WORLD COMPLIANCE ASSOCIATION

La AEPD publica unas orientaciones para Administraciones Públicas ante el riesgo de brechas de datos personales

• El documento aborda la necesidad de gestionar de forma eficaz unos riesgos que, debido al elevado volumen de datos personales y a la interconexión de infraestructuras, pueden dar lugar a brechas masivas de gran impacto • Las directrices están dirigidas

(28 de marzo de 2023). La Agencia Española de Protección de Datos (AEPD) ha publicado hoy Orientaciones para tratamientos que implican comunicación de datos entre Administraciones Públicas ante el riesgo de brechas de datos personales, un documento destinado al sector público que aborda la **necesidad de gestionar los riesgos** derivados del tratamiento de cantidades masivas de datos personales, y su intercambio entre AAPP, tanto para los derechos y libertades de las personas como para la propia sociedad en su conjunto.

Dirigido a organismos públicos y a sus delegados de protección de datos, el documento está centrado en aquellos tratamientos en los que, debido al elevado volumen de datos personales y por la interconexión permanente entre sistemas de las Administraciones, son susceptibles de sufrir brechas masivas de datos personales de alto riesgo para los derechos fundamentales.

Las Administraciones Públicas, al igual que todos los responsables del tratamiento, han de asumir que las brechas de datos personales podrían producirse y que las medidas de seguridad no garantizan una protección total. Por lo tanto, deben implementar desde el diseño del tratamiento medidas y acciones específicas para minimizar el posible impacto personal y social de una brecha en caso de producirse. **En 2021, la Agencia recibió 163 notificaciones de brechas personales provenientes del sector público, y en 2022 esa cifra se incrementó un 49% hasta las 243.**

Una gestión eficaz de los riesgos implica la actuación coordinada de las entidades implicadas en el tratamiento, un estudio conjunto de los distintos escenarios de brechas masivas en caso de fallo de las medidas de seguridad y la adopción de los procedimientos, técnicas de protección de datos y medidas de seguridad específicas y adecuadas para minimizar su impacto sobre los derechos fundamentales. Como material de ayuda, las Orientaciones incluyen un **listado de medidas preventivas** de detección, respuesta, revisión y supervisión que se podrían implementar en el marco de este tipo de tratamientos.

La Agencia apunta en estas directrices que las infraestructuras de estos tratamientos son complejas desde el punto de vista organizativo debido a los múltiples actores que intervienen, y que esa interconexión de infraestructuras para el acceso y el intercambio de datos multiplica la probabilidad de que una brecha de datos personales termine materializándose, generando un gran impacto. Esto supone que deben aplicarse **garantías de privacidad y medidas de seguridad**, tanto técnicas como organizativas, adecuadas a estos escenarios complejos, específicas para gestionar el alto impacto social con relación a la protección de datos y de forma coordinada.

Estas Orientaciones se suman a las diversas guías y herramientas que la Agencia tiene publicadas en relación con las gestión, notificación y comunicación de brechas de datos personales, que pueden consultarse en este enlace.