20191119, Nota Informativa, sobre las brechas de seguridad.

En cumplimiento de mis deberes contractuales, seguidamente le paso a comunicar qué es aquello que se debe hacer cuando se produce una brecha de seguridad en nuestros sistemas que afecte, o pueda afectar, a la protección de los datos personales que estén bajo nuestro tratamiento; a saber:

Primero. Según el Reglamento General de Protección de Datos, constituyen violaciones de seguridad de los datos personales "todas aquellas violaciones de la seguridad que ocasionen la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos".

Segundo. De acuerdo con el artículo 32 del RGPD, **tan pronto como el responsable del tratamiento tenga conocimiento de que se ha producido una brecha de la seguridad de los datos personales debe efectuar la correspondiente notificación a la autoridad de control competente**, sin dilación y a más tardar en las 72 horas siguientes.

Tercero. Cuando en el momento de la notificación no fuese posible cumplir con la obligación de facilitar toda la información exigida, se facilitará de manera gradual, a la mayor brevedad y sin dilación. La única excepción a esta obligación de notificación tendría lugar cuando, conforme al principio de responsabilidad proactiva, el responsable pueda demostrar que la brecha de la seguridad de los datos personales no entraña un riesgo para los derechos y las libertades de las personas físicas. Por el contrario, cuando la brecha de seguridad entrañe un alto riesgo para los derechos y libertades de los titulares de los datos, además de la comunicación a la autoridad de control, el responsable del tratamiento deberá, adicionalmente, comunicar a los afectados la

brecha de seguridad sin dilación indebida y con lenguaje claro y sencillo, de forma concisa y transparente.

Cuarto. Evidentemente, tal y como hemos comentado en distintas ocasiones, en caso de que se detecte una brecha de seguridad, lo primero que se ha de hacer es ponerlo en mi conocimiento para que puede evaluar el alcance y las repercusiones del incidente.

Quinto. No obstante lo anterior, la propia Agencia Española de Protección de Datos (AEPD) reconoce que es el responsable del tratamiento de datos personales, en última instancia, quien decide acerca del tratamiento y quien asume la responsabilidad de los tratamientos de datos personales que se lleven a cabo en su organización. El Delegado de Protección de Datos asume la función de supervisar la licitud de los tratamientos informando y asesorando al responsable. Por ello, quiero enfatizar que, ante cualquier duda en este sentido o temor a que alguna actuación pueda conllevar una brecha en la seguridad, contacte conmigo a fin de asegurar la protección de los datos personales de los interesados que le hayan confiado sus datos.

En todo caso, y como siempre, quedo a disposición de cualquier duda que tenga al respecto.

Hecho, conforme a mi leal saber y entender, en Manilva, a 19 de noviembre de 2019.

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2019.11.19 08:28:58 +01'00'