20210710, Nota Informativa, nueva guía evaluación de riesgos.

En virtud de mis compromisos contractuales, seguidamente paso a trasladaros el contenido de la información publicada el pasado 29 de junio en la página web de la Agencia Española de Protección de Datos sobre la puesta a disposición de una nueva guía de gestión del riesgo y evaluación de impacto en tratamientos de datos personales.

Se trata de un documento que incorpora la experiencia acumulada en la aplicación de la gestión del riesgo en el ámbito de la protección de datos desde la aplicación del Reglamento General de Protección de Datos (RGPD) y añade las interpretaciones de la AEPD, el Comité Europeo de Protección de Datos y el Supervisor Europeo de Protección de Datos.

El documento, dirigido a responsables, encargados de tratamientos y delegados de protección de datos (DPD), ofrece una visión unificada de la gestión de riesgos y de las evaluaciones de impacto en protección de datos, y facilita la integración de la gestión de riesgos en los procesos de gestión y gobernanza de las entidades.

El RGPD establece que las organizaciones que tratan datos personales deben realizar una gestión del riesgo con el fin de establecer las medidas que sean necesarias para garantizar los derechos y libertades de las personas. Además, en aquellos casos en los que los tratamientos impliquen un riesgo alto para la protección de datos, el Reglamento dispone que esas organizaciones están obligadas a realizar una Evaluación de Impacto en Protección de Datos (EIPD) para mitigar esos riesgos.

La guía presentada es aplicable a cualquier tratamiento, con independencia de su nivel de riesgo. Además, y para los casos de tratamientos de alto riesgo, incorpora las orientaciones necesarias para realizar la EIPD y, en su caso, la consulta previa a la que se refiere el artículo 36 del RGPD, que establece que el responsable debe consultar a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto sigue ofreciendo un riesgo residual alto o muy alto tras haber tomado medidas.

La Guía consta de tres apartados: el primero contiene una descripción de los fundamentos de la gestión de riesgos para los derechos y libertades; el segundo incluye un desarrollo metodológico básico para la aplicación de la gestión del riesgo, y el último está enfocado en los casos en los sea preciso realizar una EIPD, con las orientaciones necesarias para llevarla a cabo.

Además, la Agencia ha presentado "Evalúa Riesgo RGPD", el prototipo de una nueva herramienta que ayuda a responsables y encargados a identificar los factores de riesgo para los derechos y libertades de los interesados presentes en el tratamiento; hacer una primera evaluación del riesgo intrínseco, incluyendo necesidad de realizar una EIPD, y estimar el riesgo residual si se utilizan medidas y garantías para mitigar los riesgos.

Los factores de riesgo desplegados en esta herramienta no tienen carácter exhaustivo, por lo que el responsable deberá identificar aquellos que sean específicos para el tratamiento e incluirlo en su evaluación. La valoración del nivel de riesgo para cada factor que efectúa la herramienta, así como el cálculo final de nivel de riesgo, tiene carácter general y supone una evaluación mínima que, en su caso, tendrá que ser ajustada por dicho responsable para determinar con precisión el nivel de riesgo del tratamiento.

Recordemos que el análisis y la gestión de riesgos son procedimientos que permiten a las organizaciones identificar y poder anticiparse a los posibles efectos adversos o no previstos que el tratamiento pueda tener para los derechos y libertades de los interesados. Esta gestión debe permitir que el responsable tome las decisiones y acciones necesarias para conseguir que el tratamiento cumpla los requisitos del RGPD y la LOPDGDD, garantizando y pudiendo demostrar la protección de los derechos de los interesados.

Por su parte, el RGPD establece que cuando sea probable que un tipo de tratamiento entrañe un alto riesgo, el responsable debe realizar una evaluación del impacto, proceso que permite a las organizaciones identificar los riesgos que un sistema, producto o servicio puede implicar para los derechos y libertades de las personas y, tras haber realizado ese análisis, afrontar y gestionar esos peligros antes de que se materialicen.

La gestión del riesgo y la EIPD son procesos que se encuentran estrechamente vinculados, ya que la segunda es una especificidad dentro de la primera. Así, la EIPD no puede existir sin formar parte de la gestión de riesgos, por lo que mientras que la gestión del riesgo es obligatoria para todo tratamiento, las obligaciones concretas que se establecen para la EIPD lo son exclusivamente para tratamientos de alto riesgo.

Podéis acceder a la Herramienta Evalúa Riesgo RGPD a través de este enlace:

https://www.aepd.es/es/guias-y-herramientas/herramientas/evalua-riesgo-rgpd

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de julio de 2021,

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Nombre de reconocimiento (DN): c=ES, serialNumber=IDCES-32028277H, givenName=SALVADOR, sn=ZOTANO SANCHEZ, cn=ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.07.10 12:44:35 +02'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)