GDPR, el próximo reto normativo para las empresas asociadas

El 25 de mayo de 2018 es la fecha en la que se empezará a aplicar el Reglamento General de Protección de Datos europeo (GDPR, en sus siglas inglés). AUSAPE quiere acompañar a los Asociados en esta nueva adaptación normativa. En sus dos primeros eventos sobre el tema, celebrados en Madrid y Barcelona, ha reunido a 217 empresas.

Al igual que hizo con otros cambios normativos en los últimos años como, por ejemplo, SEPA, Cret@ o, el más reciente, el Suministro Inmediato de Información (SII), la Asociación va a dedicar esfuerzos para que las empresas asociadas dispongan de la información necesaria para realizar sin sobresaltos su adaptación a GDPR. Para ello, está organizando eventos presenciales, que están cosechando altos índices de asistencia.

Los dos primeros workshops sobre este tema, que han tenido lugar el día 16 de enero en Barcelona y día 18 en Madrid, reunieron a 116 y 101 profesionales, respectivamente. Ambos fueron impartidos por los expertos legales de Marzo & Abogados, Ana Marzo y Gonzalo M. Flechoso, especialistas en derecho y nuevas tecnologías que asesoran de forma habitual a la Asociación.

DE APLICACIÓN DIRECTA EN LA UE

El nuevo Reglamento, que fue aprobado en mayo de 2016, supone un reto para las organizaciones en tanto que incorpora nuevas obligaciones para las compañías en el ámbito del tratamiento de los datos y nuevos derechos para los ciudadanos.

Ambos especialistas explicaron que la norma, al ser un reglamento, deroga la anterior Directiva comunitaria sobre el tema y tiene efecto directo en todos los Estados miembro sin necesidad de transposición interna, aunque deja algún aspecto regulable a nivel local. De ahí que el Consejo de Ministros ya haya remitido el anteproyecto de ley de la LOPD al Parlamento para su aprobación antes, a ser posible, de que se aplique el nuevo Reglamento General de Protección de Datos.

Sus antecedentes se encuentran en la globalización y la gran evolución de tecnologías como Internet de las Cosas, la Inteligencia Artificial o Big Data, cuyo despliegue ha dado como resultado que hoy se procese y difunda un volumen cada vez mayor de información personal a escala mundial. “Esta es una norma que persigue reforzar la seguridad jurídica y establecer un marco de confianza para el desarrollo de la economía digital en la UE, y la unificación de los niveles de derechos y obligaciones exigibles a las empresas para garantizar la protección de los datos personales de los ciudadanos europeos”, señalaron los abogados.

Durante ambas sesiones matutinas se revisaron los principios en los que se basa el Reglamento que son el de licitud, lealtad y transparencia, y otros como el de exactitud, limitación de la finalidad, minimización de los datos, integridad y confidencialidad, exactitud, limitación del plazo del conservación, integridad y confidencialidad y responsabilidad proactiva, etc. De estos principios ‘descuelgan’ importantes obligaciones, muchas de ellas novedosas.


Barcelona

Es el caso de la necesidad de consentimiento por parte del interesado, que debe darse mediante un acto afirmativo claro que refleje su voluntad libre, específica, informada e inequívoca de aceptar el tratamiento de datos de carácter personal, es decir, el responsable del tratamiento debe ser capaz de demostrar que el interesado ha dado su consentimiento al tratamiento, debe haber garantías de que éste es consciente de que da su consentimiento y en qué media lo hace, y la declaración de consentimiento debe ser inteligible, de fácil acceso, emplear un lenguaje claro y sencillo, y que no contenga cláusulas abusivas.

Es también novedoso el principio de responsabilidad proactiva, que obliga a las empresas a adoptar medidas que aseguren razonablemente que están en condiciones de cumplir con los principios, derechos y garantías que establece el Reglamento, o sea, considera insuficiente "no incumplir, y es una infracción no disponer de las medidas que acreditan su cumplimiento, lo que significa que hay que poder demostrar que se cumple".

Otro bloque de contenidos estuvo dedicado a revisar los derechos que tendrán los ciudadanos a partir del próximo mes de mayo, entre los que figuran el de acceso a los datos, el de rectificación, el de supresión, el de oposición o el derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado con efectos jurídicos, salvo en determinadas ocasiones.

LA SEGURIDAD

Un aspecto a tener en cuenta es también que las empresas deberán establecer el nivel adecuado al riesgo para los tratamientos de los datos, por lo que será importante realizar una evaluación para decir qué medidas organizativas y técnicas tienen que aplicar.

Dos expertos en leyes y tecnología como ponentes

ANA MARZO

Licenciada en Derecho con formación ampliada que combina los aspectos legal y técnico. Ana es socia-directora de la consultora especializada en tecnologías de la información y comunicación EQUIPO MARZO con una amplia experiencia en propiedad intelectual, protección de datos, administración electrónica, publicidad digital y consultoría y auditoría en seguridad de la información.

Es autora de numerosas publicaciones y profesora en másters, cursos y seminarios en las citadas áreas. Puedes encontrarla en nuestra sección 'Rincón legal' y en @AnaMarzoP y www.equipomarzo.com

GONZALO M. FLECHOSO

Licenciado en derecho y Auditor Cisa (ISACA), con una larga experiencia en asesoramiento en Tecnologías de la Información y la comunicación, a través de MARZO ASESORES, sobre comercio electrónico, redes sociales, contratación informática, compliance y protección de datos.

Profesor en distintos masters y cursos, y colaborador en publicaciones especializadas en TI. Puedes encontrarle en nuestro "Rincón Legal", en LinkedIn y en www.marzoasesores.com

Es novedad también en este ámbito que, ante una violación de seguridad con riesgo para los derechos y libertadas de las personas físicas, se debe notificar a la autoridad de control en 72 horas, o posteriormente motivándolo.

Si la violación entraña un alto riesgo para los derechos y las libertadas de las personas físicas, se debe comunicar a los interesados sin dilación indebida.

RESPONSABILIDADES

Hay tres figuras clave a la hora de cumplir con GDPR: el responsable del tratamiento de los datos, el encargado del tratamiento y el Delegado de Protección de los Datos o por sus siglas en inglés, DPO.

El primero es el responsable de adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

El segundo es el encargado de tratar los datos y aplicar las medidas conforme a GDPR y tiene que ofrecer las suficientes garantías. Ayudará al responsable a cumplir la seguridad, la notificación de brechas y en las evaluaciones de impacto. Tiene que notificar al responsable si alguna instrucción incumple el Reglamento.

Por último, el Delegado de Protección de los Datos, que será necesario en determinados supuestos, es un garante del cumplimiento de la normativa de la protección de datos en las organizaciones, sin sustituir las funciones que desarrollan las Autoridades de Control. Puede ser alguien interno o externo a la empresa, pero deberá contar con conocimientos especializados del Derecho, y obviamente en protección de datos ya que, entre sus funciones, se encuentra informar y asesorar, así como supervisar el cumplimiento del Reglamento por parte del responsable o encargado.

Los dos abogados también profundizaron en las evaluaciones de impacto de las operaciones de tratamiento de datos que el responsable de éstos tendrá que realizar cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, entrañe un alto riesgo para los derechos y libertadas de las personas físicas.

RECOMENDACIONES

Ana Marzo y Gonzalo M. Flechoso recomendaron a las organizaciones que para llevar la adaptación a buen término destinen a este cometido los recursos suficientes para llevar la adaptación a buen término. Y no sólo eso, sino que la gerencia debe estar implicada en este proyecto teniendo en cuenta que la normativa afecta a todos los departamentos y personas que tratan los datos. Además, recordaron que cada empresa debe cumplir hasta donde sea posible teniendo en cuenta que se trata de un proceso continuo, que nunca concluye.

En su opinión, un primer paso es plantearse qué recursos se necesita la empresa para empezar a trabajar en su adaptación a GDPR, ver qué herramientas de gestión deben utilizarse así como qué se puede aprovechar de las medidas existentes y qué es lo hay que cambiar.

También es importante planificar, asignar roles, tareas, calendarios, plazos, medidas y responsabilidades.

VALORACIÓN DE LOS EVENTOS

Ambos eventos han cumplido con nota las expectativas de los asistentes, con una puntuación media general por encima de 4 sobre un total de 5 puntos, y tanto en Madrid como en Barcelona las calificaciones más elevadas fueron la capacidad de transmisión de los ponentes y también la calidad e interés de los contenidos expuestos.

La logística del evento también fue muy bien valorada por los participantes en el workshop en ambas ciudades, con promedios de 4,30 en Barcelona y 4 en Madrid.

La presentación completa ya está disponible en la web, sólo para Asociados. Además, el artículo de este número de la sección Rincón Legal profundiza en este tema.

Workshops sobre GDPR en febrero

Febrero es un mes en el que GDPR está teniendo un gran protagonismo. No sólo se han celebrado las sesiones de Barcelona y Madrid, sino en todas las Delegaciones, además de en Zaragoza.

Ya se han celebrado las jornadas en Galicia, el día 5 de febrero; en Bilbao, el día 7; en Valencia, el 13; en Palma de Mallorca, el 14, y en Canarias, el 19. Los días 20 y 27 de este mes tendrán lugar en Sevilla y Zaragoza, respectivamente.

AUSAPE tiene también la intención de organizar también eventos temáticos específicos sobre cómo afecta la aplicación de GDPR a los entornos Cloud y a las acciones de marketing.