGISTRO

El reglamento exige la obligación de registrar documentalmente las operaciones de tratamiento, tanto por parte de los Responsables de Fichero como por los Encargados de Tratamiento.

¿Qué páginas web deben solicitar un consentimiento?

Cualquier página web o tienda online que recoja datos personales a través de formularios (de contacto, de suscripción o de solicitud de presupuesto) debe solicitar el consentimiento de los usuarios para poder tratar sus datos.

¿Puedo enviar comunicaciones comerciales a clientes sin consentimiento?

Se permite el envío de mensajes publicitarios o comerciales por correo electrónico a aquellos usuarios que previamente lo hubieran solicitado o autorizado de forma expresa. También se admite el envío de comunicaciones comerciales a aquellos usuarios con los que exista una relación contractual previa, en cuyo caso el proveedor podrá enviar publicidad sobre productos o servicios similares a los contratados por el cliente.

¿Tienes dudas sobre la implementación del RGPD?

Contacta con nuestro Departamento de Protección de Datos (monica.vilallave@cinc.es) sin ningún compromiso para resolver todas tus dudas.

Cordialmente,

CINC Asesoría de Empresas