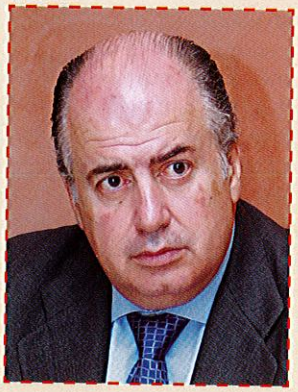
Reglamento Europeo de Protección de Datos y el sector sanitario

Ricardo De Lorenzo y Montero
Doctor en Derecho y Socio-Director en De Lorenzo Abogados. Presidente de la Asociación Española de Derecho Sanitario (AEDS).

El vigente Reglamento Europeo de Protección de Datos fue aprobado el pasado 27 de abril de 2016. No obstante, a pesar de su aprobación y consecuente entrada en vigor, su contenido será de aplicación el próximo 25 de mayo de 2018. Un periodo transitorio, especialmente en este año, en el que nuestro país deberá adecuar su normativa para dar cumplimiento a las obligaciones que el nuevo escenario jurídico aprobado por este Reglamento Europeo exige.

Adecuación en trámite, tratada ya en Consejo de Ministros el pasado mes de junio, en el que se vio el informe del Ministerio de Justicia sobre el futuro Anteproyecto de Ley Orgánica de Protección de Datos, en el que se introducen importantes novedades como el tratamiento de los datos de personas fallecidas por parte de sus herederos, teniendo en cuenta las instrucciones aportadas por las mismas incluyéndose además el "consentimiento tácito", debiendo ser expreso y afirmativo, estableciéndose la presunción de exactitud y actualización de los datos obtenidos directamente del interesado.



En cuanto a la edad para el consentimiento, se reduce desde los catorce a los trece años, tal y como permite el Reglamento Europeo, incidiéndose también en los derechos de acceso, rectificación, supresión, limitación del tratamiento, portabilidad y oposición, y se introduce la obligación de bloqueo que garantiza que esos datos queden a disposición de un tribunal, el Ministerio Fiscal u otras autoridades competentes como la propia Agencia Española de Protección de Datos, que será la autoridad de control, para la exigencia de posibles responsabilidades derivadas de su tratamiento, evitando así que se puedan borrar para encubrir el incumplimiento.

La norma europea así como la futura Ley española de Protección de Datos serán piezas centrales de la reforma de la protección de datos tanto en la UE como en nuestro país, y tendrán un impacto signifi-

cativo y de gran alcance en general para las empresas sanitarias en el contexto de una economía cada vez más basada en los datos. Así se actualizarán principios jurídicos existentes y otros que se aplicarán para afrontar los retos derivados de la globalización y los avances tecnológicos, a fin de garantizar una protección efectiva del derecho fundamental a la protección de datos.

El Reglamento, así como la futura Ley Orgánica de Protección de Datos, tendrán un impacto significativo y de gran alcance en general para las organizaciones sanitarias, ya que requieren un tratamiento de información especial de información salud de manera intensiva afectando a toda la población en caso de la Administracion Pública o en gran volumen como los centros sanitarios privados.

La norma incluye a los datos relativos en la salud entre las categorías especiales de datos, hasta ahora conocidos como datos sensibles (salud, origen racial, religión) que cuentan con obligaciones reforzadas. Las entidades cuya actividad principal consista en el tratamiento a gran escala de categorías especiales de datos personales –hospitales, clínicas, aseguradoras médicas, mutuas y, eventualmente, laboratorios y empresas farmacéuticas– estarán obligadas a nombrar un delegado de protección de datos (DPO).

Las nuevas normativas constituirán una oportunidad para adecuarse a la realidad sanitaria actual, a su futuro tecnológico y el futuro de los proyectos de investigación biomédica que contemplen la reutilización de datos, al permitir una aplicación más flexible de medidas de seguridad en función de los requerimientos de cada tipo de tratamiento de datos, adecuando proporcionalmente las salvaguardas en función de los riesgos detectados.

Las organizaciones sanitarias tendrán en consecuencia que adecuar y actualizar sus auditorías adaptándose a las nuevas normativas e implantando nuevos procedimientos de prevención y minimización del riesgo de la privacidad, como las evaluaciones del impacto de la privacidad (PIA, *Privacy Impact Analysis*) o la notificación a la autoridad de control y, en su caso, a los afectados de brechas de seguridad que puedan sucederse en sus sistemas de información.