ÁLVARO RAMOS SUÁREZ

Abogado Asociado de Abril Abogados

Reglamento General de Protección de Datos (GDPR)

Novedades de 2016 en materia de Privacidad y Ciberseguridad

La aprobación del nuevo Reglamento General de Protección de Datos (GDPR) va a suponer un gran cambio para todas las empresas que traten datos de carácter de personal. Este Reglamento se deberá implementar el 25 de mayo de 2018, sin embargo, existen multitud de dudas generadas por la complejidad de su redacción, por las novedades que trae consigo y que supondrán grandes cambios en lo que conocemos hasta ahora como protección de datos.

Desde las asociaciones de privacidad ya se está trabajando en la forma en que dicho reglamento debe de ser implementado. Además, la Agencia Española de Protección de Datos está preparando una guía de adecuación al nuevo reglamento, que esperemos no tarden en publicar. La Agencia ya en el mes de mayo publicó «el Reglamento de Protección de Datos en 12 preguntas» que despejaba algunas dudas.

Son muchas las novedades del Reglamento que deben aclararse. Por ejemplo, en relación al consentimiento se establece que cuando éste sea necesario debe darse mediante un acto afirmativo claro que refleje una manifestación de voluntad libre, específica, informada e inequívoca del interesado de aceptar el tratamiento. Por tanto, el silencio, las casillas ya marcadas o la inacción no deben constituir consentimiento. No cabe duda por tanto de que el consentimiento debe de darse en positivo a partir de ahora, pero, **¿qué sucede con los consentimientos recabados mediante el consentimiento informado admitido por nuestro reglamento de protección de datos?** Según el GDPR en su considerando 171 establece que cuando el tratamiento se base en el consentimiento de conformidad con la antigua Directiva, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio se ajusta a las condiciones del GDPR. Por tanto, según este considerando, los consentimientos informados «en negativo» no serían válidos, ¿será necesario solicitar nuevamente el consentimiento?

Existen otras muchas dudas como por ejemplo las notificaciones de las brechas de seguridad obligatorias, en qué casos es necesario nombrar al Delegado de Protección de Datos (DPO), si los datos relativos a personas de contacto de las personas jurídicas se consideran de carácter personal o por ejemplo si el tratamiento de datos para el envío de información comercial se considera interés legítimo y por tanto no requiere de consentimiento.

Esperamos que a lo largo del año 2017 todas estas dudas y otras muchas sean resueltas, pero en nuestra opinión todas las empresas deben tener presente que se avecinan grandes cambios y que, aunque hay tiempo para la implementación de los mismos, éstas deben ir preparándose.

Privacy Shield

Otra de las novedades del 2016 en protección de datos ha sido la aprobación el 12 de julio del Privacy Shield. Este acuerdo es el que sustituye al Puerto Seguro (Safe Harbour) anulado a finales del 2015 por el TJUE, y que permitirá realizar transferencias internacionales de datos desde la Unión Europea hacia Estados Unidos, sin necesidad de solicitar autorización a la entidad de control, en el caso de España, a la Agencia Española de Protección de Datos, o solicitar el consentimiento del titular de los datos.

Este nuevo acuerdo es mucho más riguroso que el antiguo Safe Harbour y persigue recuperar la confianza en los flujos de datos transatlánticos.

Este marco protege los derechos fundamentales de cualquier persona en la UE cuyos datos personales se transfieran a los Estados Unidos y aporta claridad jurídica para las empresas que dependen de transferencias transatlánticas de datos.

Directiva NIS

También a lo largo del mes de julio, el Parlamento Europeo adoptó la Directiva sobre Seguridad de Redes y Sistemas de Información, que deberá ser traspuesta a la legislación nacional antes de mayo de 2018.

El objetivo de esta Directiva, conocida como NIS, es dar una respuesta efectiva a los problemas de seguridad de las redes y sistemas de información, siendo necesario atacar estos problemas mediante un planteamiento global en la Unión que integre requisitos mínimos comunes en materia de desarrollo de capacidades y planificación, intercambio de información, cooperación y requisitos comunes de seguridad para los operadores de servicios esenciales y los proveedores de servicios digitales.