



La AEPD publica una guía para ayudar a las AAPP a realizar evaluaciones de impacto desde el diseño en las iniciativas legislativas

- El documento recoge unas orientaciones para que las Administraciones Públicas tengan en cuenta la necesidad de realizar una evaluación de impacto en la protección de datos desde el diseño de las normas • Las directrices están dirigidas a los organismos

(18 de abril de 2023). La Agencia Española de Protección de Datos (AEPD) ha publicado hoy [Orientaciones para la realización de una evaluación de impacto para la protección de datos en el desarrollo normativo](#), un documento destinado al sector público que aborda la necesidad de realizar una evaluación de impacto desde el diseño cuando la medida legislativa implica el tratamiento de datos personales, aportando consejos y recomendaciones para llevarla a cabo.

Dirigido a los organismos de las Administraciones Públicas que promuevan proyectos normativos que impliquen tratamientos de datos personales y a sus delegados de protección de datos, el documento analiza los requisitos previos que hay que analizar para saber si hay que hacer esa evaluación de impacto, cómo debe realizarse en caso afirmativo y qué aspectos que se deben tener en cuenta para evaluar la calidad de la misma.

La elaboración de una Memoria de Impacto Normativo (R.D. 931/2017) recoge que la Evaluación de impacto debe realizarse desde el diseño de la norma. Por su parte, la Ley Orgánica de Protección de Datos establece que el tratamiento de datos personales por obligación legal, interés público o ejercicio de poderes públicos solo puede llevarse a cabo cuando esté previsto o se derive de una competencia atribuida por una norma de Derecho de la Unión Europea o una norma con rango de ley. En caso de no existir dicha norma o no cumplir con los requisitos legales, deberá proponerse la elaboración de una norma con rango de ley que dé cobertura al tratamiento. Las Orientaciones recuerdan que el consentimiento no es, con carácter general, la base jurídica adecuada para un tratamiento establecido por norma, debido al desequilibrio entre el interesado y la autoridad pública responsable.

Una vez determinado que existe una base legal para llevar a cabo el tratamiento, la evaluación de impacto de la norma debe analizar el impacto que este va a tener sobre los derechos y libertades fundamentales de las personas, individualmente y como sociedad, aportando salvaguardas organizativas, jurídicas y técnicas.

La Agencia recuerda que el hecho de que una medida suponga riesgos para los derechos no significa que la medida no pueda proponerse, sino que tendrá que plantearse de forma que supere la Evaluación de impacto, es decir, que esos riesgos para las personas hayan podido mitigarse adecuadamente y se haya superado el análisis de necesidad, proporcionalidad e idoneidad.

Por otro lado, aquellas iniciativas que impliquen tratamientos en los que intervengan inteligencia artificial, decisiones automatizadas, biometría, vigilancia masiva, centralización a gran escala, tratamiento masivo de datos, datos de menores, de personas vulnerables, etc., podrían implicar riesgos adicionales e impactos colaterales indeseados que deben tenerse en cuenta en la evaluación de impacto.

Como material de ayuda, para ayudar a la identificación de riesgos para los derechos y libertades la Agencia recomienda consultar la guía [‘Gestión del riesgo y evaluación de impacto en tratamientos de datos personales’](#), la [‘Relación de tablas de la guía de Gestión del riesgo y evaluación de impacto’](#), o la herramienta [‘Evalúa Riesgo’](#), en la que se encuentran identificados más de 130 factores de riesgo que aparecen en la normativa de protección de datos. Además, el [Área de Administraciones Públicas](#) de la web de la Agencia recoge más recursos disponibles, como las recientes [Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales](#).