Actualidad Profesional

Por Francesca Corvi, abogada especializada en Derecho privado, responsabilidad civil, Derecho del seguro y Derecho de familia y sucesiones.

El nuevo Reglamento Europeo de Protección de Datos: puntos claves de la reforma y adaptación

El 25 de mayo de 2016 entró en vigor el Reglamento UE 2016/679 General de Protección Datos (RGPD) que es plenamente aplicable desde el pasado 25 de mayo, tras dos años de periodo transitorio y de adaptación. El Reglamento representa, ahora, la norma de referencia en materia de protección de datos puesto que es directamente aplicable y no necesita normas internas de transposición ni de desarrollo o aplicación.

El Reglamento homogeneiza la protección de datos en la Unión Europea, impidiendo interpretaciones o normas que rompan la unidad territorial, limitando los poderes de los Estados miembros, ya que pierden competencias legislativas y ejecutivas. Sin perjuicio de lo anterior, la ley que sustituirá a la actual Ley Orgánica de Protección de Datos podrá incluir algunas precisiones o desarrollos en materias en las que el Reglamento lo permite. La Agencia Española de Protección de Datos, como autoridad nacional responsable, seguirá siendo la encargada de velar por su cumplimiento.

La mayor innovación que introduce el Reglamento es el principio de "responsabilidad proactiva" que convierte a los destinatarios en los responsables de determinar las medidas adecuadas para proteger los datos y los derechos y libertades de las personas. La norma, contrariamente a lo que estábamos acostumbrados, no prohíbe conductas concretas sino que establece objetivos que deberán ser perseguidos por los destinatarios, fijando un marco normativo que permite a los responsables adaptar su realidad a la protección de datos.

Para ello, los destinatarios son llamados a identificar qué tipo de datos tratan, con qué finalidad lo hacen y qué tipo de operaciones de tratamiento llevan a cabo, con el fin de realizar un análisis de riesgos y determinar así, a partir de unos principios que en todo caso van a tener que respetar, las medidas adecuadas para garantizar la protección de los datos y el cumplimiento del Reglamento. Analizar los riesgos significa, en la práctica, establecer hasta qué punto una actividad de tratamiento puede causar daños a los titulares de los datos.

Pueden existir riesgos asociados a la protección de la información, como por ejemplo el acceso ilegitimo a los datos, la modificación o la eliminación de los mismos; o bien pueden existir riesgos asociados al cumplimiento de los requisitos legales del Reglamento como, por ejemplo, el tratamiento de datos sin base jurídica o la falta de un procedimiento para atender el ejercicio de los derechos de los interesados.

Identificados los riesgos, los responsables del tratamiento de datos deben emplear las medidas de seguridad idóneas, que encajan en su situación, para adaptarse al reglamento y garantizar los datos y derechos de las personas. Antes de la directa aplicación del Reglamento, el desarrollo reglamentario de la Ley Orgánica de Protección de Datos establecía con detalle las medidas de seguridad que debían aplicarse según el tipo de datos objeto de tratamiento. Ahora, los responsables y encargados establecerán las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado en función de los riesgos detectados en el análisis previo.

Un pilar del principio de la responsabilidad activa es el Delegado de Protección de Datos (DPO, Data Protection Officer), nueva figura que introduce el Reglamento y que desempeña funciones de información y asesoramiento, tanto al responsable como al encargado del tratamiento, de las obligaciones que les incumben, supervisión del cumplimiento de las previsiones del Reglamento, cooperación con la autoridad de control y punto de contacto de la autoridad de control para cuestiones relativas al tratamiento. El Delegado de Protección de Datos debe tener conocimientos especializados y su nombramiento es obligatorio sólo en los casos previstos por el Reglamento. En los demás casos, existe la posibilidad de una designación voluntaria.

Otra de las claves de la reforma radica en la regulación del consentimiento. El Reglamento mantiene el principio de que todo tratamiento de datos necesita apoyarse en una base que lo legitime que puede ser: consentimiento, relación contractual, intereses vitales del interesado o de otras personas, obligación legal para el responsable, interés público o ejercicio de poderes públicos, intereses legítimos prevalentes del responsable o de terceros a los que se comunican los datos. Identificar la base legal es indispensable para poder estar en condiciones de demostrar que se cumple con el Reglamento. Aunque no se contemple de forma explícita, se deduce del articulado del Reglamento y, en general, del principio de responsabilidad activa.

En cuanto al consentimiento, éste tiene que ser libre, por lo que no vale si no hay posibilidad de oponerse. Específico, lo que impide que se acumulen en una misma opción tratamientos que no son iguales. Informado, por lo que el interesado tiene que conocer siempre todas las circunstancias. E inequívoco por lo que tiene que ser prestado mediante una manifestación del interesado o mediante una clara acción afirmativa. A diferencia de la regulación anterior, el consentimiento no puede ser tácito.

Esto plantea una serie de consecuencias en cuanto a la información a facilitar a los interesados, cuando proporcionarla y como obtener el consentimiento. Las empresas deberán por lo tanto revisar los consentimientos obtenidos con anterioridad a la aplicación del Reglamento que seguirán siendo válidos sólo si hubieran prestado mediante una manifestación o acción afirmativa y deberán dejar de obtener el consentimiento por omisión, haciéndolo de acuerdo con las disposiciones del Reglamento.

Otro tema muy relevante son los derechos de los interesados y los procedimientos y las formas para ejercitar los derechos que deben ser visibles, accesibles y sencillos. El Reglamento contiene los derechos tradicionales de acceso, rectificación, cancelación y oposición (ARCO) aunque introduce alguna novedad. La más destacable el derecho al olvido, como consecuencia del derecho al borrado de los datos personales, y el derecho a la portabilidad que obliga al responsable a facilitar una copia completa de los datos en soporte electrónico y en formato compatible.

En definitiva, para adaptarse a la nueva regulación, será necesario nombrar un Delegado de Protección de Datos, si es obligatorio o si se asume voluntariamente; elaborar un registro de actividades de tratamiento; realizar un análisis de riesgos; revisar las medidas de seguridad a la luz de los resultados del análisis;, establecer mecanismos y procedimientos de notificación de quiebras de seguridad; adecuar los formularios; adaptar los mecanismos y procedimientos para el ejercicio de derechos; valorar si los encargados, en caso de existir, ofrecen garantías y adaptar sus contratos; adaptar la política de privacidad, etc.

Las grandes empresas empezaron ya hace tiempo el proceso de adaptación, pero la gran preocupación son las pequeñas y medianas empresas. Se trata de una normativa compleja, que establece numerosos requisitos difíciles de cumplir y que, al mismo tiempo, implanta un modelo radicalmente distinto al anterior, que implica asumir la responsabilidad de adoptar las medidas que cada responsable considere adecuadas. Esto implica conocer perfectamente el Reglamento y, para muchos empresarios y profesionales, va a resultar fundamental el asesoramiento de un abogado experto en esta materia, máxime teniendo en cuenta que las sanciones que establece el Reglamento constituye uno de los cambios que más llama la atención entre las empresas.