



Barcelona, 18 de mayo de 2016

Distinguido cliente:

La Comisión Europea publicó a principios de año 2012 su Propuesta de Reglamento sobre protección de datos personales. Desde entonces, las distintas instituciones europeas (Comisión, Parlamento y Consejo de la Unión Europea) han estado discutiendo las propuestas.

Ante esta situación, el pasado 14 de abril de 2016, el Parlamento Europeo aprobó el texto definitivo del Reglamento Europeo de Protección de Datos (el "Reglamento", en adelante). Este Reglamento renueva y sustituye el marco regulatorio de toda la Unión Europea (U.E., en adelante) en materia de protección de datos y **resultará de aplicación directa a todos los Estados Miembros de la U.E., sin necesidad de que sea traspuesto por una norma nacional.**

El presente Reglamento supone la derogación de la anterior normativa sobre protección de datos de carácter personal, con la intención de armonizar las legislaciones europeas sobre la materia vigentes en la actualidad, y que producían una diversidad de criterios en su aplicación real y práctica, con todo ello, se logra un refuerzo de la protección de los datos personales de los ciudadanos de la U.E. y la libre circulación de los mismos dentro del susodicho ámbito territorial.

Cabe recordar al respecto, que la entrada en vigor del presente Reglamento se producirá a los 20 días de su publicación en el Diario Oficial de la Unión Europea, sin embargo, su efectiva aplicación resultará en el plazo de dos años computados desde la fecha de publicación antes referenciada.

## PRINCIPALES NOVEDADES

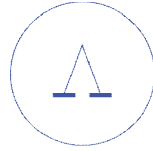
1. Su ámbito de aplicación, no sólo se centrará a los responsables y encargados de tratamiento establecidos en territorio europeo, sino que se ampliará a empresas que realicen tratamiento de datos de ciudadanos europeos.



2. Se produce un fortalecimiento de las garantías necesarias para la obtención del consentimiento de los afectados, asimismo, se exige que el consentimiento sea claramente inequívoco, y que el mismo se gestione adecuadamente.

Teniendo en cuenta lo anterior, otra de las novedades que se introducen, es que si se realiza un uso de servicios de la sociedad de la información por parte de menores de 16 años, o de 13 para los estados miembros de la U.E. que así lo acuerden, se deberá contar con el consentimiento de los progenitores o tutores legales.

3. Se reconocen una serie de nuevos derechos para los afectados, estableciéndose al respecto, que el plazo para responder a la petición de ejercicio de esos derechos por parte del destinatario del requerimiento se amplía a un mes (teniendo en cuenta que el plazo actual es de 10 días), pudiéndose prorrogar dos meses adicionales, cuando la complejidad del asunto lo aconseje. Asimismo, los derechos se pueden resumir en el derecho a información, de acceso, de rectificación y borrado (derecho al olvido), de restricción del tratamiento, de portabilidad y de objeción materia publicitaria).
4. Se establece el principio de *accountability*, en virtud del cual, los sujetos obligados, teniendo en cuenta el estado de la tecnología y los costes de implementación, y atendiendo a la naturaleza, finalidades, ámbito y contexto del tratamiento, además de la gravedad para los derechos y libertades de los individuos y los riesgos de probabilidad de cambio, deberán implementar medidas técnicas y organizativas tanto en el momento de determinación de las medidas a adoptar como antes de la obtención del dato y durante el tratamiento en sí mismo, es decir, que la privacidad debe abarcar todo el ciclo de vida del dato, introduciendo las debidas garantías que permitan cumplir con lo dispuesto en la normativa aplicable.
5. Se impone la obligación de comunicar las brechas de seguridad que afecten a datos personales a la Autoridad de Control, sin retrasos injustificados, tan pronto como sea posible, dentro del plazo de las 72 horas siguientes desde que se tenga conocimiento del incidente. De producirse pasadas el referido plazo, se deberá adjuntar a la notificación la justificación de ese retraso. Además, solo se podrá obviar este trámite si la brecha de seguridad no pone en riesgo los derechos y libertades de los individuos. Sin embargo, si la brecha la sufre el encargado de tratamiento, deberá comunicarlo al responsable del tratamiento sin demora injustificada.



6. Queda suprimida la obligación de inscribir los ficheros ante el Registro General de la Agencia Española de Protección de Datos, ya que se entiende que estas obligaciones formales no aportan valor respecto de la protección de datos personales, y en su sustitución, se imponen obligaciones internas de control y registro.
7. Aparece la obligación de realizar una evaluación de riesgos, con carácter previo al tratamiento, que permitirá que las medidas que se adopten tengan como finalidad evitar la pérdida de datos, cesiones y accesos no autorizados.
8. Se introduce la figura del Delegado de Protección de Datos (DPO), tanto en autoridades y organismos públicos, como en empresas con al menos 250 empleados. No obstante, en los casos de grupos de empresas se podrá contar con un único "DPO". Cabe anunciar que la adopción de esta figura se podrá realizar internamente o de manera externalizada a través de un tercero.
9. Se mejora el sistema de regulación para las transferencias internacionales de datos, que en la anterior regulación, la Directiva, no aparecía suficientemente especificado.
10. Por lo que se refiere al régimen sancionador previsto, y sin perjuicio del derecho de indemnización que el afectado pudiera reclamar judicialmente, las sanciones pueden alcanzar (i) hasta 10.000.000 de euros o hasta 2% del volumen de negocios mundial; o (ii) hasta 20.000.000 EUR o hasta 4% del volumen de negocios mundial, según el tipo incumplimiento en que se haya incurrido.

A modo de conclusión, y en orden a lo comentado con anterioridad, se hace esencialmente recomendable que las organizaciones busquen un asesoramiento legal para adaptarse al nuevo Reglamento. Asimismo, también sería aconsejable tener presente, que la realización de este proceso de adecuación se enmarca dentro de la cultura del cumplimiento que las organizaciones deben de adoptar, no sólo desde la perspectiva de la protección de datos, sino desde todos los ámbitos de riesgo a los que se encuentra expuesta una determinada compañía, teniendo en cuenta que el inicio de todo este proceso comienza con la evaluación de las áreas de riesgo específicas de la empresa; continúa con la recomendación de medidas correctoras, la preparación y redacción de protocolos internos y la implantación de los mismos.



Y finaliza con la revisión periódica, tanto de la evolución de la implantación, como de la adaptación del programa de cumplimiento adaptado a los cambios normativos que se vayan produciendo.

Además de los profesionales que habitualmente colaboran con su empresa, Óscar Casanovas, Mateu Lázaro y Albert Castellanos están a su entera disposición para cualquier aclaración o ampliación del contenido de la presente Circular.

Atentamente,  
AUDICONSULTORES

La presente Circular tiene como única y exclusiva pretensión la de facilitar a sus destinatarios una selección de contenidos de información general sobre novedades o cuestiones de carácter laboral, tributario o jurídico, sin que ello pueda constituir **asesoramiento** profesional de ningún tipo ni pueda ser suficiente para la toma de decisiones personales o empresariales.

© 2016 "Audiconsultores Advocats i Economistes, S.L.P.". Todos los derechos reservados