Javier Lizarralde

Socio de Tecnologías de la Información y Consultoría en PKF Attest

Normativa de protección de datos: por dónde empezamos

Desde 1992, existe en España normativa de Protección de Datos de Carácter Personal. Veamos estas obligaciones como una clara oportunidad para hacer frente a las amenazas y para garantizar y proteger uno de nuestros grandes activos en la organización: La información.

¿Cómo afecta a las empresas esta normativa? El pasado 25 de mayo de 2018 resultó de plena aplicación el Reglamento General de Protección de Datos (en adelante, RGPD), el cual constituye un nuevo marco jurídico sobre la protección de los datos personales y sobre su libre circulación.

A nivel nacional, en diciembre de 2018 entró en vigor la nueva Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), que deroga la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal. Esta normativa adapta al ordenamiento jurídico español las exigencias del RGPD, y completa sus disposiciones. Entre las novedades, se encuentra la regulación en su Título X de los denominados derechos digitales. En la actualidad, ambas normativas constituyen el marco legal vigente en materia de protección de datos de carácter personal.

¿Está mi organización preparada para dar respuesta a estas obligaciones? No conozco ninguna organización que no esté expuesta a conocer e implantar las obligaciones de esta normativa. Para poder dar cumplimiento a las obligaciones, las empresas deben estar preparadas para implementar protocolos organizativos y medidas de seguridad técnicas.

La solución que inicialmente se defina ha de ser vigilada y supervisada de forma activa, incorporando los conceptos de privacidad por diseño y seguridad por defecto. Entender esta problemática pasa por entender sus *reglas de juego*: Empresas = Obligaciones vs. Ciudadanos = Derechos.

Entre las novedades más significativas: Se amplía el contenido de la información que las empresas han de facilitar a los interesados en el momento de la recogida de sus datos: base que legitima el tratamiento de los datos, período de conservación, posibles destinatarios, y los derechos que asisten a los interesados, y la forma de su ejercicio.

Aquellos tratamientos que se basen en el consentimiento del interesado, para que sea lícito debe otorgarse de manera inequívoca y/o explícita.

No hay obligación de registrar ficheros en la Agencia de Protección de Datos y es obligatorio mantener un registro de

La solución que inicialmente se defina ha de ser vigilada y supervisada de forma activa, incorporando los conceptos de privacidad por diseño y seguridad por defecto. Saber esta problemática pasa por entender sus 'reglas de juego'

actividades de tratamiento. Existe la necesidad de contar con un protocolo ante incidencias graves o brechas de seguridad que obliga a notificar a los interesados afectados y a la Agencia Española de Protección de Datos en un plazo máximo de 72 horas. Además, aparece el Delegado de Protección de Datos como nueva figura. Sus amplias funciones y responsabilidades podrán asignarse de forma interna y/o externa a la empresa, no siendo obligatoria en todos los casos, aunque sí recomendable.

En ciertos casos puede requerirse la realización de evaluaciones de impacto (EIPD). Existe la obligación de habilitar procedimientos para el ejercicio de los derechos por parte de los interesados, incluyendo los nuevos derechos que introduce el RGPD: limitación del tratamiento, portabilidad y olvido.

Te estarás preguntando: ¿Qué tengo que hacer para cumplir con la normativa? Lo mejor es que conozcas las obligaciones de tu empresa: actividad, tipología y tratamiento de datos existentes. Comienza a trabajar, en función de tu capacidad de dar respuesta a todas las obligaciones. Recomendación: pasar del suspenso al aprobado e ir año a año, mejorando las políticas de seguridad y los controles exigibles.

Asignar funciones y responsabilidades es primordial, así como entender que este camino que se comienza ya no tiene final. Hay que conseguir implantar en nuestras organizaciones una cultura y un escenario de buenas prácticas que garanticen una correcta custodia, uso y tratamiento de la información y, además, dar respuesta a las amplias obligaciones de la normativa vigente.

¿Afecta a todas las empresas y actividades por igual? Rotundamente NO. La normativa intenta ser razonable y establecer diferentes escalas de exigencia. Si bien es cierto que debe cumplirse por todas aquellas organizaciones que traten datos de carácter personal, en los casos en los que se traten categorías especiales de datos personales (creencias religiosas, salud, ideología política, entre otros), el RGPD impone mayores obligaciones, controles y garantías.

¿Qué consecuencias tiene el incumplimiento de esta normativa? Claramente, no cumplir no aporta nada y sitúa a las organizaciones en un escenario de riesgos innecesarios, ya que las sanciones por incumplimientos son absolutamente desproporcionadas.

¿Por dónde empiezo? El mayor riesgo en la organización es el desconocimiento de sus obligaciones y los errores que pueden cometer las personas. Por tanto, hay que comenzar por preparar al equipo humano que se expone a los diferentes tratamientos de datos con mayor frecuencia.

La información y los sistemas que la soportan constituyen activos valiosos e importantes para toda organización. Aprovechemos la amenaza que supone la aplicación de esta normativa, para implantar políticas internas de seguridad que garanticen la continuidad y que permitan convertir nuestras debilidades en fortalezas. El cumplimiento de la normativa sobre protección de datos proporciona confianza tanto a nivel interno para nuestros empleados y gestores, como externo para nuestros clientes, proveedores, candidatos, etc. Además, constituye un extra para la seguridad y buenas prácticas en el manejo y custodia de la información.

Javier Lizarralde

Socio de Tecnologías de la Información y Consultoría en PKF Attest

Aprovechemos la amenaza que supone la aplicación de esta normativa, para implantar políticas internas de seguridad que garanticen la continuidad y que permitan convertir nuestras debilidades en fortalezas