Cómo actuar ante posibles brechas de seguridad

Ante el aumento de ciberataques y el riesgo de que puedan comprometer datos personales de clientes, se recuerda la importancia de que los negocios de Mediación cuenten con procedimientos claros de actuación.

Para facilitar esta tarea, el Consejo ha elaborado una infografía que recoge, en siete pasos, cómo actuar ante una brecha de datos personales, desde su detección hasta las actuaciones necesarias para gestionar el incidente, con especial atención a las obligaciones y los plazos establecidos en la normativa.

El archivo, adjunto a este comunicado, está también disponible en el canal de Dropbox de los Colegios: https://www.dropbox.com/scl/fo/pqlwltmjjz58acnv5viss/AHjhMc02TP9SjeA-3TdTdYI?rlkey=53cqcqgkxrba27r3dbl53us4r&st=if2xgkft&dl=0

Como documentación complementaria, se facilita la *Guía para la notificación de brechas de datos personales de la Agencia Española de Protección de Datos (AEPD),* que desarrolla los criterios y procedimientos para valorar y notificar estos incidentes: https://www.aepd.es/guias/guia-brechas-seguridad.pdf

El Reglamento General de Protección de Datos (RGPD) establece obligaciones específicas cuando se produce una brecha, entre ellas valorar el riesgo para los derechos y libertades de las personas afectadas, notificarla a la AEPD en un plazo máximo de 72 horas cuando proceda y comunicarla a los afectados cuando exista un alto riesgo.

Estas obligaciones también deben tenerse en cuenta cuando el incidente se produce en los sistemas de proveedores que actúan como encargados del tratamiento.