

Foro de la Privacidad del Data Privacy Institute

España se prepara ante el nuevo Reglamento Europeo de Protección de Datos

• *La Agencia Española de Protección de Datos, elogiada por representantes de Comisión Europea al posicionar a España como uno de los países más adelantados en la adaptación al nuevo marco normativo europeo de protección de datos.*



El pasado 1 de febrero, en el marco del **IX Foro de la Privacidad** del Data Privacy Institute (DPI) organizado por ISMS Forum Spain, máximos expertos, representantes institucionales y empresas se dieron cita para abordar la aplicabilidad del Reglamento General de Protección de Datos (RGPD) y otras cuestiones relacionadas con el impacto en la privacidad de las personas, producto del desarrollo de las nuevas tecnologías. Entre los ponentes más destacados, la directora de la Agencia Española de Protección de Datos (AEPD), Mar España; la subdirectora de la Unidad de Protección de Datos de Comisión Europea, Karolina Mojzesowicz; o el secretario de privacidad de la ONU, Joseph Cannataci. En el plano empresarial, empresas como HPE, Huawei o CaixaBank abordaron el impacto y la aplicación del nuevo Reglamento en su actividad.



El discurso inaugural de la directora de la Agencia Española de Protección de Datos, Mar España, giró en torno a la importancia de establecer una cultura preventiva y expuso las implicaciones que conllevará el nuevo Reglamento, con aplicación en España en mayo de 2018, así como el trabajo desarrollado por la Agencia para preparar y apoyar a las empresas en su proceso de adaptación. En este sentido, señaló Mar España, el primer borrador del anteproyecto de ley que modificará la actual Ley Orgánica de Protección de Datos, previsto para el próximo mes de marzo, tendrá como objetivo preparar y facilitar a las empresas para la aplicación del cambio que acontece. Todo ello, una apuesta firme de la Agencia en busca de flexibilidad, facilitando la resolución de conflictos de una manera amistosa, evitando las sanciones innecesarias y buscando el beneficio de las distintas partes implicadas. Además, las empresas que reconozcan su responsabilidad y voluntariamente cumplan el régimen sancionador podrán obtener una reducción de hasta el 40%.



En todo su discurso, Mar España remarcó la cercanía que mantiene con asociaciones empresariales del sector como ISMS Forum Spain, organización con la que mantiene un grupo específico y un canal de comunicación directo con el sector empresarial.

Desde Comisión Europea, Karolina Mojzesowicz, recordó algunas de las novedades en relación al nuevo Reglamento, como la unificación en una única normativa aplicable a todos los países miembro y por el que todas las empresas que ofrezcan bienes y servicios deberán ceñirse a esta única normativa europea, reduciendo así la competencia con empresas de una menor exigencia en materia de privacidad. Asimismo destacó que, en caso de un Data Breach, las empresas tanto públicas como privadas, tendrán la obligación de notificar a autoridades y clientes del suceso.



Foro de la Privacidad del Data Privacy Institute

Del papel a la práctica

A continuación, tuvo lugar una mesa redonda en la que los DPO's de las compañías Hewlett Packard Enterprise, Huawei y CaixaBank, debatieron sobre los problemas prácticos que pueden suponer la implantación de algunos artículos del Reglamento Europeo de Protección de Datos. Aspectos que preocupan al sector como el estrecho margen de 72 horas para la notificación de un data breach, el deber de información o la actualización de los consentimientos.

En relación a la externalización de servicios, todos coincidieron en la necesaria corresponsabilidad y la gestión de riesgos de terceros. En palabras de Pablo Díaz de Caixa-Bank, "no nos podemos permitir el riesgo de contratar a un proveedor que no cumpla con el GDPR".

Data Breach. Evaluando su impacto en el negocio.

Pedro López, profesor titular de organización de empresas y director del máster en comercio electrónico de la Universidad Complutense de Madrid, reveló cómo evaluar el grado de impacto y repercusión de un Data Breach en tres apartados: Número de registros afectados, sensibilidad de los datos que se están manejando y, por último, el sector que haya sido afectado. En este sentido, los sectores más perjudicados serían sanidad y finanzas por la sensibilidad de datos que se manejan y, el menos afectado sería el sector público ya que, a priori, no existe una competencia a la que los usuarios puedan acudir.

Soft skills del Data Privacy Officer

El headhunter Álvaro Bueno ofreció una visión de las competencias fundamentales que todo DPO debería tener, así como las cualidades indispensables para poder desarrollarse como un buen profesional. El headhunter las dividió en las llamadas Soft skills y Hard Skills. Las Hard skills, suponen la cara más técnica del profesional (conocimientos, competencias y aptitudes). Las Soft Skill atienden más a las cuestiones del desarrollo personal, habilidades sociales y más relativas a la personalidad tales como; la creatividad, el liderazgo, la empatía, la inteligencia emocional. Lo ideal, afirmó Álvaro Bueno, sería un equilibrio entre ambos y que los propios DPO's sean conscientes de sus habilidades para poder potenciarse y desarrollarse como profesionales.

Vigilancia, ¿Seguridad o manipulación?

El relator principal en materia de privacidad de Naciones Unidas, Joseph Cannataci, reflexionó sobre el estado actual de la privacidad ciudadana y hasta qué punto debería de verse comprometida a cambio de una mayor seguridad. Cannataci, explicó que Internet cuenta con billones de usuarios y que, todos ellos, dejan una huella cuando navegan por Internet exponiendo sus datos personales ante posibles riesgos. Además, exponía Cannataci, la gran mayoría de usuarios tienen una falta de conocimiento sobre los meta datos que generan y lo que ocurre con ellos en Internet, por lo que reafirmó la importancia del conocimiento del usuario así como de la necesidad de proporcionarle seguridad.



Foro de la Privacidad del Data Privacy Institute



Unido a lo anterior, Cannataci hizo énfasis en el poder de manipulación y control del individuo que genera su paso por Internet, apuntando que los gobiernos no hacen suficientes esfuerzos por advertir a los ciudadanos acerca de la recogida de datos que sufren constantemente por cuestiones de seguridad. A este respecto, Cannataci sugirió que el equilibrio pasa por no vigilar a todos los ciudadanos, sino a aquellos que presenten pruebas y evidencias para ello.

Código de Buenas Prácticas en Protección de Datos para proyectos de Big Data

Hoy en día, las empresas más competitivas necesitan conocer y comprender los mercados, los clientes, los productos, las normativas, los competidores y mucho más. Esta comprensión exige un uso eficaz de la información y su análisis inteligente, para ello surge el fenómeno del Big Data. Los datos de las empresas son ahora uno de sus mayores activos económicos; efectivamente el 73% de las organizaciones están invirtiendo o tienen planificado invertir en Big Data en los próximos 24 meses y el 25% de las empresas ya ha aumentado su presupuesto para habilidades de tecnología y de análisis. En cuanto a la oportunidad de negocio, la demanda de gastos en servicios de Big Data se calcula que alcanzará los 116.820 millones de euros a finales de este año, lo que supondrá una demanda de 4,4 millones de puestos de trabajo.

Con base en los riesgos para la privacidad inherentes a las iniciativas de Big Data, y las posibles acciones para su idónea gestión, el Data Privacy Institute publicará próximamente un “Código de buenas prácticas de protección de datos para proyectos de Big Data”, en el cual se abordan los aspectos que deben tenerse en cuenta ante iniciativas y/o proyectos de esta tipología, con el objetivo de constituir un documento útil y de interés para muchas empresas. La iniciativa surge desde la Asociación Española para el Fomento de la Seguridad de la Información, ISMS Forum Spain, a través del Data Privacy Institute, con la vocación de seguir contribuyendo al desarrollo y al conocimiento con un proyecto de colaboración entre empresas y organizaciones públicas y privadas para elaborar una guía de buenas prácticas de privacidad que sirva de referencia para todas aquellas organizaciones que estén pensando en llevar a cabo un proyecto de Big Data.

Bajo la dirección y promoción del Data Privacy Institute, el Informe se ha realizado con la colaboración de la Agencia Española de Protección de Datos y cuenta con la coordinación de Carlos A. Saiz Peña, como director del Data Privacy Institute, así como con un Comité Académico formado por expertos y empresas de diversos sectores (Finanzas, Operadoras, Aseguradoras, Constructoras, Universidades, Retail y Transporte, entre otras), que han aportado su know how y experiencia en la puesta en marcha de proyectos de Big Data y las consecuentes implicaciones de privacidad.

