DECÁLOGO CONTRA EL FRAUDE EN LA CONTRATACIÓN DE PROYECTOS DE ADECUACIÓN EN PROTECCIÓN DE DATOS

Ante la preocupación presente en el sector profesional, así como en el empresarial y las propias autoridades, por prácticas inadecuadas en ofertas de consultoría en materia de privacidad, APEP ofrece un decálogo de recomendaciones básicas que permiten a las organizaciones privadas y públicas identificar cuando se les ofrece un asesoramiento adecuado y cuando no.

Al contratar un proyecto de adecuación a la normativa en protección de datos debe tenerse en cuenta que:

1. Adaptarse para cumplir la normativa requiere implicación del cliente además del trabajo del consultor o profesional. Tanto la adecuación al RGPD como mantener este cumplimiento legal en el tiempo requiere que el cliente esté concienciado; incluso es necesario que determinadas personas de la organización intervengan activamente en el proyecto. Si le ofrecen documentos estándar sin haber estudiado su empresa es muy posible que NO ESTÁ ANTE UN BUEN PROYECTO.

2. El cumplimiento no es algo puntual, la normativa exige ahora garantizar la debida diligencia y demostrar la responsabilidad activa por la protección de los datos personales. Por tanto, requiere labores y recomendaciones para mantener un adecuado nivel de cumplimiento en el tiempo. Si todo el proyecto se ciñe a la entrega de una documentación tras rellenar unos cuestionarios, y no se definen acciones que han de tener su continuidad en el tiempo, definitivamente NO ESTÁ ANTE UN BUEN PROYECTO.

3. La aplicación del RGPD nunca es teórica, no existen recetas de "copiar pegar", no basta con marcar cruces en un cuestionario, debe adaptarse a la realidad específica de la organización. Con independencia del procedimiento utilizado, su asesor debe conocer en profundidad su empresa u organización visitándola físicamente si procede, y lo habitual es que así sea si se quiere diseñar medidas de seguridad en relación con el entorno físico. Si Vd. no percibe ese interés en indagar sobre el funcionamiento real de la organización en todos los ámbitos afectados por el alcance del trabajo solicitado (jurídico, físico, informático, de gestión, etc.) NO ESTÁ ANTE UN BUEN PROYECTO.

4. Un asesoramiento adecuado debe incorporar concienciación y formación de calidad y de concienciación al personal. Las formas de llevar a cabo la formación pueden ser diversas, pero deben permitir contestar afirmativamente a las siguientes cuestiones:

– ¿Incluye medidas para que los usuarios tomen conciencia de la importancia del derecho fundamental a la protección de datos personales?

– ¿Precisa las obligaciones impuestas por la normativa y cómo cumplirlas?

– ¿Transmite las consecuencias de su incumplimiento?

Si la respuesta es negativa, NO ESTÁ ANTE UN BUEN PROYECTO.

5. L**a adaptación puede suponer cambios**. Si tras el análisis de su organización no se han identificado las buenas prácticas y no se han propuesto correcciones específicas a las que pudieran ser inadecuadas, NO ESTÁ ANTE UN BUEN PROYECTO.

6. El objetivo a perseguir ha de ser la adecuación plena, por tanto, **el proyecto debe ofrecer acciones que persigan un cumplimiento real no sólo formal**. No podemos conformarnos con un registro de actividades de tratamiento "para archivar" o un análisis de riesgos estándar que proporciona un conjunto de medidas de seguridad "pendientes de implementación" como meras recomendaciones en el mejor de los casos. La plena adaptación no concluye hasta que las medidas se hayan implementado y verificado su eficacia. Si únicamente le ofrecen plantillas generales que no se adaptan a su modelo de negocio u organización, NO ESTÁ ANTE UN BUEN PROYECTO.

7. Debe exigirse al consultor formación y capacidad específica especializada. La recogida de información debe realizarla una persona con formación cualificada que le permita adquirir la capacitación profesional que la aplicación de la normativa exige. Se requieren conocimientos tanto en el ámbito jurídico como tecnológico y organizativo. El consultor debe poder acreditar su formación y experiencia y una forma de hacerlo es a través de una certificación profesional, como puede ser la certificación ACP de APEP que reconoce formación universitaria y propia. Cuando el interlocutor en la consultora no reúna estos requisitos, NO ESTARÁ ANTE UN BUEN PROYECTO.

8. Si la empresa de consultoría se compromete a ofrecerle un certificado de cumplimiento desconfíe. El RGDP regula la certificación de cumplimiento en el Artículo 42 y garantiza unos requisitos formales para los Organismos de Certificación según el Artículo 43 que aseguren la independencia de los mismos. En España todavía no se han desarrollado los marcos de certificación para entidades, pero será una labor desarrollada por la AEPD junto con ENAC. Los certificados emitidos por empresas que a su vez ejercen labores de consultoría no garantiza los requisitos de independencia necesarios. Este certificado no lo protegerá ante malas prácticas, denuncias, inspecciones ni las sanciones que se puedan derivar. Si un proyecto le ofrece certificados de cumplimiento, desconfíe, NO ESTÁ ANTE UN BUEN PROYECTO.

9. Aunque le aseguren cubrir los daños derivados del asesoramiento o del incumplimiento del RGPD Vd. nunca estará del todo a salvo. Aunque se contrate la cobertura de un seguro, Vd. siempre se enfrenta al riesgo que para la reputación de su organización comporta la declaración de una infracción y su sanción y publicación en la web de la AEPD. La confianza de sus clientes no la garantiza ninguna aseguradora, exige un esfuerzo cotidiano. Si su consultora no le ha advertido de la necesidad de adoptar medidas de seguimiento y control, si no le ha indicado la importancia de verificar su seguridad cíclicamente y corregir cualquier defecto o incidencia que advierta, si le garantizan que no pasará nada que "el seguro lo cubre todo" NO ESTÁ ANTE UN BUEN PROYECTO.

10. Lo barato sale muy caro. En ocasiones, nos ofrecen un proyecto de adaptación al RGPD con anuncios como "esto no nos va a costar nada, o casi nada, ya que aprovecharemos una subvención de otra cosa para pagarlo". El asesoramiento jurídico y técnico no puede venderse a 2X1. Si Vd. es empresario, si administra una organización sabe perfectamente que ofrecer dos servicios por uno, y generalmente a precios por debajo de los del mercado es un negocio ruinoso. Cuando una empresa ofrezca servicios de adecuación gratuitos, a "coste cero" o "bonificados" por subvenciones por fondos de formación, puede estar ante un fraude, sancionable con mas de 180.000 euros y además NO ESTÁ ANTE UN BUEN PROYECTO.

Asociación Profesional Española de Privacidad
Palacio de Miraflores
Carera de San Jerónimo, 15.
28014 Madrid
www.apep.es

RESUMEN DECÁLOGO PARA LA CONTRATACIÓN DE PROYECTOS DE ADECUACIÓN EN PROTECCIÓN DE DATOS

Guía resumen para ayudar a las empresas y PYMES a contratar servicios de adecuación a la protección de datos con proveedores de calidad y evitar tanto servicios de mala calidad como fraudes en la oferta de servicios.

1. La adecuación es una labor conjunta entre consultora / profesional y la organización.
2. La responsabilidad activa es un proceso de mejora a mantener a diario. Es necesario poder demostrar debida diligencia.
3. El análisis jurídico debe entender los tratamientos de datos de la organización, por lo que debe ser un estudio a medida.
4. El proyecto debe incluir concienciación para asegurar la problemática y asegurar la transferencia de conocimiento.
5. La adecuación supondrá cambios en los procesos y nuevas tareas, no solo documentación. **Desconfíe de plantillas no adaptadas a su negocio**.
6. La adecuación llega cuando se ponen en marcha los procesos y las tareas recomendadas. Tener los papeles no implica cumplir la normativa.
7. El profesional debe acreditar tener formación y capacitación profesional y experiencia en privacidad para aportar valor y resolver problemas.
8. **No existen certificados de cumplimiento a organizaciones**. Desconfíe de certificados de cumplimiento: no tienen ninguna validez externa.
9. Antes de contratar basándose únicamente en el precio, piense en la seguridad jurídica que le ofrecen y piense en el daño reputacional por infracción de la normativa de protección de datos. Rodéese de buenos profesionales.
10. **Lo barato sale muy caro**. No contrate servicios de adecuación gratuitos, a "coste cero" o "bonificados" por subvenciones por fondos a la formación. Puede enfrentarse a multas de más de 180.000 euros por fraude a la Seguridad Social, así como de la Agencia Tributaria.