¿CÓMO ACTUAR ANTE UNA BRECHA DE SEGURIDAD?

El artículo 4 del RGPD establece que las brechas de seguridad de datos personales son aquellos incidentes que ocasionan la destrucción, pérdida o alteración accidental o ilícita de datos personales, así como la comunicación o acceso no autorizado a los mismos.

Con la aplicación del RGPD, los responsables del tratamiento de datos personales tienen la obligación de notificar las brechas de seguridad que pudiesen afectar a los datos tratados; es por ello que cuando el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad debe notificarlo a la autoridad de control competente, a más tardar en las 72 horas siguientes a haber tenido noticia de esta. La realización de dicha comunicación ante la Agencia es obligatoria, a no ser que sea improbable que la brecha de seguridad entrañe un riesgo para los derechos y las libertades de las personas físicas.

Si la brecha de seguridad constituye un alto riesgo para los derechos y libertades de las personas, de forma adicional a la notificación de la autoridad de control, el responsable del tratamiento deberá comunicar a los afectados la brecha de seguridad de manera clara, sencilla, concisa y transparente.

Es por ello que la AEPD ha publicado la **Guía para la gestión y notificación de brechas de seguridad** la cual va dirigida a los responsables de tratamientos de datos personales con el objetivo de facilitar la aplicación del RGPD en lo relativo a la obligación de notificar a la autoridad competente y, en su caso, a los afectados. Se trata de un documento de apoyo que ofrece recomendaciones preventivas y planes de actuación para que las organizaciones tengan conocimiento de cómo evitar las posibles brechas de seguridad y cómo actuar en caso de que estas se produzcan.

Para más información acceda a la Guía para a gestión y notificación de brechas de seguridad