Barcelona, 20 de febrero de 2018

CUESTIONES PRÁCTICAS RELATIVAS A LA NUEVA REGULACIÓN

DEL TRATAMIENTO DE DATOS PERSONALES

COMO RESULTADO DE LA PRÓXIMA APLICACIÓN DEL

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS (RGPD)[1].

La aplicación del RGPD, a partir del 25 de mayo de 2018, será, según apuntan los indicadores europeos, estricta y desde ese mismo día, en la medida en que las empresas y colectivos afectados han tenido un plazo aproximado de dos años, desde la entrada en vigor del RGPD, para adaptar sus procesos a la nueva normativa.

El RGPD, en su condición de Reglamento europeo, tiene alcance general y es directamente aplicable en cada uno de los Estados miembros, por lo que, a su entrada en vigor, quedarán derogadas, tanto la Directiva comunitaria 95/46 como las correspondientes normas nacionales de desarrollo, que únicamente seguirán vigentes en aquellas cuestiones que el Reglamento no contemple y no la contradiga.

[1] Reglamento UE 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

Debido a la importancia de lo anterior y el impacto que tendría para las empresas, comentamos en este documento las principales novedades y obligaciones a considerar por las compañías y entes afectados en su proceso de adaptación al RGPD.

Los principios básicos sobre los que descansa el RGPD son:

(i) el de responsabilidad proactiva: cada responsable del tratamiento de datos aplicará las medidas técnicas y organizativas apropiadas a su organización en función de los datos que trata, con qué fin y qué tipo de operaciones realiza y

(ii) el nuevo enfoque del riesgo: el cumplimiento en el tratamiento de los datos dependerá de la naturaleza, ámbito, contexto, fines y riesgo que tal tratamiento pueda suponer para los derechos y libertades de las personas. Cada organización determinará sus medidas en esta materia en función de los riesgos que el tratamiento suponga en su propio ámbito.

En concreto, y a los efectos oportunos, señalamos las principales novedades del RGPD y cómo correspondería, a los responsables del tratamiento de datos, abordar su implementación práctica.

1.- El RGPD se basa en la aplicación de los mismos **principios,** ahora vigentes, para la emisión del consentimiento, es decir: libertad, información y emisión de éste de forma específica e inequívoca.

No obstante, con la nueva normativa cabría indicar que:

- Se introduce la obligación de que el consentimiento, además de todo lo anterior, sea "explícito".
- Se eleva el umbral de edad, estableciéndose condiciones especiales para los menores de 16 años.
- El concepto de "datos" se amplía a todo lo que pueda identificar a una persona (ubicación, apps que consume, dispositivos utilizados…).

Revisión por parte de la empresa *respecto a la solicitud de consentimiento:*

- *Cotejo de cómo se recaba actualmente el consentimiento y modificar, en su caso, la declaración del interesado o fijar una acción positiva que manifieste conformidad.*
- *En caso de solicitar datos de carácter personal, como puede suceder en los departamentos de Recursos Humanos, que afecten a información sobre ideología,*

afiliación sindical, religión, etc., será necesario preparar documentos para recabar el consentimiento expreso y por escrito, si no se dispone de ellos.

- *Revisar y modificar las posibles prácticas de "consentimiento tácito", especialmente en el tratamiento de datos sensibles, la adopción de decisiones automatizadas y, sobre todo, en caso de transferencias internacionales. Deberán evitarse fórmulas en las que el consentimiento se entienda otorgado por la simple navegación en la web de la compañía.*
- *Modificar los umbrales de edad, si procede, teniendo en cuenta que en España el RLOPD reduce dicho umbral, por el momento, a 14 años.*
- *Eliminar los datos almacenados, recabados con anterioridad a la nueva normativa que nos sean necesarios.*
- *Solicitar de nuevo los datos que se desee mantener.*

2.- Se amplía la **obligación de información** por parte de la empresa. Sin embargo, se reduce de tres meses a uno el plazo para informar que los datos personales se han obtenido de terceros.

Revisión por parte de la empresa *respecto a la información que se da a los interesados porque con la aplicación del RGPD deberá a ampliarse de la siguiente forma:*

- *Informar de los datos de contacto del delegado de protección de datos.*
- *Documentar e identificar la base legal para el tratamiento de datos y sus destinatarios. Todo tratamiento de datos necesita apoyarse en una base que lo legitime: consentimiento, relación contractual, intereses vitales del interesado o de terceros, obligación legal, interés público, intereses legítimos del responsable, etc. Debe proporcionarse la información en el momento de recogerse los datos y especificar los intereses legítimos.*
- *Fijar cuál es el periodo de conservación de los datos.*
- *Dar la opción al interesado para que pueda dirigir sus reclamaciones a las autoridades de protección de datos.*
- *Informar que el responsable del tratamiento dispone de la existencia de decisiones automatizadas en el proceso de toma de datos (tales como la elaboración de perfiles).*

La información de todo tipo, referente a la recogida de datos o a las condiciones del tratamiento de los mismos, debe facilitarse por escrito (incluidos los medios electrónicos) de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo.

3.- Se **amplían los derechos reconocidos** a los interesados como pueden ser: el de transparencia de la información; de supresión o derecho al olvido; de limitación y de portabilidad.

Revisión por parte de la empresa *respecto al reconocimiento de los nuevos derechos de los interesados a indicar en las leyendas de los procesos de recogida de datos y la facilitación de su ejercicio.*

- *El responsable deberá posibilitar el acceso remoto a un sistema seguro que ofrezca a los interesados un acceso directo a sus datos personales. El objetivo es permitir al afectado que conozca si sus datos se están tratando y, en caso afirmativo, acceder a los mismos.*
- *Transcribir en las leyendas el derecho a no ser objeto de decisiones automatizadas reconociéndose el derecho del interesado a oponerse en determinadas circunstancias.*
- *Transcribir, también, el derecho a la limitación del tratamiento: derecho creado específicamente por el RGPD que impide el tratamiento de datos personales por el responsable cuando el afectado plantee determinadas reclamaciones contra el responsable o los necesite para ejercer su derecho de defensa.*
- *Deberá facilitarse el derecho al olvido o borrado de datos si no se está aplicando ya la jurisprudencia de la sentencia Google Spain. Será necesario prever que si se han hecho públicos los datos deberán tomarse medidas para informar de la solicitud de borrado.*
- *Informar en las leyendas que los datos de terceras personas o proporcionados por terceros no podrán ser objeto de portabilidad. Se traduce en la posibilidad de que el interesado solicite copia de los datos personales en un formato estructurado, de uso común y lectura mecánica, que se hayan facilitado a un responsable de tratamiento de datos, e incluso en pedir al responsable que transmita esos datos a otro responsable del tratamiento. Este derecho facilita la contratación electrónica y el cambio de proveedor de servicios, facilitando el traslado de datos y garantizando que no se retienen estos.*
- *Se regula el derecho a que el interesado no sea objeto de elaboración de perfiles de comportamiento, de lo que se le deberá informar o facilitar el ejercicio a negarse a dar sus datos.*
- *Asegurarse de dar la opción de ejercitar el derecho de rectificación, consistente en la posibilidad de solicitar la corrección de los datos que sean inexactos o completar aquellos que se estén tratando de forma parcial.*
- *Proporcionar medios para que las solicitudes del ejercicio de los derechos se presenten por medios electrónicos (en particular si los datos se han recabado de esa forma).*

4.- **Evaluación del impacto** ("Privacy Impact Assesment"). Esta nueva obligación para las empresas resulta imprescindible en aquellos casos en los que la recogida de datos puede implicar un alto riesgo para los derechos y libertades de las personas físicas[2].

Revisión por parte de la empresa *si incurre en alguno de los supuestos que establece la Guía en este punto (vid. nota al pie de página).*

En cualquier caso, se recomienda que, ante cualquier duda al respecto, la Compañía se someta a una evaluación de impacto.

[2] De acuerdo con la Guía publicada por la AEPD de 2014 sería aconsejable llevar a cabo **una evaluación de impacto**: Cuando se enriquezca la información existente sobre las personas mediante la recogida de nuevas categorías de datos o se usen las existentes con nuevas finalidades o en formas que antes no se usaban, en particular, si los nuevos usos o finalidades son más intrusivos o inesperados para los afectados; Cuando se lleve a cabo un tratamiento significativo no incidental de datos de menores o dirigido especialmente a tratar datos de estos, en particular si tienen menos de catorce años; Cuando se vaya a llevar a cabo un tratamiento destinado a evaluar o predecir aspectos personales relevantes de los afectados su estado de salud, fiabilidad o adecuación para tareas determinadas, situación financiera, laboral, social (en particular, en relación con la concesión de beneficios o subsidios), familiar (estructura familiar, datos de menores…), su ideología, creencias, formación, gustos, aficiones, compras, etc. su comportamiento, su encuadramiento en perfiles determinados (para cualquier finalidad), encaminado a tomar medidas que produzcan efectos jurídicos que los atañen o los afectan significativamente y, en particular, cuando establezcan diferencias de trato o trato discriminatorio, especialmente cuando se vayan a tomar decisiones que afectan de manera significativa a determinados colectivos o individuos, que establezcan diferencias entre ellos o puedan comportar un riesgo de discriminación de cualquier tipo (económica, social, política, racial, sexual, etc.) como, por ejemplo, la concesión o denegación de un determinado beneficio social, el ajuste de tarifas o precios o la oferta diferenciada de productos o servicios en función de los datos personales que se traten o que puedan afectar a su dignidad o su integridad personal; Cuando se traten grandes volúmenes de datos personales a través de tecnologías como la de datos masivos (Big data), internet de las cosas (Internet of Things) o el desarrollo y la construcción de ciudades inteligentes (smart cities); Cuando se vayan a utilizar tecnologías que se consideran especialmente invasivas con la privacidad como la videovigilancia a gran escala, la utilización de aeronaves no tripuladas (drones), la vigilancia electrónica, la minería de datos, la biometría, las técnicas genéticas, la geolocalización, o la utilización de etiquetas de radiofrecuencia o RFID (especialmente, si forman parte de la llamada internet de las cosas) o cualesquiera otras que puedan desarrollarse en el futuro; Cuando el tratamiento afecte a un número elevado de personas o, alternativa o adicionalmente, se produzca la acumulación de gran cantidad de datos respecto de los interesados; Cuando se cedan o comuniquen los datos personales a terceros y, en particular, siempre que se pongan en marcha nuevas iniciativas que supongan compartir datos personales con terceros que antes no tenían acceso a ellos, ya sea entregándolos, recibiéndolos o poniéndolos en común de cualquier forma; Cuando se vayan a transferir los datos a países que no forman parte del Espacio Económico Europeo (EEE) y que no hayan sido objeto de una declaración de adecuación por parte de la Comisión Europea o de la Agencia Española de Protección de Datos; Cuando se vayan a utilizar formas de contactar con las personas afectadas que se podrían considerar especialmente intrusivas; Cuando se vayan a utilizar datos personales no disociados o no anonimizados de forma irreversible con fines estadísticos, históricos o de investigación científica y; Cuando la recogida tenga como finalidad el tratamiento sistemático y masivo de datos especialmente protegidos.

5.- **La comunicación de fallos de seguridad** a la autoridad de Protección de Datos deberá realizarse en 72 horas como máximo.

La empresa deberá prever protocolos de comunicación al respecto, así como a los interesados afectados, salvo que se hubieran adoptado medidas de protección adecuadas, como por ejemplo la encriptación de datos.

6.- **Aplicación de medidas técnicas y organizativas de seguridad apropiadas**. Desaparecen de la normativa los antiguos niveles de seguridad de datos (básico, medio y alto) y, en sustitución suya las empresas deberán aplicar medidas según el estado de la técnica, los costes de aplicación, naturaleza, alcance y contexto y fines del tratamiento y riesgos para los derechos y libertades de las personas físicas.

Revisión por parte de la empresa *de la existencia y aplicación de medidas técnicas y organizativas de seguridad.*

- *Debe mantenerse actualizado el documento de seguridad siempre que garantice la seguridad, integridad y privacidad de la información personal.*

7.- **Las empresas son las responsables de la protección de los datos** personales que tratan a efectos de lo cual se les exigirá tener un *registro por escrito y con información detallada de las actividades de tratamiento que se realicen.*

8.- El RGPD añade la figura del **Delegado de Protección de Datos** (Data Protection Officer), que será obligatorio en las empresas responsables[3] o encargadas del tratamiento de datos[4], siendo voluntario para el resto. Las funciones que se le asignan son:

- Informar y asegurar al responsable (empresa) de las obligaciones para cumplir con el RGPD. Debe quedar constancia de las comunicaciones.

[3] **El responsable** de un fichero o tratamiento es la entidad, persona o el órgano administrativo que decide sobre la finalidad, el contenido y el uso del tratamiento de los datos personales. Así, una empresa será la responsable de los ficheros que contienen datos relativos a sus empleados y a sus clientes; un autónomo o empresario individual será responsable del tratamiento de los datos personales de sus clientes, un hotel será responsable del fichero de sus huéspedes; un gimnasio será responsable del fichero de sus socios; un centro educativo será responsable del fichero de sus alumnos, un Ayuntamiento será responsable del fichero del padrón...

[4] **El encargado** del tratamiento es la persona física o jurídica, pública o privada, u órgano administrativo que, solo o juntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Así lo será una empresa que preste servicios para la realización de envíos postales; el informático ajeno a la organización del responsable que realiza tareas de mantenimiento de software o hardware; el gestor administrativo que confecciona nóminas y gestiona el fichero de personal...

- Supervisar la aplicación de las normas por el encargado (el que trata los datos): asignación de responsabilidades, formación del personal y auditorías.
- Supervisar la documentación, notificación y comunicación de las violaciones de datos personales.
- Supervisar las respuestas a las solicitudes de la autoridad.
- Contacto con la autoridad.

Revisión por parte de la empresa *porque deberá implementar o incorporar, en su caso, esta figura asignándosele el job description que corresponda y otorgándose, en su caso, los oportunos contratos.*

9.- **Cumplimiento normativo**. Propuesta de mecanismos efectivos de verificación del cumplimiento, la adhesión a códigos de conducta o mecanismos de certificación, lo que supone proceder a:

- Análisis del riesgo.
- Registro de actividades de tratamiento.
- Adopción de medidas organizativas y técnicas para integrar en los tratamientos garantías que permitan la aplicación del RGPD.

10.- **Sanciones.** El incumplimiento de las cuestiones recogidas en el RGPD puede llegar a suponer para las compañías afectadas sanciones que alcancen los 20 millones de euros o el 4% de su facturación anual, sin perjuicio de los daños reputacionales que todo ello pudiera causar.

Como consecuencia de todo lo anterior, antes del 25 de mayo de 2018 se recomienda:

- *Revisar la estructura interna de los mecanismos relativos a la protección de datos.*
- *Comunicación a los empleados de la existencia de los protocolos de protección nuevos y necesarios que ha implementado la empresa como consecuencia de la aplicación del RGPD.*
- *Proceder con el tratamiento adecuado de los datos de acuerdo con la nueva normativa.*
- *Dar cumplimiento con los deberes de información ampliados.*
- *Facilitar el ejercicio de los nuevos derechos reconocidos.*

A 25 de mayo de 2018 deberán estar revisadas y con capacidad para ser aplicadas las siguientes actuaciones:

- Designación o nombramiento de un delegado de protección de datos.
- El análisis de riesgos de los tratamientos de datos.

- La identificación de los tipos de tratamiento a realizar.
- La evaluación del impacto, en su caso.
- El redactado de los avisos oportunos.
- El cambio, si procede, de los mecanismos de emisión del consentimiento, el almacenamiento anónimo y bajo pseudónimo.

Departamento Mercantil
Persona de contacto: Pilar Carreras Boj
Email: pcarreras@ortega-condomines.com