Alentia
ABOGADOS

CIRCULAR 3/2018

– PROTECCIÓN DE DATOS –

NUEVA NORMATIVA EUROPEA DE PROTECCIÓN DE DATOS ¡QUE NO CUNDA EL PÁNICO!

Como a estas alturas casi todo el mundo debe ya conocer, pues el bombardeo mediático de asesorías y consultoras especializadas ha sido intenso durante los últimos meses, a partir del próximo 25 de mayo resulta de aplicación en España, y en los restantes Estados miembros de la Unión Europea, el *Reglamento (UE) 2016/679, 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 de estos datos* (en adelante el "**Reglamento**"). Esta norma europea, que resulta de aplicación directa en cada Estado sin necesidad de una ley interna de trasposición, deroga la *Directiva 95/46/CE, de 24 de octubre de 1995*, que fue incorporada a nuestro ordenamiento jurídico por medio de la *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos*, que entró en vigor el 14 de enero del año 2000 y, desde esa fecha, debía ser cumplida.

El Reglamento no es más que una evolución de la normativa anterior, que pretende establecer un marco jurídico uniforme en el ámbito de la Unión Europea y, al mismo tiempo, actualizar determinadas previsiones de la regulación del año 1995, - especialmente motivadas por cambios tecnológicos acaecidos desde entonces -, y todo ello con el **objetivo de lograr una mejor protección de la privacidad de las personas físicas en cuanto al tratamiento que de sus datos de carácter personal realizan las empresas y, en general, las instituciones**.

Ahora bien, quien estuviera en situación de cumplimiento de la Ley Orgánica 15/1999, - desde 14 de enero de 2000 debía estarlo -, en algunos aspectos bastante más estricta y garantista que el Reglamento, simplemente tendrá que ajustar determinadas cuestiones de su organización para cumplir las previsiones de la nueva norma comunitaria. El que, por el contrario, no hubiera adecuado el tratamiento que en su empresa realiza de datos de carácter personal a la normativa del año 1999 está en la misma "mala" situación, desde un punto de vista de sus riesgos jurídicos, que en los últimos 18 años.

No olvidemos además que el propio Estado español debe adecuar su normativa interna al Reglamento y que tal adecuación debía producirse también antes del 25 de mayo de 2018. A la fecha de redacción de esta Circular nos consta la existencia de un Proyecto de Ley remitido a las Cortes Generales[1] que, en su disposición final quinta, indica que entra en vigor el 25 de mayo próximo. ¿Llegará a tiempo el Estado español para cumplir con ese plazo? No daría muy buen ejemplo si no fuera así.

Expondremos en la presente Circular, a modo de DECÁLOGO, las principales novedades que introduce el Reglamento y que pueden servir de guía para que cada responsable verifique cuán cercano o lejano se encuentra de su efectivo cumplimiento.

1 UNA NUEVA FILOSOFÍA: AUTO-EVALUACIÓN Y PROACTIVIDAD

Con carácter general, el Reglamento parte de un **"principio de responsabilidad proactiva"** y de un **"enfoque de riesgo"**, lo que conlleva que el responsable debe analizar su propia organización y los tratamientos de datos personales que realice para, en función de su propia auto-evaluación del riesgo para los derechos de las personas físicas, determinar las medidas adecuadas para cumplir con el Reglamento, lo que deberá ser capaz de acreditar ante los propios interesados y las autoridades de supervisión.

[1] Boletín Oficial de las Cortes Generales de 24 de noviembre de 2017.

Edificio Géminis
Av. Cortes Valencianas, 39.
46015 - VALENCIA
Tel: 963 384 801
Fax: 963 384 802

Al margen de estas dos previsiones generales, que deben servir para interpretar todo el Reglamento y que llevan a conceder un **amplio margen de autonomía al responsable del fichero**, veamos a continuación sus principales novedades prácticas respecto de la normativa vigente.

2 YA NO CABEN LOS CONSENTIMIENTOS TÁCITOS

Cuando el tratamiento de los datos se base en el consentimiento del interesado éste debe ser, como mínimo[2], "inequívoco", es decir, mediante una declaración o una clara acción afirmativa, debiendo ser capaz el responsable de demostrar el otorgamiento de este consentimiento. En definitiva, ya no valen las fórmulas de consentimiento tácito que admitía la legislación española y que tanto se utilizaban en la práctica, en las que se entendía otorgado si, por ejemplo, transcurría un plazo desde la recepción de una comunicación en la que pedían tu consentimiento y no manifestabas nada.

En materia de consentimiento llamamos también la atención sobre el hecho de que para que sea lícito el de un menor de 16 años se precisará que lo haya otorgado o autorizado el titular de la patria potestad o tutor, lo que lleva a entender que los mayores de esa edad, aun siendo menores de edad conforme a la legislación española, -entre 16 y 18 años -, sí pueden consentir válidamente para el tratamiento de sus datos personales[3].

3 MÁS INFORMACIÓN Y MÁS DERECHOS PARA EL INTERESADO

En materia de **información** al interesado, a las previsiones de la Ley española del año 1999, el Reglamento añade el proporcionar detalles sobre: (i) los datos de contacto del delegado de protección de datos cuando esta figura resulte necesaria, - más adelante nos referiremos a ella -, (ii) la base jurídica que legitima el tratamiento[4], (iii) el plazo o los criterios de conservación de la información[5], (iv) la existencia de decisiones automatizadas incluida la elaboración de perfiles, (v) la previsión de transferencia a terceros países y (vi) el derecho a presentar una reclamación ante la autoridad de control.

En aquellos casos en que los datos no se hayan obtenido del propio interesado se le deberá informar además, en un plazo máximo de 1 mes, del origen de los datos y de las categorías de datos.

Toda **la información debe proporcionarse al interesado en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, y por escrito**, siendo admisibles los medios electrónicos[6]. Desde luego la concisión difícilmente se compadece con la gran cantidad de información que debe proporcionarse, por lo que las autoridades de control[7] abogan por un suministro de la misma por capas o niveles, es decir, presentar una información básica en un primer nivel, que resulte fácilmente accesible en el mismo momento de la recogida, y una más detallada en

[2] Decimos como mínimo porque para determinadas categorías de datos (opiniones políticas, convicciones religiosas, afiliación sindical,…) se precisará, tal y como prevé el artículo 9 del Reglamento, un consentimiento explícito.

[3] El Reglamento (artículo 8.1) permite incluso que los Estados miembros puedan establecer una edad inferior siempre y cuando no esté por debajo de los 13 años.

[4] Nos referimos a la causa lícita que nos permite tratar los datos personales de un tercero, y que puede consistir en: consentimiento, relación contractual, intereses vitales del interesado, obligación legal, interés público o intereses legítimos prevalentes sobre los del propio interesado.

[5] El Reglamento (artículo 1.e)) prevé que los datos no pueden ser mantenidos de manera que se permita la identificación de los interesados durante más tiempo del necesario para los fines del propio tratamiento.

[6] El artículo 12.1 del Reglamento permite que la información se facilite de forma verbal cuando lo solicite el interesado y se demuestre por otros medios su identidad, si bien no debemos olvidar que la carga de la prueba sobre el cumplimiento de esta información recae en el responsable.

[7] Esta cuestión se explica con detalle en la Guía elaborada por la Agencia Española de Protección de Datos en colaboración con dos agencias autonómicas y que puede obtenerse en este link: http://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/modeloclausulainformativa.pdf

un segundo nivel o capa, al que pueda acceder el interesado si así lo desea.

Por lo que se refiere a los **derechos del interesado**, además de los ya tradicionales derechos ARCO[8] recogidos en la española Ley Orgánica de 1999, el Reglamento introduce como novedades:

1. Derecho al olvido. Más que un nuevo derecho autónomo es una manifestación del derecho de cancelación u oposición en el entorno online y requiere que el responsable, en aquellos casos en que ya haya hecho públicos los datos, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adopte medidas razonables con miras a informar a los responsables que estén tratando esos datos de la solicitud del interesado de supresión de cualquier enlace a los mismos, o cualquier copia o réplica.

2. Limitación del tratamiento. Conlleva que los datos, a petición del interesado, solo podrán ser objeto de tratamiento con su consentimiento o para unos fines muy concretos: (i) formulación, ejercicio o defensa de reclamaciones, (ii) con miras a la protección de los derechos de otra persona física o jurídica o (iii) por razones de interés público.

   Este derecho puede ser ejercitado: (i) en determinados supuestos que podríamos llamar de *impasse* en el tratamiento (cuando el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos, o cuando el interesado se haya opuesto al tratamiento mientras se verifica si los motivos del responsable prevalecen sobre los del interesado), (ii) cuando éste sea ilícito pero el propio interesado se oponga a la supresión y solicite en su lugar la limitación y (iii) cuando el responsable ya no necesite los datos pero el interesado sí los precise para la formulación, el ejercicio o la defensa de reclamaciones.

3. Portabilidad. Es el derecho del interesado a recibir los datos que le incumban en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, siempre y cuando el tratamiento esté basado en el consentimiento o en un contrato y el tratamiento se efectúe por medios automatizados. Cuando sea técnicamente posible el interesado tendrá derecho a que los datos se transmitan directamente de responsable a responsable.

   Se trata sin duda de un supuesto pensado para compañías de telecomunicaciones, eléctricas, de gas,... y pretende facilitar que el ciudadano pueda ir aprovechando las ofertas comerciales más ventajosas sin los inconvenientes propios de tener que proporcionar todos sus datos en cada nueva alta.

4 MÁS CONTROL SOBRE LOS TERCEROS QUE TRATAN DATOS POR MI CUENTA (EL ENCARGADO DEL TRATAMIENTO)

Con la normativa actual cuando un tercero nos prestaba un servicio que requería el acceso a los datos de nuestros ficheros (piénsese en la gestoría que realiza las nóminas o la empresa que nos ofrece alojamiento de nuestros ficheros en sus servidores) bastaba con que se suscribiera con él un contrato con determinado contenido previsto en la ley española, siendo únicamente responsable ese encargado del tratamiento cuando incumplía las disposiciones contractuales.

Con el nuevo Reglamento **el encargado del tratamiento tiene obligaciones legales propias** que van más allá de las recogidas en el contrato, - que en todo caso deberá suscribirse[9] -, y que se

[8] Derechos de acceso, rectificación, cancelación y oposición.

[9] El Reglamento regula el contenido del contrato con el encargado del tratamiento de una forma mucho más completa y exhaustiva que la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, exigiendo que contenga el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Un detalle de su contenido mínimo consta en el artículo 28 del Reglamento y para una exposición más detallada puede accederse a las directrices publicadas por la Agencia Española de Protección de Datos en este enlace:

refieren, básicamente, al mantenimiento de un registro de actividades de tratamiento, - conforme mencionamos en el punto 6 de la presente Circular -, al establecimiento de medidas de seguridad y a la designación de un delegado de protección de datos cuando resulte preceptivo – vid. apartados 7 y 8 siguientes -.

Además, **el responsable del fichero asume responsabilidad en la elección de ese prestador de servicios** que accede a los datos de carácter personal, debiendo asegurarse, y estar en condiciones de demostrar, que éste ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas para que el tratamiento de datos sea conforme con lo dispuesto en el Reglamento.

5 YA NO TENGO QUE INSCRIBIR MIS FICHEROS, PERO…

Con el Reglamento desaparece la obligación de notificación de los ficheros al Registro de la Agencia Española de Protección de Datos, de hecho desde el 14 de mayo de 2018 dejan de estar operativos los sistemas de inscripción de los ficheros.

6 …, EN SU LUGAR, DEBO LLEVAR UN REGISTRO DE LAS ACTIVIDADES DE TRATAMIENTO

Dentro de las medidas de responsabilidad activa a que hacíamos referencia al inicio de esta Circular, cada responsable debe llevar un registro de las actividades que conlleven un tratamiento de datos de carácter personal, que deberá figurar por escrito, - entiéndase en soporte electrónico -, y que estará a disposición de la autoridad de control.

Este "documento", que no debe notificarse a ninguna autoridad pero nos puede ser requerido en cualquier momento, debe contener una información muy similar a la que la Agencia Española de Protección de Datos exigía en sus formularios de notificación de ficheros, es decir: (i) identidad y datos de contacto del responsable, de su representante y, en su caso, del delegado de protección de datos; (ii) los fines del tratamiento; (iii) una descripción de las categorías de interesados y de las categorías de datos personales; (iv) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales; (v) cuando sea posible los plazos previstos para la supresión de las diferentes categorías de datos, y; (vi) una descripción general de las medidas técnicas y organizativas de seguridad.

Para la confección de este documento, y dado que la información a incluir es muy similar a la que constaba en los formularios que en su día se utilizaban para la inscripción, la propia Agencia de Protección de Datos española recomienda partir de tales formularios o modelos. De hecho la autoridad española ofrece en su sede electrónica una opción que permite a los responsables descargar el contenido completo de la inscripción que en su día realizó.

La confección y llevanza de este registro de actividades también es exigible a los encargados del tratamiento respecto de tratamientos efectuados por cuenta de un responsable.

Ahora bien, **esta obligación no aplica a ninguna empresa que emplee a menos de 250 personas**, a menos que el tratamiento que realice pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales de datos personales[10] o datos personales relativos a condenas e infracciones penales[11].

https://www.agpd.es/portalwebAGPD/temas/reglamento/common/pdf/directricescontratos.pdf

[10] Aquellos datos que revelen el origen étnico o racial, las opiniones políticas, las convicciones religiosas o filosóficas, la afiliación sindical, el tratamiento de datos genéticos, datos biométricos, datos relativos a la salud o a la vida u orientación sexual de una persona física (art. 9.1 del Reglamento).

[11] El tratamiento de este tipo de datos, conforme al artículo 10 del Reglamento, únicamente puede llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice una norma legal.

7 DEBO VELAR POR LA SEGURIDAD DE LOS DATOS SEGÚN MI PROPIO CRITERIO

La normativa española pre-Reglamento, concretamente el *Real Decreto 1720/2007, de 21 de diciembre* que venía a desarrollar la *Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal*, regulaba con detalle y de forma exhaustiva las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento, adquiriendo gran protagonismo el llamado "documento de seguridad" que, a modo de manual interno, debía preparar y llevar el responsable. Ello ofrecía gran seguridad y certeza al responsable.

Frente a ello, el Reglamento, en materia de medidas de seguridad, se despacha en su artículo 32 con una previsión del siguiente tenor: *"Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo."*

Este precepto es el mayor exponente del enfoque de responsabilidad proactiva que informa el Reglamento y al que aludíamos al inicio de esta Circular, y que conlleva que el responsable, tras un análisis previo de su situación y del riesgo que entrañen los tratamientos que vaya a llevar a efecto, establezca sus propias medidas de seguridad.

Tal indefinición normativa y ese amplio margen de autonomía sin duda va en detrimento de la seguridad jurídica, - o al menos de la certeza -, de las empresas que tratan datos de carácter personal, por lo que el Reglamento contempla la adhesión a códigos de conducta[12] o a un mecanismo de certificación[13] como elementos para demostrar el cumplimiento de las obligaciones legales en lo que se refiere a la seguridad de los ficheros.

En materia de seguridad el Reglamento también contempla como novedad la obligación de notificar a la autoridad de control de datos competente, dentro de las 72 horas siguientes a que se haya tenido conocimiento, las quiebras o violaciones de seguridad de los datos. En los casos en que sea probable que entrañe un alto riesgo para los derechos y libertades de las personas físicas el responsable deberá comunicarlo además al interesado.

8 ¿QUIÉN ES EL DELEGADO DE PROTECCIÓN DE DATOS? ¿ES OBLIGATORIO NOMBRARLO?

Se trata de una nueva figura que crea el Reglamento, y cuyo rol es informar y asesorar al responsable o al encargado del tratamiento, así como supervisar el cumplimiento de lo dispuesto en la norma europea, actuando además como persona de contacto con la autoridad de control.

Ahora bien, la designación de este experto, - que puede ser un empleado del responsable o un profesional externo, si bien siempre actuando de forma independiente en el desempeño de sus funciones -, es obligatoria siempre que:

1. El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales en el ejercicio de su función jurisdiccional.

2. Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala.

3. Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos (vid. nota al pie nº 10 de esta Circular) y de

[12] Vienen a ser códigos elaborados por asociaciones y organismos representativos de categorías de responsables que han sido validados por la autoridad de control y a los que se puede adherir la empresa (ya existen códigos tipo sectoriales en ámbitos como el del seguro, las actividades sanitarias privadas, las farmacias,...).

[13] Se trata de la validación de los tratamientos que realice determinado responsable por parte de un tercero independiente que confiere una certificación, sello o marca de protección de datos.

datos relativos a condenas e infracciones penales.

Por tanto, **en la mayor parte de los casos no va a ser necesario**, ni siquiera respecto de grandes compañías, **el tener que disponer de un delegado de protección de datos**.

9 EVALUACIÓN PREVIA EN TRATAMIENTOS DE ALTO RIESGO

En aquellos casos en que se considere que un determinado tratamiento entraña un alto riesgo para los derechos y libertades de las personas físicas, especialmente si utiliza nuevas tecnologías, el responsable debe realizar con carácter previo una "evaluación del impacto de las operaciones de tratamiento en la protección de datos personales". Esta evaluación debe contemplar[14] una descripción de las operaciones de tratamiento previstas, una evaluación de los riesgos probables y las medidas previstas para afrontarlos.

Conforme al Reglamento se entiende que un tratamiento es de alto riesgo y, por tanto, requiere de la previa evaluación de impacto, cuando

1. Conlleve una evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para esas personas físicas o les afecten significativamente.

   Piénsese por ejemplo en tratamientos automatizados de datos personales para la concesión de financiación o para la cobertura de un seguro de salud.

2. Se trate de un tratamiento a gran escala de las categorías especiales de datos (nota a pie de página nº 10 de esta Circular) o de datos relativos a condenas e infracciones penales.

3. Nos encontremos ante una observación sistemática a gran escala de una zona de acceso público, como por ejemplo la videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales.

Las autoridades de control establecerán listados de tipos de operaciones de tratamiento que requieren la previa evaluación de impacto así como de tipos de tratamiento para los que no es necesaria. En aquellos casos en que el tratamiento no esté en ninguno de los listados, ni positivo ni negativo, habrá que atender a la enumeración anterior o, en su defecto, será el propio responsable quien determine si va a realizar un tratamiento de alto riesgo.

10 TRANSFERENCIAS INTERNACIONALES DE DATOS

El Reglamento parte de los criterios que ya estaban contemplados en la legislación interna española, es decir, que sólo se pueden transmitir datos a aquellos países u organismos internacionales, - entiéndase como transferencia fuera del Espacio Económico Europeo -, respecto de los que la Comisión Europea haya considerado que disponen de un nivel adecuado de protección o, en otro caso, se obtenga autorización previa de la autoridad de control.

A partir de ahí nos encontramos con relevantes novedades:

1. El Reglamento establece que **el exportador de datos puede ser tanto un responsable como un encargado del tratamiento**, con lo que se facilita que un prestador de servicios establecidos en la Unión Europea pueda subcontratar con otros proveedores ubicados en terceros países.

2. A falta de decisión de adecuación por la Comisión Europea (resolución por la que declara que el tercer país garantiza un nivel de protección adecuado), **cabe la transferencia internacional de datos cuando se ofrezcan garantías adecuadas** sobre la protección que los datos recibirán en su destino, para lo que adquieren protagonismo los códigos de

[14] La Agencia Española de Protección de Datos ha elaborado una guía sobre la metodología a seguir para la elaboración de la evaluación de impacto que puede descargarse en este enlace: https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/2018/Guia_EvaluacionesImpacto.pdf

conducta y mecanismos de certificación a los que aludíamos en el punto 7 de la presente Circular.

3. También cabe entender que se dan garantías adecuadas cuando existan **normas corporativas vinculantes**, en los casos de flujos de datos en el seno de grupos multinacionales, aprobadas por la autoridad de control competente.

4. En ausencia de decisión de adecuación o de garantías adecuadas, cabrá la transferencia a terceros países si se dan, entre otras, las siguientes condiciones: (i) el interesado haya dado explícitamente su consentimiento tras haber sido informado de los posibles riesgos, (ii) la transferencia sea necesaria para la celebración o ejecución de un contrato; (iii) sea necesaria por razones importantes de interés público; (iv) para la formulación, el ejercicio o la defensa de reclamaciones, o; (v) para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento.