ECIJA

NOTA INFORMATIVA

Sanción a grupo hospitalario por incumplimiento de medidas de seguridad de un proveedor de servicios TIC

¿Pueden sancionar a tu empresa por no hacer un seguimiento suficiente del cumplimiento de tus proveedores en materia de ciberseguridad?

Lo que necesitas saber

- El responsable del tratamiento es quien debe supervisar que se garantiza la seguridad de los tratamientos que aunque estos estén contratados a proveedores externos, dado que debe supervisar y verificar que se implementan las medidas adecuadas.

- Las medidas de seguridad que se asignen a tratamientos de datos de categorías especiales y a gran escala deben implementarse de acuerdo con el riesgo que presentan este tipo de tratamientos, por lo que los niveles básicos se muestran insuficientes.

- Las auditorías en materia de protección de datos se presentan como herramientas para comprobar los niveles de cumplimiento de aquellos tratamientos inspeccionados, y demuestran diligencia por parte del responsable del tratamiento.

- En lo que respecta al encargado de tratamiento, la implementación de medidas de seguridad adicionales para mejorar la seguridad de sus tratamientos durante la investigación ha contribuido a eximirle de una sanción.

Una reciente resolución de la Agencia Española de Protección de Datos (en adelante, "***AEPD***") sirve como el último recordatorio para responsables del tratamiento de la importancia de poder acreditar la diligencia y la responsabilidad proactiva que impone el Reglamento General de Protección de Datos (en adelante, "***RGPD***").

Esta resolución impone una sanción de 200.000 euros a un conocido grupo de hospitales que opera en todo el país, con base en un incumplimiento del artículo 32 RGPD, donde se recoge la obligación de imponer medidas de seguridad técnicas y organizativas suficientes.

A través de esta resolución, se ha podido comprobar una vez más la importancia de hacer patente el control que las empresas Responsables de tratamiento deben hacer patente de manera diligente y continuada sobre aquellos de sus proveedores que actúan como Encargados de tratamiento.

(I) Tipos de datos y medidas de seguridad

El tratamiento de datos que llevaba a cabo el Encargado del tratamiento consistía en el mantenimiento y el alojamiento de la infraestructura del software de Historia Clínica Electrónica de los hospitales del grupo sancionado.

De esta forma, dentro de este programa informático se tratan un gran número de datos personales relativos a los pacientes de este grupo, entre los que se encuentran los **siguientes datos de carácter especial: (i)** datos relativos al origen étnico o racial, **(ii)** opiniones políticas, **(iii)** convicciones religiosas o filosóficas, **(iv)** afiliación sindical, **(v)** datos genéticos o biométricos que permitan la identificación unívoca de una persona, **(vi)** datos relativos a la salud o a la vida y **(vii)** orientación sexual.

El volumen de estos datos que dentro del tratamiento de Historia Clínica Electrónica es además muy elevado, tratándose así de un **tratamiento de datos a gran escala**.

Estas dos características del tratamiento incrementan de manera significativa el riesgo que conlleva el mismo, obligando a una mayor vigilancia sobre la eficacia de las medidas de seguridad para asegurar la confidencialidad, disponibilidad e integridad de estos datos personales.

Dentro de la fase de investigación de este procedimiento, la AEPD ha encontrado las siguientes deficiencias en las medidas de seguridad interpuestas en el sistema de alojamiento del programa de *software*, alojado y mantenido por el Encargado de tratamiento:

- **Errores en el sistema de asignación de perfiles** y del sistema de trazabilidad para los accesos a la Historia Clínica Electrónica. Así las cosas, no se registraban los accesos que se hicieran con mero carácter de visualización, únicamente se guardaban, asignadas a un perfil del profesional, las modificaciones incorporadas en la Historia Clínica.

- **Incorrecta asignación de permisos**, resultando que en ciertos perfiles de trabajadores que, al no haberse delimitado los permisos correctamente,

permitían a personal no autorizada el acceso a datos especialmente protegidos innecesarios para el desarrollo de sus funciones.

- **Cifrado insuficiente**, de acuerdo con la AEPD, al tratarse de un cifrado que se aplica parcialmente sobre la información del sistema, no incluyendo a las bases de datos, y al limitarse su nivel de complejidad a un nivel bajo, sin entrar a estudiar la necesidad de medidas más robustas, necesarias y adecuadas a la tipología específica de datos personales tratados.

(II) Actuación del responsable del tratamiento

Tal y como se ha establecido anteriormente, estas deficientes medidas de seguridad se encontraban implementadas sobre los sistemas del proveedor, actuando en calidad de Encargado de tratamiento del grupo de hospitales. Sin embargo, es **el responsable del tratamiento la entidad sancionada**, debido a que la AEPD considera que ha faltado a las obligaciones intrínsecas a su rol como supervisor último de la efectividad y suficiencia de las medidas adoptadas para un tratamiento al que recurre a un proveedor en concreto.

En esta misma línea, la consideración de que la diligencia no se ha mostrado en un nivel suficiente, es alegada por la autoridad como motivo que **impide que proceda alguna disminución o graduación en la cuantía de la sanción.**

Desde la AEPD se solicitaron en varias ocasiones **los informes de posibles auditorías** que se hubiesen realizado sobre el programa inspeccionado, tanto al responsable del tratamiento como al Encargado. Esto indica la importancia de la realización de estos procesos para poder comprobar posibles deficiencias y llevar a cabo una responsabilidad proactiva tanto en las cuestiones de materia de seguridad que afecta a la propia entidad, como en sus relaciones con terceros.

Área de Protección de Datos de ECIJA

info@ecija.com

Telf: + 34 91.781.61.60