Como informar de una brecha de seguridad adecuadamente a los afectados

Se entiende como brecha de seguridad un incidente que afecta a datos de carácter personal. Este incidente puede tener un origen accidental o intencionado y además puede afectar a datos tratados digitalmente o en formato papel. En general, se trata de un suceso que ocasione destrucción, pérdida, alteración, comunicación o acceso no autorizado a datos personales.

El Reglamento (UE) 679/2016 (Reglamento General de Protección de Datos) concretamente en su artículo 33 establece que el Responsable del Tratamiento deberá notificar en un plazo máximo de 72 horas a la Agencia Española de Protección de Datos.

Si se produce una brecha con afectación a datos personales, cuando sea probable que la brecha de datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, **el responsable del tratamiento deberá realizar una comunicación a las personas afectadas describiendo en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la siguiente información:**

- Identificación comercial o pública del responsable del tratamiento y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- Descripción de la naturaleza de la brecha de seguridad: Describir si se trata de un ciberincidente, ciberataque, envío de datos por error, pérdida de documentación etc.… Especificar si concierne a datos básicos, de contacto, de email, usuarios y contraseña, copias de DNI o pasaporte, contratos, facturas etc.…

- Descripción de las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la brecha de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.
- Recomendaciones a los afectados: cambio de contraseñas, estar atentos a correos sospechosos que intenten obtener más información personal o si se está produciendo cualquier actividad inusual.

Las brechas de seguridad pueden suceder en todas las organizaciones, y resulta de vital importancia actuar en relación con las mismas de manera rápida y acorde a la ley.

Recomendamos proceder con celeridad a las brechas de seguridad, ya que la inacción puede ser causa de importantes sanciones pecuniarias.

El artículo 33 del RGPD establece que los responsables del tratamiento deben notificar a la autoridad de control competente las brechas de datos personales cuando estas puedan constituir un riesgo para los derechos y libertades de las personas. Esta notificación debe realizarse en un plazo de 72 horas desde que se tiene constancia de la brecha.

La Agencia de Protección de datos, ha publicado una guía en relación a como debe de procederse en estos supuestos. Puede acceder a la misma en el siguiente enlace :

Notificación de brechas de datos personales a la Autoridad de Control | AEPD